CONFERENCE MANUAL

DAY TWO

SPONSORED BY:

AMERICAN BAR ASSOCIATION
STANDING COMMITTEE ON LAW & NATIONAL SECURITY

CENTER FOR NATIONAL SECURITY LAW
UNIVERSITY OF VIRGINIA SCHOOL OF LAW

CENTER ON LAW, ETHICS AND NATIONAL SECURITY
DUKE UNIVERSITY SCHOOL OF LAW

CENTER ON NATIONAL SECURITY AND THE LAW
GEORGETOWN LAW

WASHINGTON COLLEGE OF LAW
AMERICAN UNIVERSITY

NATIONAL SECURITY LAW INSTITUTE
ANTONIN SCALIA LAW SCHOOL, GEORGE MASON UNIVERSITY

GEORGE WASHINGTON UNIVERSITY LAW SCHOOL

THE CENTER ON LAW AND SECURITY & JUST SECURITY
NEW YORK UNIVERSITY LAW SCHOOL

INSTITUTE FOR NATIONAL SECURITY AND COUNTERTERRORISM
SYRACUSE UNIVERSITY COLLEGE OF LAW

NOVEMBER 16 — NOVEMBER 17, 2017

THE CAPITAL HILTON
1001 16TH STREET, NW
WASHINGTON, D.C.
<table>
<thead>
<tr>
<th>Panel VI</th>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The Foreign Intelligence Surveillance Act (FISA)</strong></td>
<td>Choosing Both: Making Technology Choices at the Intersections of Privacy and Security — Alexander Joel</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Principles of Intelligence Transparency for the Intelligence Community — Office of the Director of National Intelligence</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>The FISA Amendments Act: Q&amp;A</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Statement before the United State Senate Committee on the Judiciary Hearing on the FISA Amendments Act: Reauthorizing America’s Vital National Security Authority and Protecting Privacy and Civil Liberties — Elizabeth Goitein</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>Guide to Posted Documents Regarding Use of National Security Authorities – as of June 2017 — Office of the Director of National Intelligence</td>
<td>61</td>
</tr>
<tr>
<td></td>
<td>Statistical Transparency Report Regarding Use of National Security Authorities for Calendar Year 2016 — Office of the Director of National Intelligence</td>
<td>66</td>
</tr>
<tr>
<td></td>
<td>IC Governance Framework Fact Sheet — The Office of the Director of National Intelligence</td>
<td>92</td>
</tr>
<tr>
<td></td>
<td>In Defense of FAA Section 702 — Chris Inglis and Jeff Kosseff</td>
<td>94</td>
</tr>
<tr>
<td></td>
<td>Trends and Predictions in Foreign Intelligence Surveillance — David Kris</td>
<td>126</td>
</tr>
<tr>
<td></td>
<td>The Fourth Amendment in the Information Age — Robert Litt</td>
<td>174</td>
</tr>
<tr>
<td></td>
<td>Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence — Office of the Director of National Intelligence</td>
<td>187</td>
</tr>
<tr>
<td></td>
<td>On Petition for Review of a Decision of the United States Foreign Intelligence Surveillance Court</td>
<td>252</td>
</tr>
<tr>
<td></td>
<td>Principle of Professional Ethics for the Intelligence Community — Office of the Director of National Intelligence</td>
<td>281</td>
</tr>
<tr>
<td></td>
<td>FISC Order Appointing an Amicus Curiae</td>
<td>282</td>
</tr>
<tr>
<td></td>
<td>Brief of Amicus Curiae</td>
<td>293</td>
</tr>
<tr>
<td></td>
<td>Government’s Response to the Court’s Briefing Order of September 16, 2015</td>
<td>327</td>
</tr>
<tr>
<td></td>
<td>Transcript of Proceedings held before the Honorable Thomas F. Hogan, Foreign Intelligence Surveillance Court</td>
<td>366</td>
</tr>
<tr>
<td></td>
<td>Memorandum Opinion and Order</td>
<td>416</td>
</tr>
<tr>
<td></td>
<td>Report on the Surveillance Programs Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act — Privacy and Civil Liberties Oversight Board</td>
<td>496</td>
</tr>
<tr>
<td></td>
<td>The Case for Reforming Section 702 of U.S. Foreign Intelligence Surveillance Law — Laura Donohue</td>
<td>692</td>
</tr>
<tr>
<td></td>
<td>The Fourth Amendment in a Digital World — Laura Donohue</td>
<td>702</td>
</tr>
</tbody>
</table>
### Panel VII

**The Arctic: National Security and Oceans Law for the New Maritime Frontier**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Warming Heats Up the American-Canadian Relationship: Resolving the Status of the Northwest Passage Under International Law — William Kim</td>
<td>929</td>
</tr>
<tr>
<td>Testimony before the U.S. Senate Foreign Relations Committee Hearing on Senate Advice on Consent to the Law of the Sea — John Norton Moore</td>
<td>950</td>
</tr>
<tr>
<td>Arctic Overview Map</td>
<td>983</td>
</tr>
<tr>
<td>Unclassified Presentation on the Arctic: National Security and Ocean’s Law for the New Maritime Frontier — Julie Gascon</td>
<td>984</td>
</tr>
</tbody>
</table>

### Panel VIII

**Current Events in National Security Law and Cyber Policy**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats — George Washington University Center for Cyber &amp; Homeland Security</td>
<td>1009</td>
</tr>
<tr>
<td>Facebook’s Community Standards: How and Where We Draw the Line — Monika Bickert</td>
<td>1085</td>
</tr>
<tr>
<td>Hard Questions: How We Counter Terrorism — Monika Bickert and Brian Fishman</td>
<td>1089</td>
</tr>
<tr>
<td>Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act — William Jeremy Robison</td>
<td>1096</td>
</tr>
<tr>
<td>Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment — Alexander Scolnik</td>
<td>1136</td>
</tr>
<tr>
<td>Electronic Communications Privacy Act of 1986</td>
<td>1182</td>
</tr>
</tbody>
</table>

### Panel IX

**Looking Forward: National Security Law Beyond 2020**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Surveillance — Office of the United States Attorney</td>
<td>1209</td>
</tr>
<tr>
<td>ISBA Professional Conduct Advisory Opinion — Illinois State Bar Association</td>
<td>1220</td>
</tr>
<tr>
<td>Electronic Surveillance – Title III Applications — Office of the United States Attorney</td>
<td>1224</td>
</tr>
<tr>
<td>Electronic Surveillance – Title III Affidavits — Office of the United States Attorney</td>
<td>1226</td>
</tr>
<tr>
<td>Electronic Surveillance – Title III Orders — Office of the United States Attorney</td>
<td>1230</td>
</tr>
<tr>
<td>Omnibus Crime Control and Safe Streets Act</td>
<td>1232</td>
</tr>
<tr>
<td>Formal Opinion 477R — American Bar Association</td>
<td>1280</td>
</tr>
</tbody>
</table>
### Conference Material: Day Two (Cont’d)

#### Panel IX (cont.)

**Looking Forward: National Security Law Beyond 2020**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Countering America’s Adversaries Through Sanctions Act</td>
<td>1291</td>
</tr>
<tr>
<td>Lawfare and U.S. National Security — Orde Kittre</td>
<td>1361</td>
</tr>
<tr>
<td>Resolution 2371 — United Nations Security Council</td>
<td>1390</td>
</tr>
<tr>
<td>Resolution 2375 — United Nations Security Council</td>
<td>1399</td>
</tr>
<tr>
<td>NASA finds ingredients for life spewing out of Saturn’s icy moon Enceladus — Sarah Kaplan</td>
<td>1408</td>
</tr>
<tr>
<td>Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure</td>
<td>1412</td>
</tr>
<tr>
<td>Foreign Intelligence Surveillance Act of 1978 Amendment Act of 2008</td>
<td>1422</td>
</tr>
<tr>
<td>Opinion 648 — Texas Center for Legal Ethics</td>
<td>1466</td>
</tr>
<tr>
<td>What Would Zero Look Like? A Treaty for the Abolition of Nuclear Weapons — David Koplow</td>
<td>1470</td>
</tr>
</tbody>
</table>

#### Panel X

**The Model Rules in the National Security Context**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Model Rules of Professional Conduct; Rules 1.1, 1.2, 1.3, 1.4, 1.6, 1.13, 3.3, 5.2 — American Bar Association</td>
<td>1571</td>
</tr>
<tr>
<td>Leaders and Lawyers — Judge James Baker</td>
<td>1593</td>
</tr>
</tbody>
</table>
Panel VI:

The Foreign Intelligence Surveillance Act (FISA)

Moderator:
Robert Litt

Discussants:
Laura Donohue
Elizabeth Goitein
Susan Hennessey
Jamil Jaffer
Alexander Joel
Choosing Both: Making Technology Choices at the Intersections of Privacy and Security

Alexander W. Joel*

Advanced technology and its creative application remain a comparative advantage for the United States, but we fear that the Intelligence Community is not adequately leveraging this advantage . . . . And this problem affects not only intelligence collection; we also lag in the use of technologies to support analysis.1

It’s six minutes before midnight as a surveillance society draws near in the United States. With a flood of powerful new technologies that expand the potential for centralized monitoring . . . we confront the possibility of a dark future where our every move, our every transaction, our every communication is recorded, compiled, and stored away, ready for access by the authorities whenever they want.2

[The Intelligence Community] must exemplify America’s values: operating under the rule of law, consistent with Americans’ expectations for protection of privacy and civil liberties, respectful of human rights, and in a manner that retains the trust of the American people.3

[“Buridan’s ass”:] a paradox whereby a hungry and thirsty donkey, placed between a bundle of hay and a pail of water, would die of hunger and thirst because there was no reason for him to choose one resource over the other.4

When you come to a fork in the road, take it.5

Technology plays a critical role in intelligence activities, enabling intelligence agencies to pursue their national-security mission more effectively and efficiently. The United States has long been a leader in

* Alexander Joel is the Civil Liberties Protection Officer for the Office of the Director of National Intelligence (ODNI). The views expressed in this Article are his own and do not imply endorsement by the ODNI or any other U.S. government agency.


technological innovation,⁶ and the Intelligence Community⁷ (IC) has recognized the importance of leveraging American technological advantages.⁸ Calls for the IC to make better use of technology are not uncommon, nor are complaints about its failure to capitalize on the latest technological developments;⁹ this is particularly true following news of a major event that the IC did not anticipate.¹⁰ Such calls often raise concurrent concerns about the civil liberties and privacy implications of placing powerful new capabilities in the hands of intelligence operatives, where they might be used in potentially unanticipated ways, cloaked from public scrutiny by rules that protect “sources and methods” from disclosure.¹¹

Intelligence officers and policy makers standing at the intersection of security and privacy can find themselves presented with a conundrum: how to make prudent technology choices? Moving in one direction seems imperative for accomplishing important national-security missions, yet raises red flags about potential impacts on privacy and civil liberties. Moving in another direction seems necessary to protect civil liberties, yet raises alarms about potentially dangerous security gaps. This dilemma calls up the image of Buridan’s ass, caught between two competing and compelling

---

⁷ The term “Intelligence Community” is defined in § 3(4) of the National Security Act of 1947, 61 Stat. 495 (codified as amended at 50 U.S.C. § 401(a) (2006)), in relatively general terms. The specific members of the IC are listed in the Director of National Intelligence’s guide. NATIONAL INTELLIGENCE: A CONSUMER’S GUIDE 9 (2009), available at http://www.dni.gov/IC_Consumers_Guide_2009.pdf. There are seventeen elements of the IC: Office of the Director of National Intelligence; Central Intelligence Agency; National Security Agency; Defense Intelligence Agency; Federal Bureau of Investigation National Security Branch; National Reconnaissance Office; National Geospatial-Intelligence Agency; Drug Enforcement Administration, Office of National Security Intelligence; Department of Energy Office of Intelligence and Counterintelligence; Department of Homeland Security Office of Intelligence and Analysis; Department of State Bureau of Intelligence and Research; Department of Treasury Office of Intelligence and Analysis; Air Force Intelligence; Army Intelligence; Coast Guard Intelligence; Marine Corps Intelligence; and Naval Intelligence. Id.
⁸ See Michael N. Schmitt, The Principle of Discrimination in 21st Century Warfare, 2 YALE HUM. RTS. & DEV. L.J. 143, 153 (1999) (asserting that developed states leverage their technological advantages in areas such as information management).
¹⁰ Indeed, soon after the attempted attack on December 25, 2009, on Flight 253, the White House announced that “[t]he U.S. government had sufficient information to have uncovered and potentially disrupted the December 25 attack . . . but analysts . . . failed to connect the dots that could have identified and warned of the specific threat. . . . Information technology . . . did not sufficiently enable the correlation of data that would have enabled analysts to highlight the relevant threat information.” Press Release, White House, White House Review Summary Regarding 12/25/2009 Attempted Terrorist Attack (Jan. 7, 2010), http://www.whitehouse.gov/the-press-office/white-house-review-summary-regarding-12252009-attempted-terrorist-attack.
considerations. It also brings to mind Yogi Berra’s famous advice on encountering a fork in the road: when forced to choose between security and privacy, find ways to “take it”—to have it both ways. Through it all, intelligence agencies must remember this: protecting privacy and civil liberties is not optional. The question they face is not whether to provide such protections—agencies are obligated, by law and duty, to provide them. Rather, the question is how to provide them while accomplishing the intelligence mission.

I. The Broader Context

The paradoxical directive that the IC use technology more aggressively because of its potential to make agencies more effective at their missions (which includes, of course, “spying”), yet refrain from using technology because of its potential intrusiveness, is a recurring one. Concerns that authorities for “espionage” might be abused if not properly overseen, given the advent of new capabilities, find eloquent expression in Justice Louis Brandeis’s dissent in a 1928 Supreme Court case. In discussing wiretapping and the invention of the telephone, Justice Brandeis warned:

Subtler and more far-reaching means of invading privacy have become available to the Government . . . . The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.

Fifty years later, the Church Committee echoed Justice Brandeis’s concerns, warning that at a time when “the technological capability of Government relentlessly increases, we must be wary about the drift toward ‘big brother government.’ The potential for abuse is awesome and requires special attention to fashioning restraints which not only cure past problems but anticipate and prevent the future misuse of technology.” Privacy and civil liberties advocacy groups, academic commentators, and others have similarly raised such concerns over the years.

12. See supra note 4 and accompanying text.
13. See supra note 5 and accompanying text.
15. S. SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS, FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES OF THE UNITED STATES SENATE, S. REP NO. 94-755, at 276 (1976).
16. See Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong. (2010) (statement of James X. Dempsey, Center for Democracy and Technology), available at http://www.judiciary.house.gov/hearings/pdf/Dempsey100505.pdf (“[I]t is clear that the balance among . . . the individual’s right to privacy, the government’s need for tools to conduct investigations, and the interest of service providers in clarity and customer trust . . . has been lost as
Public discourse is complicated in the IC arena by information disclosure restrictions and inhibitions that have traditionally gone hand-in-hand with intelligence activities.\textsuperscript{17} In part due to this lack of public transparency, popular imagination, as reflected in and fueled by fiction, television, and movies, is free to take leaps in different directions, uninhibited by the constraints—legal, policy, technical, operational, budgetary, and cultural—under which intelligence agencies operate. Satellites that peer around corners, analysts who can instantaneously access data from any source by tapping on a laptop, watch centers that can redirect surveillance cameras at any point on the globe to follow an individual running through a crowded square, supercomputers that can contact someone on his cell phone and then send him a message on an electronic billboard—these are the capabilities commonly portrayed in books and movies. Even while knowing that creative imaginations are at work, commentators focus on the imagery emerging from these works for the insights they may provide into potential intelligence capabilities, and concomitantly, potential abuses.\textsuperscript{18}

Whether fact or fiction, such imagery can affect public perceptions, and thus expectations, of the IC’s capabilities. Some may wonder whether agencies could deploy technology to instantaneously and precisely detect, identify, and track a terrorist before an attack.\textsuperscript{19} To achieve that capability, should the government acquire more computing power, access more data, and deploy more surveillance equipment? This vision of a technologically enabled future obscures bothersome details about technology that do not

\textsuperscript{17} See 50 U.S.C. § 403-1 (2006) (directing the Director of National Intelligence to protect intelligence sources and methods from unauthorized disclosure); CIA v. Sims, 471 U.S. 159, 177 (1985) (upholding the CIA’s decision to withhold its sources and methods from a disclosure request under the Freedom of Information Act).

\textsuperscript{18} For example, EAGLE EYE (DreamWorks Pictures 2008), directed by D.J. Caruso, is about a secret Department of Defense computer system that uses its ability to both access and control nearly all networked computers and devices to surveil and direct the actions of an ordinary American. A leading advocacy organization noted that “beneath the fast-paced, action packed plot are looming questions about the future of technology and the importance of government accountability.” ELEC. PRIVACY INFO. CTR., EPIC ALERT, June 22, 2009, http://epic.org/alert/EPIC_Alert_16.12.html. Similarly, ENEMY OF THE STATE (Touchstone Pictures 1998), directed by Tony Scott, about a rogue cell within the National Security Agency (NSA) that uses NSA’s surveillance technology to track every move and conversation of an American (portrayed by Will Smith), leading him at one point to disrobe to avoid surveillance, has been cited in discussions about domestic surveillance. See, e.g., Patricia Mell, Big Brother at the Door: Balancing National Security with Privacy Under the USA PATRIOT Act, 80 DENV. U. L. REV. 375, 376 n.7 (2002) (noting the Orwellian themes of the movie).

\textsuperscript{19} See, e.g., 24 (Fox Broadcasting Co. 2001) (portraying government agencies as using a variety of sophisticated technology to identify suspects, prevent terrorism, and apprehend criminals); MINORITY REPORT (Twentieth Century Fox & Dreamworks Pictures 2002) (telling the story of a world in which technology allows police to see the future and arrest potential offenders before the “precrimes” are committed).
always get comparable screen time.\textsuperscript{20} Technology functions imperfectly resulting in the potential for error. Moreover, as technology enables access to more data, it increases demands on human analysts to review and act on that data. Thus, even without considering the ways in which fiction writers have imagined that the government could abuse such technologies, we should be concerned with the less dramatic aspects of these technology-enabled visions, such as false positives and increased “noise” in the system.\textsuperscript{21}

Conversely, fictional imagery of the IC’s technological prowess may cause others to fear that such powerful capabilities could be abused or misused and to question how these types of capabilities could ever be properly controlled.\textsuperscript{22} Is the answer simply to prevent intelligence agencies from using advanced technological capabilities so as to minimize the risk of an Orwellian future? Or would there be consequences to outright prohibitions, affecting how well intelligence agencies can perform their authorized missions?

These contrasting visions of technology’s promise and peril may play a role in the paradoxical signals sent to the IC: do both more and less with technology. As the Church Committee put it thirty years ago in the midst of documenting what it characterized as a “massive record of intelligence abuses”:

We must acknowledge that the assignment which the Government has given to the Intelligence Community has, in many ways, been impossible to fulfill. It has been expected to predict or prevent every crisis, respond immediately with information on any question, act to meet all threats, and anticipate the special needs of Presidents. And then it is chastised for its zeal.\textsuperscript{23}

\begin{itemize}
\item \textsuperscript{20} See, e.g., NAT’L COMM’N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 88 (2004) (describing problems of technology development including its cost, tendency to fail, and use by terrorists for their own purposes, but concluding that in spite of all of this “Americans’ love affair with [technology] leads them to also regard it as the solution”).
\item \textsuperscript{21} See, e.g., Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs Before the S. Judiciary Comm., 110th Cong. 12 (2007) (statement of Kim Taipale, Executive Director, Center for Advanced Studies in Science and Technology Policy) (discussing false positives in data mining); ROBERTA WOHLSTETTER, PEARL HARBOR: WARNING AND DECISION (1962) (discussing the failure to anticipate the Japanese attack on Pearl Harbor as a failure to identify “signals” from the “noise,” with “signal” meaning a sign of an enemy move, and “noise” meaning competing signals that are useless for predicting that move).
\item \textsuperscript{22} See, e.g., JAY STANLEY & BARRY STEINHARDT, AM. CIVIL LIBERTIES UNION, BIGGER MONSTER, WEAKER CHAINS 1–3 (2003), available at http://www.aclu.org/files/FilesPDFs/aclu_report_bigger_monster_weaker_chains.pdf (using George Orwell’s writings and the movie Minority Report to illustrate the real-world pervasiveness of surveillance systems and the fact that such systems “rarely remain confined to their original purpose”).
\item \textsuperscript{23} S. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS, FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES OF THE UNITED STATES SENATE, S. REP NO. 94-755, at 290 (1976).
\end{itemize}
II. Keeping the Scale Balanced

Faced with these competing considerations, the obvious way ahead is to strike a balance: capitalize on America’s technological prowess while protecting privacy and civil liberties through safeguards and oversight. Even the use of the term “balance,” however, presents difficulties, returning us to the imagery of either/or choices. It raises the specter of a government official using a scale to make a decision about whether to deploy a program, where the official metaphorically weighs the benefits for national security that a new technology has to offer against the costs to privacy or civil liberties that using the technology might entail. In this vision, if the security benefits outweigh the liberty costs, the official approves the program. Alternatively, if there are only slight security benefits but heavy liberty costs, the official disapproves the program. Inherently, this view assumes a tradeoff between security and liberty—what weighs down one side of the scale necessarily causes the other side to go up—with no compromise options.24

This is a limited and ultimately unhelpful use of the balance metaphor. While it is true that there are tensions between security and liberty interests, forcing either/or choices is neither helpful to practitioners nor realistic. In practice, programs are frequently adjusted to address concerns during successive review and approval stages. And protecting privacy and civil liberties is not optional; the question is not “whether,” but “how.” Thus, rather than imagining using a scale to weigh security interests against liberty interests in forcing an either/or choice to approve a new technological capability, consider viewing the scale as a means to determine the “weight” that is needed on each side to keep the scale balanced between security and liberty. Our focus should be not on which side outweighs the other to inform a go/no-go decision. It should be on giving equal weight to security and liberty interests affected by the technology so that the scale remains balanced.25

On the security side of the scale, imagine that a new program will add weight to the scale with aspects that are potentially intrusive on privacy or that impact civil liberties.26 We should examine the program to determine

---

24. When appearing on a PBS Frontline special, a former FBI counterterrorism official stated, “I can give you more security, but I’ve got to take away some rights. And so there’s a balance. Personally, I want to live in a country where you have a common-sense, fair balance because I’m worried about people that are untrained, unsupervised, doing things with good intentions that at the end of the day, harm our liberties.” Frontline: Spying on the Home Front (PBS television broadcast May 15, 2007), available at http://www.pbs.org/wgbh/pages/frontline/homefront/etc/script.html.

25. Since program personnel are already focused on the security benefits of the new technology, the net effect of this approach is to provide a methodology for addressing the civil liberties implications of that technology under which those implications are on at least an equal footing with security interests. Of course, if there are legal requirements that apply, those must be followed regardless.

26. For purposes of this use of the balance metaphor, the scale only measures security/liberty interests that are in tension with one another, and thus only records weight on the security side of the scale if a technology program’s security measures intrude on liberty interests. The more
whether the degree of intrusiveness occasioned through use of technology is legally authorized, necessary, and narrowly tailored toward achieving a legitimate security purpose. We should also ask whether there is a less intrusive way of achieving the same purpose. The effect of these inquiries is to find ways to add only as much weight to this side of the scale as is necessary and appropriate to achieve legitimate security purposes. On the liberty side of the scale, our inquiry should focus on determining whether and how to add weights in the form of safeguards and oversight to counterbalance the impacts of the added weight on the security side. Certain technologies, then, could add weight to the security side, such as surveillance technologies, while others could add weight to the liberty side—such as anonymization and auditing applications.27

III. Protections for the Liberty Side of the Scale

Of course, this approach to the balance metaphor in evaluating new uses of technology is only helpful if there are effective privacy and civil liberties protections from which to draw to counterbalance any potential new challenges. Public discussion regarding the sources of such protections tends to focus on the Constitution—typically the First and Fourth Amendments—and statutes such as the Foreign Intelligence Surveillance Act of 197828 (FISA), the Electronic Communications Privacy Act,29 and the Privacy Act of 1974.30 However, the IC operates within an infrastructure for protecting privacy and civil liberties, for which the Constitution and applicable laws lay only the foundation.31 Beyond this foundation, the IC conducts its activities under the Executive Branch framework established by Executive Order 12,333.32 It

27. The idea of weighing considerations in a manner that avoids a zero-sum decision-making approach has been put forward by others as well. For example, Amitai Etzioni, in The Limits of Privacy, discusses four criteria for determining whether privacy concerns and the common good are in balance: Is there a well-documented, macroscopic threat to the common good, not merely a hypothetical threat? Can the threat be countered by non-privacy-intrusive measures? Can the threat be countered by minimally intrusive measures? If privacy-intrusive measures are needed, are there safeguards and measures to address “undesirable side effects”?


31. Indeed, all government employees, including intelligence officers, take an oath to support and defend the Constitution, as required by statute. 5 U.S.C. § 3331 (2006). Note that Article VI of the Constitution requires that all “executive and judicial Officers, both of the United States and of the several States, shall be bound by Oath or Affirmation, to support this Constitution.” U.S. CONST. art. VI, cl. 3.

begins by directing that “[a]ll reasonable and lawful means must be used to ensure that the United States will receive the best intelligence possible,” and makes clear that “[a]ll means, consistent with applicable Federal law and this order, and with full consideration of the rights of United States persons, shall be used.” The Order goes on to provide, “The United States Government has a solemn obligation, and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law.”

Part 1 then identifies the roles and responsibilities of the national-security and intelligence elements of the Executive Branch. Part 2 enumerates restrictions on the conduct of intelligence activities. Section 2.3 governs how IC elements may handle information concerning U.S. persons. It provides that:

[IC elements] are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order, after consultation with the Director.

As further protection, those procedures, some of which are classified, go into extensive detail about what IC elements can do with respect to such information. Section 2.3 additionally provides that “[t]hose procedures

---

33. Id. (emphasis added).
34. Id. § 1.1(a). The Order defines “United States person” broadly, as “a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.” Id. § 3.5(k).
35. Id. § 1.1(b).
37. Exec. Order No. 12,333 § 2.3.
38. Id.
shall permit collection, retention, and dissemination of the following types of information,” and lists specific types, including “information that is publicly available,” “information constituting foreign intelligence or counterintelligence,” “information obtained in the course of a lawful foreign intelligence, counterintelligence, international drug or international terrorism investigation,” “information acquired by overhead reconnaissance not directed at specific United States persons,” and “incidentally obtained information that may indicate involvement in activities that may violate Federal, state, local, or foreign laws.”

Thus, it is not enough for IC elements to satisfy requirements imposed by the Constitution or applicable statutes when collecting, retaining, and disseminating information concerning U.S. persons. They must also ensure that their actions are consistent with Executive Order 12,333 and the implementing procedures. For example, an IC element’s procedures may require it to review lawfully collected information concerning a U.S. person within a certain time period after collection to determine whether it is “information constituting foreign intelligence or counterintelligence” or whether it meets other collection and retention criteria under the Executive Order. If information fails to meet such criteria, the agency’s procedures may require the agency to destroy the information or transfer it (with no copies retained) to another agency that has proper authority. These rules are interpreted and applied by agency Offices of General Counsel and by the Department of Justice, and are audited and overseen by agency Offices of Inspector General. Possible violations are reported to the Intelligence Oversight Board of the President’s Intelligence Advisory Board.

In addition to Executive Branch protections, there are protections from the other branches as well. For example, the FISA Court issues and enforces orders relating to activities under FISA jurisdiction. Congress conducts

---


40. Exec. Order No. 12,333 § 2.3.

41. Id.

42. See, e.g., DOD DIRECTIVE, supra note 39, at 20–21 (describing procedures for retention of information about U.S. persons). Note also that section 2.3 of Executive Order 12,333 authorizes IC elements to collect, retain, and disseminate information concerning U.S. persons “consistent with the authorities provided by Part 1 of this Order.” Even if information is “publicly available,” under section 2.3(a) of the Order, the collection, retention, and dissemination of that information must be “consistent with the authorities” of that IC element. Intelligence officials must always be mindful of tying their activities to their authorized mission, even when dealing with information that is available to the public at large. This point becomes particularly relevant in considering the implications of technological change.

43. Exec. Order No. 12,333 § 1.6.

44. Exec. Order No. 13,462, 73 Fed. Reg. 11,805 (Mar. 4, 2008), as amended by Exec. Order No. 13,516, 74 Fed. Reg. 56,521 (Nov. 2, 2009). Section 1.6(c) of Executive Order 12,333 requires IC elements to report to the Intelligence Oversight Board “intelligence activities of their elements that they have reason to believe may be unlawful or contrary to executive order or presidential directive.”
oversight as a co-equal branch of government. Congressional oversight is a fundamentally important element of the civil liberties and legal infrastructure for the Intelligence Community, since Congress has access to classified information and can therefore assess the propriety of IC programs and exercise its constitutional prerogatives with respect to such activities, including the power of the purse. And there are new entities involved in providing privacy and civil liberties advice and oversight in the post-9/11 era, including the DNI’s Civil Liberties Protection Officer, the Privacy and Civil Liberties Oversight Board, and Privacy and Civil Liberties Officers established under the Implementing Recommendations of the 9/11 Commission Act of 2007. Nongovernmental organizations also play an important role by providing focused attention, expertise, and advocacy on the intersection of technology, privacy, and national security.

IV. Responding to Technological Change: Can Liberty Keep Up?

The importance of this infrastructure of laws, rules, and oversight extends beyond serving as a source from which to draw protections to

45. Congress oversees and authorizes intelligence activities through the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence and appropriates funds for such activities through appropriations committees. Due to the diversity of the community (various elements are nested within other departments, and activities impact areas of concern to multiple committees), various other committees of Congress are also involved in reviewing intelligence activities. Section 502 of the National Security Act of 1947 requires that congressional intelligence committees be kept “fully and currently informed” of all intelligence activities (covert action is covered under section 503), “with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources or methods and other exceptionally sensitive matters.” 50 U.S.C. § 413(a) (2006). Moreover, section 501 of that Act requires the President to ensure any “illegal intelligence activity is reported promptly to the intelligence committees.” Id.

46. While Congress has historically played a role in overseeing intelligence activities since the founding of the nation, the current system of intelligence oversight was explicitly established following the Church Committee era, to work in conjunction with legislation such as FISA and with Executive Branch measures such as Executive Order 12,333 and its predecessors. See Richard A. Posner, Uncertain Shield: The U.S. Intelligence System in the Throes of Reform 195 (2006); Loch K. Johnson, Governing in the Absence of Angels (detailing the relatively few times since the 1970s when Congress has devoted significant attention to reforming oversight of the IC), in Who’s Watching the Spies 57, 60 (Hans Born et al. eds., 2005).

47. The National Security Act states,

[T]he Civil Liberties Protection Officer shall ensure that the protection of civil liberties and privacy is appropriately incorporated in the policies and procedures . . . implemented by the . . . elements of the intelligence community . . . and ensure that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information.


counterbalance the impact of new capabilities being considered by the IC. Intelligence officers act on—and react to—the world around them, which is changing at ever-increasing rates due to technology.\(^{50}\) Staggering amounts of communications and data course through the world’s telecommunications systems and databases, with processing capabilities being added to smaller and smaller devices (themselves networked in new and innovative ways).\(^{51}\) Consumers now have at their fingertips impressive capabilities to access and process data from public or commercial sources. Seemingly simple query tools—coupled with the profusion of content made available by users, providers, and publishers on the Internet—provides the average computer user access to information that was unimaginable when certain of the IC-related rules just described were originally written.

The explosion of information that the average consumer has access to today—which is also accessible to the average terrorist—has implications for protections on the liberty side of the scale. Rules written with particular technologies in mind, for example, might now be seen to impede intelligence activities in ways that were not originally contemplated; they might be portrayed as weighing down the liberty side in a manner that unduly restricts intelligence capabilities. For example, in supporting the successive FISA amendments (the Protect America Act in 2007\(^{52}\) and the FISA Amendments Act in 2008\(^{53}\)) government officials stated that proposed amendments were needed to modernize FISA’s provisions.\(^{54}\) Conversely, concerns might also be raised that, because technological changes have made so much information available from so many sources, the existing rules are no longer weighty enough to adequately restrict intelligence capabilities in the manner originally intended. For example, commentators have pointed out that the growing amount of data about people’s personal lives now processed and stored by third parties is not protected by the Fourth Amendment (sometimes referred to as the “third party doctrine”).\(^{55}\)

\(^{50}\) See, e.g., John F. Duffy, *Inventing Invention: A Case Study of Legal Innovation*, 86 Texas L. Rev. 1, 66 (2007) (asserting that the electronics and software industries particularly have seen “highly rapid” technological change in the last quarter century).

\(^{51}\) See, e.g., June Jamrich Parsons & Dan Oja, *New Perspectives on Computer Concepts* 304 (2010 ed.) (“[T]he Internet is huge. Although exact figures cannot be determined, it is estimated that the Internet handles more than an exabyte of data every day. An exabyte is 1.074 billion gigabytes, and that’s a nearly unimaginable amount of data.”).


\(^{54}\) See, e.g., *Modernization of the Foreign Intelligence Surveillance Act: Hearing Before the S. Select Comm. on Intelligence*, 110th Cong. 19 (2007) (statement of J. Michael McConnell, Director of National Intelligence) (“Communications technology has evolved in ways that have had unforeseen consequences under FISA. Technological changes have brought within FISA’s scope communications that the IC believes the 1978 Congress did not intend to be covered. In short, communications currently fall under FISA that were originally excluded from the Act.”).

\(^{55}\) Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083, 1137–38 (2002) (“[I]t is only recently that we are truly beginning to see the profound implications of the Court’s third party doctrine . . . . Government information gathering
When confronted with changes in technology that seemingly outpace anything originally contemplated, what should practitioners do? It may be illuminating to briefly reconsider *Olmstead v. United States* in this context. In that 1928 case, the government used warrantless surveillance to track a “conspiracy of amazing magnitude” involving a network that included financiers, scouts, drivers, and even an attorney. The surveillance worked: the FBI disrupted the plot. On appeal, the Supreme Court confronted the question of how to apply an “old rule”—the Fourth Amendment’s requirements with its references to “persons, houses, papers, and effects”—to a “new tool,” wiretapping of telephone wires. The Court upheld the surveillance as legal, reasoning that “the invention of the telephone . . . and its application for the purpose of extending communications” could not justify expanding the Fourth Amendment “to include telephone wires, reaching to the whole world from the defendant’s house or office.” In doing so, the Court declined invitations to extend the principles of the Fourth Amendment by analogy to the “invention of the telephone,” rejecting, for example, the analogy of postal mail. Instead, the Court deferred to Congress to address the broader implications of government wiretapping.

Of course, *Olmstead* is best known for Justice Louis Brandeis’s eloquent dissent. In contrast to the majority, Justice Brandeis found that, just as the Court had previously “sustained the exercise of power by Congress . . . over objects of which the fathers could not have dreamed,” clauses guaranteeing individual protection must also “have a similar capacity of adaptation to a changing world.” Justice Brandeis reasoned that “[t]ime works changes [and] brings into existence new conditions and purposes. Therefore a principle to be vital must be capable of wider application than the mischief which gave it birth.” Justice Brandeis did not believe that a new constitutional amendment, or legislative action, was called for to address the Fourth

from the extensive dossiers being assembled with modern computer technology poses one of the most significant threats to privacy of our times.”

---

56. 277 U.S. 438 (1928).
57. *Id.* at 455.
58. The Fourth Amendment provides,

> The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.
60. *Id.* at 465.
61. *Id.*
62. *Id.* at 465–66.
63. *Id.* at 472.
64. *Id.* at 472–73 (Brandeis, J., dissenting) (quoting *Weems v. United States*, 217 U.S. 349, 373 (1910)).
Amendment’s use of terms such as “papers” and “effects.” Rather, he reasoned by analogy and found that “[t]here is, in essence, no difference between the sealed letter and the private phone message.”

What is the lesson for us? For intelligence professionals facing a landscape where new telephone-type inventions seem to multiply at an ever-increasing rate, pressure may be brought to bear to make a sharp break from prior rules—even technology-neutral ones—and to write new rules for a new era and address changes in technology that were not contemplated when the original rules were developed, particularly where those rules are oriented toward outdated technologies. Perhaps, like the Olmstead majority, we should accept that, for certain new developments, the old rules do not apply and policy makers must develop new ones.

However, when existing rules are based on sound, technology-neutral principles that protect privacy and civil liberties while enabling agencies to pursue their mission, it is not clear that writing new ones will leave us in a better place, even if those who originally crafted the rules did not imagine what technology enables today. Rules can and should be harmonized, clarified, and updated. Where wholesale revision is called for to address technological change, the challenge will be this: technology is complex, difficult to understand and describe, and continues to change rapidly. It is, therefore, a daunting task to pose to lawyers, policy makers, and the rule-making process to capture the essence of technology’s implications—in all its richness—and in a way that will enable its effective use while addressing civil liberties implications.

A visualization exercise illustrates the problem. The rate at which technology changes over time can be depicted on a chart as a steep, diagonal line, to show that it changes rapidly. Indeed, the line might also be jagged, to illustrate how technology can leap ahead in sudden spurts. By contrast, the line showing the rate at which government policies change, be they laws or internal government regulations, would be more horizontal, with periodic step increases to show that policy changes gradually and predictably. The two lines probably would not intersect—notwithstanding the title of this

65. Id.
66. Id. at 475. Indeed, he found wiretapping more problematic, since it involved the communications of more people. Id. at 476.
67. Id. at 465–66.
68. See supra note 50 and accompanying text.
69. See, e.g., Ivan K. Fong, Law and New Technology: The Virtues of Muddling Through, 19 YALE L. & POL’Y REV. 443, 454–56 (2001) (describing courts throughout the twentieth century as “struggling to fit new technologies” into then-existing legal concepts); Bradley C. Karkkainen, Bottlenecks and Baselines: Tackling Information Deficits in Environmental Regulation, 86 TEXAS L. REV. 1409, 1414 (2008) (reporting that innovative industrial sectors often complain that technology-based regulations are obsolete once promulgated because the industry has moved on to new production technologies).
symposium—leaving a gap between policy and technology at any given point in time.

This exercise illustrates a fairly obvious truth: by the time the lawyers, technologists, privacy officers, and policy makers agree on a new policy to address a technological change, that technology may well have changed again.\(^70\) If the goal is to update rules to keep pace with such change, the process may be a never-ending one. More specifically, since technologists and lawyers speak different languages, there is a risk of “technical translation error,” that the new policy will get the technology wrong.\(^71\) In addition, it is quite possible that the new policy will use terminology, or assumptions, specific to a particular technology and therefore will quickly become outdated.\(^72\)

Referring again to the imaginary chart, since it shows a steep line with technology changing quickly and a shallow line with policies changing gradually, we can predict that policies will perpetually lag technologies, leaving a gap. How to fill it? Proceeding without rules is not an option; privacy and civil liberties must be protected. Waiting to deploy the technology while new rules are written (standing there like Buridan’s ass) is no more attractive.

It may be prudent to consider Justice Brandeis’s approach,\(^73\) to find the underlying principles animating the existing rules, to reason by analogy,\(^74\) and to find ways to apply those principles to the new conditions created by technological change (akin to our common law tradition). This can help fill policy gaps while also informing policy makers as they develop new rules, should they determine such rules are called for. Applying these principles to

\(^{70}\) I am referring to policies that require acts of Congress or formal departmental or interagency processes to implement, rather than policies that could be implemented at the operating level.


\(^{72}\) See, e.g., id. at 2190 (“Detailed, technology-specific provisions reflecting the passing concerns of a moment have proven difficult to adapt to new technologies.”). Of course, it may well be important to write rules with specific technologies in mind. Yet, excess specificity can have interesting consequences. For example, in conducting oversight, an office’s mission may be to assure compliance with legal requirements, and the office may therefore find it important to require a detailed description of the relevant technology being deployed and the agency’s implementing procedures governing its use. Indeed, the absence of such detail poses problems, since it may otherwise be difficult to ascertain compliance with general standards. However, creating detailed documentation for purposes of oversight risks technical translation errors, which could later result in compliance incidents if the implementation does not match the submitted documentation. Moreover, because technology changes rapidly and unpredictably, if an agency’s procedures are premised on a certain set of external technical conditions and those conditions unexpectedly change, program personnel will need to be alert to submit modifications.

\(^{73}\) See supra note 64 and accompanying text.

new situations must, of course, occur under the civil liberties protection infrastructure discussed earlier, subject to congressional oversight and to judicial supervision where appropriate. Measures to review and enhance elements of this infrastructure, and to provide greater transparency, are in process. Seen in this context, filling any policy gaps “the Brandeis way” appears to offer a helpful way forward, even in situations where comprehensive rule changes are ultimately deemed necessary.

V. Conclusion

Making technology choices at the intersections of privacy and security does not require tradeoffs. The IC need not stand paralyzed by the choice between its core mission to provide security and its solemn obligation to protect privacy and civil liberties. Instead, we should maintain the balance between security and liberty. We should ensure, on the one side, that a new technological capability is lawful, narrowly tailored to achieve an appropriate security purpose, and that there are no less intrusive means available, while we add, on the other side, counterbalancing privacy and civil liberties protections. We should look to Justice Brandeis’s example, which remains more relevant than ever: find core principles in our tried-and-tested rules, apply them to new changes in the technological landscape, and use those principles to help us clarify and, where necessary, update our rules and develop new protections. In the end, Yogi Berra’s approach may prove truest of all: when facing a fork in the road between security and privacy, take it.

75. See supra note 31 and accompanying text.
76. See, e.g., Exec. Order No. 13,526, 75 Fed. Reg. 707 (Jan. 5, 2010) (“Protecting information critical to our Nation’s security and demonstrating our commitment to open Government through accurate and accountable application of classification standards and routine, secure, and effective declassification are equally important priorities.”).
77. See supra note 5 and accompanying text.
PRINCIPLES OF INTELLIGENCE TRANSPARENCY FOR THE INTELLIGENCE COMMUNITY

The Principles of Intelligence Transparency for the Intelligence Community (IC) are intended to facilitate IC decisions on making information publicly available in a manner that enhances public understanding of intelligence activities, while continuing to protect information when disclosure would harm national security. These Principles do not modify or supersede applicable laws, executive orders, and directives, including Executive Order 13526, Classified National Security Information. Instead, they articulate the general norms that elements of the IC should follow in implementing those authorities and requirements.

The Intelligence Community will:

1. Provide appropriate transparency to enhance public understanding about:
   a. the IC's mission and what the IC does to accomplish it (including its structure and effectiveness);
   b. the laws, directives, authorities, and policies that govern the IC's activities; and
   c. the compliance and oversight framework that ensures intelligence activities are conducted in accordance with applicable rules.

2. Be proactive and clear in making information publicly available through authorized channels, including taking affirmative steps to:
   a. provide timely transparency on matters of public interest;
   b. prepare information with sufficient clarity and context, so that it is readily understandable;
   c. make information accessible to the public through a range of communications channels, such as those enabled by new technology;
   d. engage with stakeholders to better explain information and to understand diverse perspectives; and
   e. in appropriate circumstances, describe why information cannot be made public.

3. In protecting information about intelligence sources, methods, and activities from unauthorized disclosure, ensure that IC professionals consistently and diligently execute their responsibilities to:
   a. classify only that information which, if disclosed without authorization, could be expected to cause identifiable or describable damage to the national security;
   b. never classify information to conceal violations of law, inefficiency, or administrative error, or to prevent embarrassment;
   c. distinguish, through portion marking and similar means, classified and unclassified information; and
   d. consider the public interest to the maximum extent feasible when making classification determinations, while continuing to protect information as necessary to maintain intelligence effectiveness, protect the safety of those who work for or with the IC, or otherwise protect national security.

4. Align IC roles, resources, processes, and policies to support robust implementation of these principles, consistent with applicable laws, executive orders, and directives.
The FISA Amendments Act: Q&A

The Intelligence Community’s top legislative priority for 2017 is reauthorization of the FISA Amendments Act.

The FISA Amendments Act (FAA), codified as Title VII of the Foreign Intelligence Surveillance Act (FISA) authorizes foreign intelligence surveillance activities that have been vital to keeping the nation safe. It will sunset on December 31, 2017 unless Congress passes legislation to remove or extend the sunset provision. Title VII includes not only Section 702, which concerns targeting non-United States (U.S.) persons abroad for surveillance, but also Sections 703, 704 and 705, which concern and provide statutory procedures and protections for surveillance of U.S. persons abroad. Section 702 has been the subject of significant discussion over the last several years and is the focus of this paper.

Title VII of FISA permits the government to acquire foreign intelligence information about the plans and identities of terrorists and terrorist organizations, including how they function and receive support. It enables collection of foreign intelligence information about the intentions and capabilities of spies, weapons proliferators and other foreign adversaries who threaten the United States, and it informs U.S. Intelligence Community (IC) cybersecurity efforts. Allowing the FAA to sunset would greatly impair the ability of the United States to respond to national security threats and to respond to foreign intelligence collection opportunities. Further, the additional protections established by Title VII for U.S. persons located abroad would expire with the FAA sunset.

What is the Foreign Intelligence Surveillance Act? FISA was originally enacted in 1978 to provide the Executive Branch with a court-authorized process for conducting four specific types of electronic surveillance against foreign powers or their agents operating inside the United States. The statute is still used for that original purpose, but has been amended a number of times to provide a comprehensive statutory vehicle for certain additional types of court-authorized foreign intelligence collection. Congress added Title VII of FISA in 2008 to permit additional procedures for targeting certain persons located outside the United States with surveillance. Congress reauthorized the FAA in 2012.

What is Traditional FISA? Titles I and III of FISA are often called “Traditional FISA.” These provisions apply, respectively, to the conduct of electronic surveillance and physical searches for foreign intelligence purposes of persons, facilities, or property inside the United States. Under Title I, the government files a detailed application asking the Foreign Intelligence Surveillance Court (FISC) to authorize the electronic surveillance of a facility (e.g., a telephone number or email account) or place. For this request to be granted, the government must show probable cause to believe both that the proposed target is a foreign power or an agent of a foreign power and that the facility or place is or is about to be used by that target. Under Title III, the government files a

1 U.S. persons are U.S. citizens or lawful permanent residents of the United States, as well as U.S. corporations and unincorporated associations where a substantial number of members are U.S. persons (unless the corporation or association is a foreign power). For purposes of this paper, “foreign target” or “foreign person” includes any entity that does not meet this U.S. person definition.
similar application seeking authority to search premises or property that is or is about to be owned, used, possessed by, or in transit to or from a foreign power or an agent of a foreign power. If the FISC agrees that there is probable cause and that the government’s proposed collection techniques and minimization procedures adequately protect U.S. person information acquired in the course of the collection activity, then the FISC grants the government authority to conduct the electronic surveillance or physical search.

Of note, this requirement for a judicial order based on probable cause is intended to protect the constitutional rights of U.S. persons and persons inside the United States against unreasonable searches and seizures. The Constitution does not require this practice for foreign persons located abroad.

**Why was FISA amended in 2008 through enactment of the FAA?**

When Congress enacted FISA in 1978, it drafted the law so that foreign persons located outside the U.S. would be outside of FISA’s ambit. This was accomplished in large part by defining electronic surveillance based on the technology of 1978. However, by 2008, technology had changed considerably and many terrorists and other foreign intelligence targets abroad were using communications services based in this country, especially those provided by U.S.-based Internet service providers (ISPs).

This change in technology and methods of communication meant that under FISA, as it was constructed before the FISA Amendments Act (FAA), the government often had to obtain a Traditional FISA order to compel U.S.-based ISPs to provide to the government communications of foreign persons located abroad, such as communications of a foreign terrorist using a U.S.-based ISP. As a result, in many instances, the same processes were used to conduct surveillance on foreign persons located abroad— including demonstration of probable cause — as were required to conduct surveillance on U.S. persons and persons inside the U.S. This result proved very costly. First, the significant resource demands of obtaining judicial approval for FISA surveillance meant that the government was unable to process Traditional FISA orders for numerous foreign intelligence targets outside the United States. Instead, the government prepared Traditional FISA applications for a relatively small subset of the highest-priority targets, leaving many valid foreign intelligence targets, including terrorists, outside the reach of surveillance. Second, in some instances— including high-priority cases—the government could not establish that the foreign targets met the statutory requirements intended to protect U.S. persons and persons inside the United States, including the probable cause requirements.

To address these unanticipated effects of changing technologies, and after many months of effort and public debate, Congress enacted Section 702 of FISA as part of the 2008 FAA with significant bipartisan support. It was reauthorized in 2012, again with significant bipartisan support.

**What does FISA Section 702 permit the U.S. Government to do?**

**SUMMARY**

As described in more detail below, Section 702 permits the government to target for surveillance foreign persons located outside the United States for the purpose of acquiring foreign intelligence information (with the compelled assistance of electronic communication service providers) while also providing a comprehensive oversight regime by all three branches of government to protect the constitutional and privacy interests of any U.S. person whose information may be incidentally acquired during the collection activity.
Generally, Section 702 permits the Attorney General (AG) and the Director of National Intelligence (DNI) to authorize the IC to target foreign persons reasonably believed to be located outside the U.S. for the purpose of acquiring foreign intelligence information. This acquisition is conducted pursuant to a FISC order approving a certification and accompanying targeting and minimization procedures. As described in further detail below, these documents regulate the government’s use of Section 702 and provide protections for U.S. persons. The IC acquires this foreign intelligence information with the compelled assistance of electronic communication service providers, as directed by the AG and the DNI.

Instead of issuing individual court orders, the FISC approves annual certifications submitted by the AG and the DNI that specify categories of foreign intelligence information, as defined by FISA, that the government is authorized to acquire pursuant to Section 702. The Office of the DNI (ODNI) has publicly released a sample of a certification, with required supporting documents, on its website IC on the Record.2

The AG and the DNI must also certify that IC elements will follow targeting procedures and minimization procedures that are approved by the FISC as part of the annual package.

- The targeting procedures are designed to ensure that only foreign persons located outside the U.S. are targeted for foreign intelligence collection purposes.
- The minimization procedures are intended to protect any U.S. person information that is incidentally acquired in the course of Section 702 collection. Like all other forms of legal authority that permit the government to target someone for foreign intelligence collection, Section 702 authorizes collection of communications sent or received by the target—in other words, the collection will generally include information sent to the target from other communicants and vice versa. As Congress understood when it passed the FAA, and as is true with any form of surveillance, a foreign person who has been targeted for collection under FISA Section 702 may communicate with, or discuss information concerning, a U.S. person. This is considered “incidental” acquisition of the information concerning the U.S. person, as the U.S. person was not the target of collection. Protection of this incidentally acquired U.S. person information is the reason why Congress requires minimization procedures for Section 702 collection. FISC approved minimization procedures regulate the retention and dissemination of information concerning U.S. Persons, including who may receive such information and how it is handled. Recently approved minimization procedures are available on IC on the Record.3

Once the FISC approves the certifications, including the targeting and minimization procedures, the AG and the DNI can compel electronic communications service providers to assist in IC elements’ collection against authorized Section 702 targets. A recent FISC opinion, dated November 2015, approving Section 702 certifications is available on IC on the Record.4

---

2 These documents were posted on September 29, 2015 on IC on the Record. https://tmblr.co/ZZQjısq1yCrECl. The certification is available at https://www.dni.gov/files/documents/0928/DNI-AG%20702g%20Certification.pdf.


4 This FISC opinion (“November 2015 FISC opinion”) was posted on April 19, 2016, https://tmblr.co/ZZQjısq25FHi2t, and is available at https://www.dni.gov/files/documents/20151106. April 18, 2017
UNCLASSIFIED

Why is FISA Section 702 necessary to protect national security?

Title VII of FISA is vital to keeping the nation safe. These authorities provide the government with a uniquely effective way to acquire information about the plans and identities of terrorists and terrorist organizations, including how they function and receive support. These authorities also enable collection of information about the intentions and capabilities of weapons proliferators and other foreign adversaries who threaten the U.S., and inform cybersecurity efforts. Losing these authorities would greatly impair the ability of the United States to respond to threats and to exploit important intelligence collection opportunities.

Some examples of the significant information collected through FISA Section 702 include:

- NSA has used collection authorized under FISA Section 702 to acquire extensive insight into the highest level decision-making of a Middle Eastern government. This reporting from Section 702 collection provided U.S. policymakers with the clearest picture of a regional conflict and, in many cases, directly informed U.S. engagement with the country. Section 702 collection provides NSA with sensitive internal policy discussions of foreign intelligence value.

- NSA has used collection authorized under FISA Section 702 to develop a body of knowledge regarding the proliferation of military communications equipment and sanctions evasion activity by a sanctions-restricted country. Additionally, Section 702 collection provided foreign intelligence information that was key to interdicting shipments of prohibited goods by the target country.

- Based on FISA Section 702 collection, CIA alerted a foreign partner to the presence within its borders of an al-Qaeda sympathizer. Our foreign partner investigated the individual and subsequently recruited him as a source. Since his recruitment, the individual has continued to work with the foreign partner against al-Qaeda and ISIS affiliates within the country.

- CIA has used FISA Section 702 collection to uncover details, including a photograph, that enabled an African partner to arrest two ISIS-affiliated militants who had traveled from Turkey and were connected to planning a specific and immediate threat against U.S. personnel and interests. Data recovered from the arrest enabled CIA to learn additional information about ISIS and uncovered actionable intelligence on an ISIS facilitation network and ISIS attack planning.

- NSA FISA Section 702 collection against an email address used by an al-Qaeda courier in Pakistan resulted in the acquisition of a communication sent to that address by an unknown individual located in the United States. The message indicated that the United States-based individual was urgently seeking advice regarding how to make explosives. The NSA passed this information to the FBI. Using a National Security Letter (NSL), the FBI was able to quickly identify the individual as Najibullah Zazi. Further investigation revealed that Zazi and a group of confederates had imminent plans to detonate explosives on subway lines in Manhattan. Zazi and his co-conspirators were arrested and pled guilty or were convicted of their roles in the planned attack. As the Privacy and Civil Liberties Oversight Board (PCLOB) found in its report, “[w]ithout the initial tip-off about Zazi and his plans, which came about by monitoring an overseas foreigner under Section 702, the subway-bombing plot might have succeeded.”

What are the privacy and civil liberties protections of FISA Section 702?

There are a number of provisions in the statute, the annual certifications and the targeting and minimization procedures that protect the privacy and civil liberties of U.S. persons and others located in the United States. Additionally, these provisions ensure that collection activities are focused on acquisition of specific types of information needed to protect national security.

- All acquisitions must be consistent with the Fourth Amendment.
A significant purpose of any acquisition must be to obtain foreign intelligence information. No targeting may occur outside the scope of the specified foreign intelligence purpose of a certification.

The government may not intentionally target a U.S. person anywhere in the world.

The government may not intentionally target any person known at the time of acquisition to be in the United States, regardless of nationality.

The government may not target someone located outside the United States for the purpose of targeting a particular, known person in this country or any U.S. person, regardless of location (often called “reverse targeting”).

The government may not target for acquisition “any communication as to which the sender and all intended recipients are known at the time of the acquisition” to be in the United States.

Finally, Section 702 does not involve bulk collection and does not result in “mass” surveillance. The Government individually identifies or tasks each specific communications facility, such as a phone number or email address, based on an individualized assessment that it is used by a foreign intelligence target located abroad who communicates, possesses, or is likely to receive one of the categories of foreign intelligence information authorized for acquisition by the AG and DNI.

Section 702 requires that IC elements follow targeting and minimization procedures, which must be approved by the FISC, in effectuating Section 702 collection. As discussed in more detail above, the targeting procedures are designed to ensure that only foreign persons located abroad are targeted for foreign intelligence collection purposes. The minimization procedures are intended to protect any U.S. person information incidentally acquired in the course of collection activities.

Additionally, as further discussed below, the Department of Justice (DOJ), ODNI, the Judicial Branch, and Congress perform regular and rigorous approval and oversight of the IC’s use of Section 702.

Finally, the IC itself is committed to furthering the principles of transparency—in FISA Section 702 and in other areas—as evidenced by the copious materials it has proactively declassified and provided to the public. For example, the IC and DOJ worked together to declassify and publicly release over 300 FISA-related documents, including many FISC opinions, to the maximum extent possible consistent with the need to protect classified sources, methods and techniques. This group also worked to make publicly available more than 5,000 additional pages, including IC-related official statements, congressional testimony, and transparency reporting. Many of these materials relate to the implementation of FISA Section 702.

Who oversees FISA Section 702?

The IC’s use of FISA Section 702 is overseen by the FISC itself, ODNI, DOJ, Congress, and by internal IC element entities (such as Inspectors General and civil liberties protection officers). Additionally, certain formal entities, like the Privacy and Civil Liberties Oversight Board (PCLOB), may choose to further examine and make recommendations regarding FISA Section 702-related issues.

1. The Foreign Intelligence Surveillance Court (FISC)

Oversight of FISA Section 702 collection is conducted by the FISC, which reviews the government’s Section 702 certifications, targeting procedures and minimization procedures for compliance with statutory and Fourth Amendment requirements. The intelligence agencies, via the DOJ’s National Security Division (NSD) and with notice to ODNI, regularly report to the FISC any incidents of noncompliance with those targeting and minimization procedures.5 (In 2015, ODNI publicly released certain letters notifying the FISC of incidents of

---

5 The FISC Orders approving Section 702 activities require the government to adhere to the FISC Rules of Procedure, which include Rule 13 “Correction of Misstatement or Omission; Disclosure of Non-Compliance.” These FISC Rules of Procedure are available at [http://www.fisc.uscourts.gov/rules-proofed](http://www.fisc.uscourts.gov/rules-proofed).
noncompliance, available on *IC on the Record*.\(^6\) The FISC takes those incident reports into consideration when making determinations on any subsequent certifications and targeting and minimization procedures submitted by the government.

2. **ODNI and DOJ**

The statute requires ODNI and DOJ oversight of FISA Section 702 activities. Agencies using Section 702 authority must report any potential incidents of noncompliance promptly to DOJ and ODNI. At least once every 60 days, NSD and ODNI conduct oversight of the agencies’ activities under Section 702. These reviews are normally conducted on-site by a joint team from NSD and ODNI. The team evaluates and, where appropriate, investigates each potential incident of noncompliance and conducts a detailed review of agencies’ targeting and minimization decisions. DOJ reports any identified incidents of noncompliance to the FISC. A summary of DOJ and ODNI’s oversight of Section 702 activities that was submitted to the FISC as part of the 2015 certification application is available on *IC on the Record*.\(^7\) An additional description of this oversight process is included in FISA Section 702 reports referred to as “Joint Assessments” (discussed below).

3. **Congress**

In addition to the Intelligence and Judiciary Committees’ oversight of Section 702 activities, Congress receives regular reports, mandated by statute, describing IC elements’ use of FISA-based collection authorities and any instances of noncompliance. The statute requires the AG and the DNI to report twice per year to the Intelligence and Judiciary Committees certain information concerning the implementation of Title VII. In particular, the statute requires the AG and the DNI to assess compliance with certain procedures and guidelines issued pursuant to FISA Section 702, reports referred to as “Joint Assessments.” These Joint Assessments discuss trends in compliance and may include recommended changes to help reduce compliance incidents. Several of these past reports are available on IC on the Record.\(^8\) In addition, the statute requires the AG to report twice per year on every incident of noncompliance relating to Section 702 that occurred during the applicable reporting period, requires certain Inspector Generals and certain heads of agencies to report on compliance with Section 702, and requires that Congress receive copies of the Section 702 certifications submitted to the FISC and copies of certain significant FISC opinions and related pleadings. Finally, FISA requires declassification review and public release of certain FISC opinions related to Section 702 and the public reporting of certain statistics related to the government’s use of Section 702.

4. **IC Element Internal Oversight**

Components in the intelligence agencies themselves carry out oversight of activities conducted under Section 702. For instance, Section 702 requires that each Section 702 certification be supported, as appropriate, by one or more senior IC officials, such as the head of an IC element involved in implementing Section 702. This ensures such officials’ regular involvement in the program. Moreover, all IC personnel who work with Section 702-acquired information must be trained on their agencies’ Section 702 minimization procedures,

---


7 This oversight summary was posted on *IC on the Record* on August 11, 2016, [https://tmblr.co/ZZQjsq2Aa_hL0](https://tmblr.co/ZZQjsq2Aa_hL0), and is available at [https://www.dni.gov/files/documents/UnclassOversightSummary.pdf](https://www.dni.gov/files/documents/UnclassOversightSummary.pdf).

8 The most recent publicly released joint assessments were posted on *IC on the Record* on January 13, 2017, [https://tmblr.co/ZZQjsq2H73g3F](https://tmblr.co/ZZQjsq2H73g3F), and are available at [https://icontherecord.tumblr.com/post/155810963663/release-of-joint-assessments-of-section-702](https://icontherecord.tumblr.com/post/155810963663/release-of-joint-assessments-of-section-702).
and are also trained on how to report potential compliance issues to their agency’s respective FISA program managers and other offices with oversight responsibilities. Additionally, internal bodies at the IC elements involved in implementing Section 702, such as compliance officers, civil liberties and privacy officers and inspectors general, have been involved in monitoring their agencies’ compliance with FISA and the Section 702 targeting and minimization procedures. This reflects a multi-layered approach that builds U.S. person privacy protections into the design and operation of use of this authority. As with any healthy compliance program, there is a persistent, dedicated effort to reduce the occurrence of incidents, identify incidents or risks of incidents at the earliest possible moment, and implement mitigation measures wherever possible.

5. The Privacy and Civil Liberties Oversight Board (PCLOB)

In 2014, following an extensive review, the PCLOB issued a comprehensive and public report on Section 702 that addressed certain privacy concerns, ultimately concluding that the government’s Section 702 program operates within legal constraints, collects valuable information and is both well-managed and effective in protecting national security. The PCLOB specifically noted that, “To date, there are no known instances in which government personnel deliberately violated the statute, targeting procedures, or minimization procedures.”

In that report, the PCLOB made a number of recommendations to the government intended to enhance safeguards for privacy and civil liberties in the Section 702 program. In February 2016, the PCLOB reported that all of its recommendations had been implemented in full or in part by the government.

---


- NSA’s targeting procedures should require written statements regarding the expected foreign intelligence value of collection against particular targets (Recommendation 1);
- FBI’s minimization procedures should more clearly reflect FBI’s U.S. person querying practices (Recommendation 2);
- Additional limits should be placed on the FBI’s use and dissemination of Section 702 data in connection with non-foreign intelligence criminal matters (Recommendation 2);
- NSA and CIA queries of Section 702 information using U.S. person query terms (i.e., identifiers) should be accompanied by a written explanation of the reasonable likelihood the query will return foreign intelligence (Recommendation 3);
- A random sampling of tasking sheets, as well as NSA and CIA U.S. person query terms, should be submitted annually to the FISC to assist in the FISC’s consideration of the FISA Section 702 certification renewals (Recommendation 4);
- Any rules governing the conduct of the Section 702 program should be incorporated into the annual certification process to the extent the FISC agrees that those rules are mandatory (Recommendation 5);
- NSA should continue to periodically assess the availability of additional or more advanced filtering techniques for “upstream” and for “about” collection (Recommendations 6 and 7);
- The government should publicly release the current Section 702 minimization procedures used by the CIA, FBI and NSA (Recommendation 8);
- The government should work to develop metrics for Congress and for public release providing additional insight about the extent to which NSA acquires and uses the U.S. persons information incidentally acquired through the Section 702 program (Recommendation 9); and
- The government should develop a comprehensive methodology for assessing the efficacy and relative value of counterterrorism programs (Recommendation 10).

10 Id. at 87-88 fn. 403.

What makes FISA Section 702 constitutional?
Congress recognized the constitutionality of Section 702 when it reauthorized the FAA in 2012. Further, federal courts have consistently upheld the constitutionality of Section 702. For example, in United States v. Mohamud, (9th Cir. Dec. 5, 2016), the court unanimously held that no warrant is required for a search targeted at a foreign person abroad, who lacks Fourth Amendment rights, even though some U.S. person communications were incidentally acquired in that collection. The court found that Section 702 collection was reasonable under the Fourth Amendment’s reasonableness balancing test, and that the targeting and minimization procedures sufficiently protected the defendant’s privacy interests.

What are the other components of the FAA that are due to expire?
While this paper focuses principally on Section 702, other FAA provisions also provide critical intelligence tools and civil liberties and privacy protections. Prior to the enactment of the FAA, certain of these activities fell outside the scope of FISA and were governed by Section 2.5 of Executive Order 12333, but with FAA enactment, these activities were brought within the FISC’s jurisdiction.

In contrast to Section 702, which focuses on foreign targets, Section 704 provides additional protection for collection activities directed against U.S. persons located outside of the United States. Section 2.5 of Executive Order 12333 requires the AG to approve the use of “any technique for which a warrant would be required if undertaken for law enforcement purposes” against U.S. persons abroad for intelligence purposes. The AG’s approval must be based on a determination that probable cause exists to believe the U.S. person is a foreign power or an agent of a foreign power. Section 704 builds upon these pre-FAA requirements and provides that, in addition to the AG’s approval, the government must obtain an order from the FISC in situations where the U.S. person target has “a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes.” The FISC order must be based upon a finding that there is probable cause to believe that the target is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power and that the target is reasonably believed to be located outside the United States. By requiring the approval of the FISC in addition to the approval of the AG, Section 704 provides an additional layer of civil liberties and privacy protection for U.S. persons located abroad.

In addition to Sections 702 and 704, the FAA added several other provisions to FISA. Section 701 provides definitions for Title VII. Section 703 allows the FISC to authorize an application targeting a U.S. person located outside the U.S. when the collection is conducted inside the United States. Like Section 704, Section 703 requires a finding by the FISC that there is probable cause to believe that the target is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power and is reasonably believed to be located outside the United States. Section 705 allows the government to obtain various authorities targeting U.S. persons simultaneously, provided that the requisite probable cause standard is met. Section 706 governs the use of Title VII-derived information in litigation; as with Traditional FISA, it requires the government to give notice to aggrieved persons when the government intends to use evidence obtained or derived from Title VII collection in legal proceedings. Section 707 provides for congressional oversight. Finally, Section 708 clarifies that nothing in the FAA is intended to limit the government’s ability to obtain authorizations under other parts of FISA.

What FISA Section 702 issues are likely to arise in the re-authorization discussion?
1. Amount of U.S. Person Information Incidentally Acquired under Section 702
As described above, in enacting the FAA, Congress required minimization procedures to protect the privacy of U.S. person information acquired pursuant to Section 702. Some members of Congress and others have
requested that the DNI and NSA provide a public estimate of the number of U.S. person communications incidentally acquired under Section 702. The IC and DOJ have met with staff members of both the House and Senate Intelligence and Judiciary Committees, the PCLOB, and advocacy groups to explain the obstacles that hinder the government’s ability to count with any accuracy or to even provide a reliable estimate of the number of incidental U.S. person communications collected through Section 702. For example, communicants do not usually self-identify or indicate their citizenship when communicating with the target. However, the IC recognizes the valid desire to have some sense of the nature of acquisition of incidental U.S. person communications and is working to produce a relevant metric that will inform the reauthorization debate.

2. Queries of Raw FISA Section 702 Data Using U.S. Person Identifiers

The government’s minimization procedures restrict the ability of analysts to query the databases that hold “raw” Section 702 information (i.e., where information identifying a U.S. person has not yet been minimized for permanent retention) using an identifier, such as a name or telephone number, that is associated with a U.S. person. Generally, queries of raw content are only permitted if they are reasonably designed to identify foreign intelligence information, although the FBI also may conduct such queries to identify evidence of a crime. As part of Section 702’s extensive oversight, DOJ and ODNI review the agencies’ U.S. person queries of content to ensure the query satisfies the legal standard. Any compliance incidents are reported to Congress and the FISC.

Querying databases containing Section 702 information does not result in any new acquisition of data; it is instead only an examination or re-examination of previously acquired information. Therefore, those queries are not separate “searches” for Fourth Amendment purposes. The IC queries its databases to more quickly and efficiently sort and identify communications already lawfully collected, such as information potentially related to a terrorist plot against the United States, without having to sift through each individual communication that has been collected. For example, a query made by the IC is similar to a person searching an email inbox for a particular message: An analyst could try to read every message to find the one he or she is seeking, or—instead—could query the inbox to find a particular item or to quickly ascertain that the item is not present. Queries using U.S. person identifiers in Section 702 collection help the IC detect and evaluate connections between U.S. persons and lawfully targeted foreign persons involved in perpetrating terrorist attacks or other serious national security threats. Further, these queries can assist the IC in identifying situations where a U.S. person may be the subject of an imminent threat, with the goal of protecting the U.S. person from harm. Of note, several federal courts, including the FISC, have considered this issue and have concluded that queries using U.S. person identifiers are lawful. Some have questioned whether a warrant requirement should be imposed, so that the IC would need to obtain a warrant before using a U.S. person identifier to query raw Section 702 collection. Adding such a requirement would severely hamper the speed and efficiency of operations by creating an unnecessary barrier to national security professionals’ ability to identify potential threat information already in the lawful possession of the IC.

3. Upstream Collection

For most Section 702 collection, the government acquires data from the company providing the electronic communication service to the user. Some of NSA’s Section 702 collection, however, has been obtained via “upstream” collection, in which the NSA obtains communications directly from the Internet backbone, with

---

12 Queries of Section 702 data using U.S. person identifiers are sometimes mischaracterized in the public discourse as “backdoor searches.”

the compelled assistance of companies that maintain those networks. In addition to collecting information via upstream that is “to” or “from” a target of Section 702 collection, NSA has also acquired information “about” targets of Section 702 – for example, where the target is neither the sender nor the recipient of the collected communication, but the target’s tasked selector, such as an email address, is being passed between two other communicants. The FISC has considered upstream collection and concluded that it is lawful. Furthermore, this collection has allowed the IC to acquire unique intelligence that informs cybersecurity efforts.
STATEMENT OF

ELIZABETH GOITEIN
CO-DIRECTOR, LIBERTY AND NATIONAL SECURITY PROGRAM
BRENNAN CENTER FOR JUSTICE AT NEW YORK UNIVERSITY SCHOOL OF LAW

BEFORE THE

UNITED STATES SENATE
COMMITTEE ON THE JUDICIARY

HEARING ON

THE FISA AMENDMENTS ACT: REAUTHORIZING AMERICA’S VITAL NATIONAL SECURITY AUTHORITY AND PROTECTING PRIVACY AND CIVIL LIBERTIES

JUNE 27, 2017
Introduction

Chairman Grassley, Ranking Member Feinstein, and members of the committee, thank you for this opportunity to testify on behalf of the Brennan Center for Justice at New York University School of Law. The Brennan Center is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. I co-direct the Center’s Liberty and National Security Program, which works to advance effective counterterrorism policies that respect constitutional values and the rule of law.

Congress’s goal, when it passed the FISA Amendments Act in 2008 (thus creating Section 702 of FISA), was to give our government more powerful tools to address terrorist threats. In keeping with this goal, the authorities conferred by Section 702 have been used to monitor suspected terrorists overseas in order to trace their networks and interrupt their plots. This use of the law is widely recognized as appropriate and has caused little controversy.

In writing the law, however, Congress did not expressly limit Section 702 surveillance to such activities. Instead, Congress gave significant discretion to the executive branch and the FISA Court, trusting them to ensure that the law was implemented in a manner consistent with its objective. For instance, Congress allowed the government to target any foreigner overseas, counting on intelligence agencies to focus their efforts on those who pose a threat to our interests. Congress also did not specify what minimization should look like, leaving that to the agencies and the judges of the Foreign Intelligence Surveillance Court.

It would be wrong to suggest that this trust has somehow been betrayed. There has been very little evidence of intentional abuse or misuse. The executive branch, however, has taken full advantage of the leeway provided in the statute. Instead of simply acquiring the communications of suspected terrorists or foreign powers overseas, the government is scanning nearly all of the international communications that flow into and out of the United States via the Internet backbone, and is acquiring hundreds of millions of these communications each year. This surveillance inevitably pulls in massive amounts of Americans’ calls and e-mails.

We have also seen mission creep. A statute designed to protect against foreign threats to national interests has become a major source of warrantless access to Americans’ data, and a tool for ordinary domestic law enforcement. This outcome is contrary, not only to the original intent of the Foreign Intelligence Surveillance Act, but to Americans’ expectations and their trust that Congress will protect their privacy and freedoms.

It is now up to Congress to enact reforms that will provide such protection. The core of Section 702 is the ability it gives the government to obtain the communications of foreign powers and suspected foreign terrorists without obtaining a warrant. There are several potential reforms that would leave this core intact, while adding badly needed protections for law-abiding citizens of this country and others. Most important, Congress should narrow the scope of

---

1 This testimony is submitted on behalf of a Center affiliated with New York University School of Law but does not purport to represent the school’s institutional views on this topic. More information about the Brennan Center’s work can be found at http://www.brennancenter.org.
permissible targets to those suspected of posing a threat to the U.S. and its interests, and it should shore up protections for Americans whose communications are “incidentally” collected by requiring a warrant to search their calls and e-mails and by tightening minimization requirements.

I. Section 702: A Massive Expansion in the Scope of Foreign Intelligence Surveillance

Technological advances have revolutionized communications. People are communicating at a scale unimaginable just a few years ago. International phone calls, once difficult and expensive, are now as simple as flipping a light switch, and the Internet provides countless additional means of international communication. Globalization makes such exchanges as necessary as they are easy. As a result of these changes, the amount of information about Americans that the NSA intercepts, even when targeting foreigners overseas, has exploded.²

But instead of increasing safeguards for Americans’ privacy as technology advances, the law has evolved in the opposite direction since 9/11. In its zeal to bolster the government’s powers to conduct surveillance of foreign threats, Congress has amended surveillance laws in ways that increasingly leave Americans’ information outside their protective shield (the USA FREEDOM Act being the notable exception). Section 702 is a particularly striking example.

Before 2007, if the NSA, operating domestically, sought to wiretap a foreign target’s communications with an American inside the U.S., it had to show probable cause to the Foreign Intelligence Surveillance Court (FISA Court) that the target was a foreign power – such as a foreign government or terrorist group – or its agent. The Protect America Act of 2007 and the FISA Amendments Act of 2008 (which created Section 702 of FISA) eliminated the requirement of an individualized court order. Domestic surveillance of communications between foreign targets and Americans now takes place through massive collection programs that involve no case-by-case judicial review.³

Executive officials have often argued that Section 702 was necessary to address changes in communications technology and “modernize” FISA. It is true that, before 2007, the NSA was legally required to obtain a FISA Court order to collect foreign-to-foreign e-mails that were stored inside the United States – something Congress almost certainly did not intend when it originally passed FISA. Section 702, however, went much further than necessary to correct that problem. It did not simply allow the warrantless collection of foreign-to-foreign e-mails stored inside the U.S.; it allowed the warrantless collection of communications, both stored and in transit, between foreign targets and Americans. This state of affairs differs fundamentally from the regime Congress designed in 1978.⁴

---

⁴ Some executive branch officials have suggested that Congress in 1978 intended to regulate surveillance only for purely domestic communications. They note that FISA required the government to obtain an individual court order.
Another critical change is that the pool of permissible targets is no longer limited to foreign powers or their agents. Under Section 702, the government may target for foreign intelligence purposes any person or group reasonably believed to be foreign and located overseas. The person or group need not pose any threat to the United States, have any information about such threats, or be suspected of any wrongdoing. This change not only renders innocent private citizens of other nations vulnerable to NSA surveillance; it also greatly increases the number of communications involving Americans that are subject to acquisition – as well as the likelihood that those Americans are ordinary, law-abiding individuals.

Further expanding the available universe of communications, the government and the FISA Court have interpreted Section 702 to allow the collection of any communications to, from, or about the target. The inclusion of “about” in this formulation is a dangerous leap that finds no basis in the statutory text and little support in the legislative history. In practice, it has been applied to collect communications between non-targets that include the “selectors” associated with the target (e.g., the target’s e-mail address or phone number). In theory, it could be applied even more broadly to collect any communications that even mention ISIS or a wide array of foreign leaders and public figures who are common topics of conversation. Although the NSA is prohibited from intentionally acquiring purely domestic communications, such acquisition is an inevitable result of “about” collection.

A more plausible explanation for the original FISA’s complex scheme was put forward by David Kris, a former head of the Justice Department’s National Security Division. Mr. Kris concluded that Congress intended to require a court order for international wire communications obtained in the U.S., and that the purpose behind its definitional acrobatics was to leave legislation covering surveillance conducted outside the U.S. and NSA satellite surveillance for another day. Id. at 13-23. Although Congress never followed up, the legislative history of FISA made clear that the gaps in the statute’s coverage of NSA’s operations “should not be viewed as congressional authorization for such activities as they affect the privacy interests of Americans.” S. REP. NO. 95-701, at 35 (1978), reprinted in 1978 U.S.C.C.A.N. 3973, 4004.

50 U.S.C. § 1881a(b).

The NSA’s failure to comply with minimization rules for “about” collection (discussed later in this testimony), which delayed the FISA Court’s approval of the program in 2016, led the agency to stop the practice in April of this year. However, the agency is reportedly working to solve the problems that may have led to the non-compliance. It is thus not only possible but likely that the agency will attempt to resume “about” collection in the future.

Other than the foreignness and location criteria (and certain requirements designed to reinforce them), the only limitation on collection imposed by the statute is that the government must certify that acquiring foreign intelligence is a significant purpose of the collection. FISA’s definition of foreign intelligence, however, is not limited to information about potential threats to the U.S. or its interests. Instead, it includes information “that relates to . . . the national defense or the security of the United States; or . . . the conduct of the foreign affairs of the United States.” This could encompass everyday conversations about current events. A conversation between friends or colleagues about the merits of the North American Free Trade Agreement or whether the United States should build a wall along the border with Mexico, for instance, “relates to the conduct of foreign affairs.” Moreover, while a significant purpose of the program must be the acquisition of foreign intelligence, the primary purpose may be something else altogether. Finally, the statute requires the FISA Court to accept the government’s certifications under Section 702 as long as they contain the required elements. These factors greatly weaken the force of the “foreign intelligence purpose” limitation.

The government uses Section 702 to engage in two types of surveillance. The first is “upstream collection,” whereby communications flowing into and out of the United States on the Internet backbone are scanned for selectors associated with designated foreigners. Although the data are first filtered in an attempt to weed out purely domestic communications, the process is imperfect and domestic communications are inevitably acquired. The second type of Section 702 surveillance is “PRISM collection,” under which the government provides selectors, such as e-mail addresses, to U.S.-based electronic communications service providers, who must turn over any communications to or from the selector.

Using both approaches, the government collected more than 250 million Internet transactions a year as of 2011. Because agencies generally may store Section 702 data for at least five years, a yearly intake of 250 million communications would result in at least 1.25 billion communications residing in government databases at any given time. The actual number

---

11 In re Sealed Case, 310 F.3d 717, 734 (FISA Ct. Rev. 2002).
13 PCLOB 702 REPORT, supra note 6, at 36-41.
14 Id. at 33-34.
is almost certainly higher, as the 250 million figure does not include telephonic communications, and the number of targets today is likely significantly larger than in 2011.16

Due to these changes wrought by Section 702, it can no longer be said that FISA is targeted at foreign threats. To describe surveillance that acquires hundreds of millions of communications each year as “targeted” is to elevate form over substance. And on its face, the statute does not require that the targets of surveillance pose any threat, or that the purpose of the program be the collection of threat information.

Congress no doubt trusted that the executive branch would exercise these broad powers judiciously, and would not conduct surveillance of innocent private citizens abroad simply because the statute, on its face, allows it. And it is certainly possible that the government has chosen to focus its surveillance more narrowly than Section 702 requires. The certifications that the government provides to the FISA Court – which include the foreign intelligence categories at which surveillance is aimed, and could therefore shed some light on this question – have not been publicly disclosed by the government.

Even assuming that actual practices stop short of what the law allows, however, the available statistics suggest a scope of surveillance that is difficult to reconcile with claims of narrow targeting. A leaked copy of one of the certifications, listing the foreign nations and factions about which foreign intelligence may be sought, lends support to the conclusion that surveillance is in practice quite broad: it includes most of the countries in the world, ranging from U.S. allies to small countries that play little role on the world stage.

More important, Americans’ privacy should never depend on any given administration’s voluntary self-restraint, or on the hope that the FISA Court will impose additional requirements beyond those laid out in the statute. Section 702 establishes the boundaries of permissible surveillance, and it clearly allows collection of communications between Americans and foreigners who pose no threat to the U.S. or its interests. That creates an enormous opening for unjustified surveillance and implicates a range of other harms discussed in Part III of this testimony.

II. The Impact of Section 702 on Americans

Because the “target” of surveillance must be someone reasonably believed to be a foreigner overseas, the collection of Americans’ communications with those targets is described as “incidental,” and the statute requires “minimization” of those Americans’ information. These are terms of art that have particular legal meanings. Legal and policy defenses of Section 702 in its current form rely heavily on these terms and concepts.

16 The number of targets under Section 702 has increased for each of the 4 years that the statistic has been made available. See Office of the Dir. of Nat’l Intelligence, Statistical Transparency Report Regarding the Use of National Security Authorities for Calendar Year 2016 (Apr. 2017), available at https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2016.
The impact on Americans’ privacy, however, does not. If the government is collecting tens of millions of Americans’ communications and keeping them for years in databases where they are vulnerable to abuse, inadvertent mishandling, or hacking, it matters little – from a practical perspective – that their initial acquisition was “incidental,” or that the procedures allowing them to be kept and stored include “minimization” in their title. And if FBI agents are searching this data for Americans’ communications, reading and listening to them, and using them against Americans in legal proceedings, those Americans will not be particularly comforted (indeed, they may well be baffled) to hear that they are not “targets.”

For these reasons, it is critical for Congress and the public to have a sense of the volume of Americans’ communications being collected and stored, to examine whether the retention and dissemination of Americans’ information is in fact being “minimized,” and to confront the problem of back door searches.

A. How Many Americans’ Communications Does the NSA Collect?

Section 702 surveillance obtains the communications, not only of foreign targets, but of any Americans who are in contact with them. The number of Americans’ communications thus collected is likely quite large: if only one out of every twenty communications is with an American, that would still add up to more than 12.5 million communications a year. But there is no official public information on how many Americans’ communications are in fact swept up in Section 702 surveillance.

In 2011, Senators Wyden and Udall asked the Inspectors General of the Intelligence Community and the NSA to come up with a public estimate of this number.17 The Inspectors General responded that generating an estimate would itself violate Americans’ privacy, ostensibly because it might involve reviewing communications that would otherwise not be reviewed.18 In October of 2015, however, a coalition of more than thirty advocacy groups – including many of the nation’s most prominent privacy organizations – sent a letter to the Director of National Intelligence (DNI) urging that the NSA go forward with producing an estimate.19 The letter noted that, as long as proper safeguards were in place, the result would be a net gain for privacy.

In April 2016, a bipartisan group of fourteen House Judiciary Committee members sent the DNI a letter making the same request.20 Eight months later, the members wrote again to

memorialize their understanding, in light of interim conversations and briefings, that the DNI would provide the requested estimate “early enough to inform the debate,” and with a target date of January 2017.21 By all private and public accounts, the intelligence community was close to launching its count at the beginning of this year.

It appears, however, that the government is now backing down from this commitment. In recent testimony, DNI Dan Coats suggested that it was technologically infeasible to generate an estimate without invading Americans’ privacy – the very same claim that was addressed and seemingly resolved under the previous administration.22 In short, the government is retreating to its 2012 assertion that there is no automated way to assess whether a particular communication is to or from an American.

The problem with this claim is that the NSA can, and routinely does, make such an assessment when it conducts upstream surveillance. The FISA Court has held that the Constitution requires the government to take certain concrete steps to minimize the acquisition, retention, and searching of wholly domestic communications. One of these steps, as the Privacy and Civil Liberties Board reported in 2014, is the NSA’s use of IP addresses and “comparable technical means” to automatically filter out domestic communications when conducting upstream surveillance of Internet transactions.23 Both the NSA and the FISA Court consider this method of identifying the domestic-versus-foreign status of communicants sufficient for purposes of complying with the Constitution. If it is sufficient for that purpose, it is certainly adequate to give Congress and the public a rough sense of how Section 702 collection impacts Americans.

In addition, there should be no difficulty in generating an estimate of how many Americans’ telephone calls are collected: the government can simply use the country code as a proxy. The method is not perfect – a cell phone’s country code does not always correspond with the location or nationality of the user – but again, lawmakers are seeking a rough estimate, not an exact count.

Stored e-mails, obtained through the PRISM program, are admittedly a harder case, and it is possible that some research would be required to ascertain the status of the communicants. The privacy community is nonetheless unanimous in its conclusion that the NSA should perform a one-time limited sampling of e-mails, under conditions (such as the immediate deletion of the communications after review) that would minimize the privacy intrusion.24 Such a sampling would certainly be feasible: the NSA conducted a similar exercise in 2011 when the FISA Court ordered it to ascertain how many wholly domestic communications were captured in upstream

23 See PCLOB 702 REPORT, supra note 6, at 38.
24 See Letter from Brennan Ctr. for Justice, et. al, to James Clapper, supra note 19.
surveillance.\textsuperscript{25} Given the privacy community’s overwhelming support for such an endeavor, the DNI’s reliance on privacy concerns rings hollow.

Finally, if the government is truly incapable of ascertaining, even roughly, how many Americans’ communications it is collecting, that fact is in itself alarming. Regardless of whether it is lawful, the “incidental” collection of Americans’ communications has real and significant effects on privacy – particularly when (as discussed below) that information can be stored for years, searched, and used in legal proceedings. The government cannot simultaneously assure the public that the impact of Section 702 surveillance on Americans’ privacy is minimal, while also maintaining that it has no idea – and no way to discover – how many Americans’ communications it is acquiring and storing.

\section*{B. Minimization and Its Loopholes}

Minimization procedures are intended to mitigate the effects of “incidental” collection. The concept behind minimization is fairly simple: The interception of Americans’ communications when targeting foreigners is inevitable, but because such interception would otherwise require a warrant or individual FISA order, incidentally collected U.S. person information generally should not be kept, shared, or used, subject to narrow exceptions.

The statutory language, however, is much more complex. It requires the government to adopt minimization procedures, which it defines as procedures “that are reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.”\textsuperscript{26} The statute also prohibits disseminating non-foreign intelligence information in a way that identifies U.S. persons unless their identity is necessary to understand foreign intelligence information or assess its importance. The one caveat is that the procedures must “allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.”\textsuperscript{27}

The lack of specificity in this definition, and the tension between its general rule and its caveat, has allowed the government to craft rules that are permissive and contain multiple exceptions. To begin with, the NSA may share raw data from its PRISM collection with the FBI, the CIA, and (as of April 2017) the National Counterterrorism Center (NCTC).\textsuperscript{28} All four agencies generally may keep unreviewed raw data – including data about U.S. persons – for five

\footnotesize
\textsuperscript{26} 50 U.S.C. § 1801(h)(1).
\textsuperscript{27} 50 U.S.C. § 1801(h)(3).
years after the certification expires;29 they also can seek extensions from a high-level official,30
and the 5-year limit does not apply to encrypted communications (which are becoming
increasingly common among ordinary users of mobile devices) or communications “reasonably
believed to contain secret meaning.”31 The agencies may keep indefinitely any U.S. person
information that has foreign intelligence value or is evidence of a crime.32

If the NSA discovers U.S. person data that has no foreign intelligence value and contains
no evidence of a crime, the agency is supposed to purge the data.33 The NSA, however, interprets
this requirement to apply only if the NSA analyst determines “not only that a communication is
not currently of foreign intelligence value to him or her, but also would not be of foreign
intelligence value to any other present or future foreign intelligence need.”34 This is an
impossibly high bar, and so, “in practice, this requirement rarely results in actual purging of
data.”35

The FBI, CIA, and NCTC have no affirmative requirement to purge irrelevant U.S.
person data on detection, relying instead on age-off requirements. Moreover, if the FBI reviews
U.S. person information and makes no determination regarding whether it is foreign intelligence
information or evidence of a crime, the 5-year limit evaporates, and the FBI may keep the data
for a longer period of time that remains classified.36 If the NCTC reviews U.S. person

29 Id. at § 3(c)(1) (2016) (although the retention period for communications obtained through upstream collection is
two years, as specified in section 3(c)(2)); Loretta Lynch, U.S. Dep’t of Justice, Minimization Procedures
Used by the Federal Bureau of Investigation in Connection with Acquisitions of Foreign Intelligence
Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as
Amended § III.G.1.a (2016) [hereinafter FBI 702 Minimization Procedures], available at
_part_1_and_part_2_merged.pdf; Loretta Lynch, U.S. Dep’t of Justice, Minimization Procedures Used by
the Central Intelligence Agency in Connection with Acquisitions of Foreign Intelligence
Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as
Amended § 2 (2016) [hereinafter CIA 702 Minimization Procedures], available at
pdf; Loretta Lynch, U.S. Dep’t of Justice, Minimization Procedures Used by the National
Counterterrorism Center in Connection with Acquisitions of Foreign Intelligence Information
Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended § B(2)(a)
(2016) [hereinafter NCTC 702 Minimization Procedures], available at
.pdf.

30 PClOB 702 Report, supra note 6, at 60; NCTC 702 Minimization Procedures, supra note 29, at § B(2)(a).
31 NSA 702 Minimization Procedures, supra note 28, at § 6(a)(1)(d); CIA 702 Minimization Procedures, supra
note 29, at § 3.c.
32 NSA 702 Minimization Procedures, supra note 28, at § 6(a); FBI 702 Minimization Procedures, supra note
29, at § III.G; CIA 702 Minimization Procedures, supra note 29, at §§ 3.a, 7.d; NCTC 702 Minimization
Procedures, supra note 29, at § B(3).
33 NSA 702 Minimization Procedures, supra note 28, at §§ 3(b)(1), 3(c).
34 PCLOB 702 Report, supra note 6, at 62.
35 Id.
36 FBI 702 Minimization Procedures, supra note 29, at § III.G.1.b.
information and makes no determination as to its status, it can keep the information for 15 years.37

If any of the four agencies – all of which have access to raw data – disseminate information to other agencies, they must first obscure the identity of the U.S. person; but once again, there are several exceptions to this rule. For instance, the agencies need not obscure the U.S. person’s identity if it is necessary to understand or assess foreign intelligence or if the communication contains evidence of a crime.38

In short, the NSA routinely shares raw Section 702 data with the FBI, CIA, and NCTC; and the agencies’ minimization procedures suggest that U.S. person information is almost always kept for at least five years and, in many circumstances, much longer. The sharing and retention of U.S. person information are not unrestricted, but it is a stretch to say that they are “minimized” under any common sense understanding of the term.

C. Back Door Searches

Perhaps the most problematic aspect of the minimization procedures is that they allow all four agencies to query Section 702 data using U.S. person identifiers, with the express goal of retrieving and analyzing Americans’ communications.39

If the government wishes to obtain an American’s communications for foreign intelligence purposes, it must secure an individual court order from the FISA Court after demonstrating that the target is an agent of a foreign power. If the government wishes to obtain an American’s communications for law enforcement purposes, it must get a warrant from a neutral magistrate. To ensure that Section 702 is not used to avoid these requirements, the statute contains a prohibition on “reverse targeting” – i.e., targeting a foreigner overseas when the government’s intent is to target “a particular, known person reasonably believed to be in the United States.” Before conducting Section 702 surveillance, the government must certify that it does not intend to target particular, known Americans.

And yet, immediately upon obtaining the data, all four agencies may sort through it looking for the communications of particular, known Americans – the very people in whom the government just disclaimed any interest. Worse, even though the FBI would be required to obtain a warrant in order to access Americans’ communications absent a significant foreign intelligence purpose, the FBI may – and, “with some frequency,”40 does – search the Section 702 data for Americans’ communications to use in criminal proceedings having no foreign

38 FBI 702 MINIMIZATION PROCEDURES, supra note 29, at § V.A-B; NSA 702 MINIMIZATION PROCEDURES, supra note 28, at § 6(b); CIA 702 MINIMIZATION PROCEDURES, supra note 29, at §§ 5, 7.d; NCTC 702 MINIMIZATION PROCEDURES, supra note 29, at § D(1)-(2).
39 NSA 702 MINIMIZATION PROCEDURES, supra note 28, at § 3(b)(5); FBI 702 MINIMIZATION PROCEDURES, supra note 29, at § III.D; CIA 702 MINIMIZATION PROCEDURES, supra note 29, at § 4; NCTC 702 MINIMIZATION PROCEDURES, supra note 29, at § C(1).
40 PCLOB 702 REPORT, supra note 6, at 59.
intelligence dimensions whatsoever. This is a bait and switch that is utterly inconsistent with the spirit, if not the letter, of the prohibition on reverse targeting. It also creates a massive end run around the Fourth Amendment’s warrant requirement.

Some have defended these “back door searches,” claiming that as long as information is lawfully acquired, agencies may use the information for any legitimate government purpose. This argument ignores Congress’s command to agencies to “minimize” information about U.S. persons. The very meaning of “minimization” is that agencies may not use the information for any purpose they wish. Minimization is a constitutional requirement as well as a statutory one: as Judge Bates of the FISA Court has observed, “[T]he procedures governing retention, use, and dissemination bear on the reasonableness under the Fourth Amendment of a program for collecting foreign intelligence information.”

Indeed, restrictions on searches of lawfully obtained data are the constitutional norm, not the exception. In executing warrants to search computers, the government routinely seizes and/or copies entire hard drives. However, agents may only conduct searches reasonably designed to retrieve those documents or files containing the evidence specified in the warrant. Moreover, if a different agency wishes to search the seized data for a different purpose, it must obtain a separate warrant for that search. The fact that the government lawfully obtained and is in possession of the computer’s contents does not give it license to conduct any search it wishes; that would violate the terms on which the government obtained the computer’s contents in the first place.

The same principle holds true in the analog world. When the police obtain a warrant to search a house for a murder weapon, they may enter the house and, in appropriate cases, search every room. But after they find (or fail to find) the murder weapon, they are not allowed to continue searching for other items they may have some interest in, simply because they are now in the house. Their entrance into the house was legal, but that does not entitle them to search for anything inside it. That would be exceeding the terms accompanying their initial access to the house.

---

42 [Redacted], 2011 WL 10945618, at *27 (FISA Ct. Oct. 3, 2011). In cases involving the foreign intelligence exception to the warrant requirement, the reasonableness of a surveillance scheme turns on weighing the government’s national security interest against the privacy intrusion. While the surveillance scheme should be evaluated as a whole, it is difficult to see how any scheme could pass the reasonableness test if a significant component of the scheme were not justified by any national security interest. This is one of several errors, in my view, in the FISA Court’s 2015 decision upholding the constitutionality of back door searches. See Elizabeth Goitein, The FBI’s Warrantless Surveillance Back Door Just Opened a Little Wider, JUST SEC. (Apr. 21, 2016), https://www.justsecurity.org/30699/fbis-warrantless-surveillance-door-opened-wider/.
43 See, e.g., United States v. Gancias, 755 F.3d 125 (2nd Cir. 2014), rev’d en banc on other grounds, 824 F.3d 199 (2nd Cir. 2016).
Under Section 702, the terms on which the government is authorized to collect data without a warrant include a limitation on whom the government may target – i.e., the government may only target foreigners overseas. To obtain access to the data on those terms and then search for Americans’ data is the equivalent of seizing a computer to search for child pornography and then searching for evidence of tax fraud, or obtaining access to a house to search for a murder weapon and then conducting a search for drugs.

Back door searches are not rare occurrences. In 2016, the NSA and CIA – agencies that are have limited jurisdiction within the United States – performed U.S. person queries of communications content on 5,288 occasions. The NSA further conducted U.S. person queries of communications metadata 30,355 times (the CIA does not report this data). The FBI, however, is by far the most prolific user of back door searches. Although the FBI is exempt from the statutory requirement to report U.S. person query statistics, the Privacy and Civil Liberties Oversight Board (PCLOB) has reported that the FBI searches databases containing 702 data “whenever [i]t opens a new national security investigation or assessment,” and conducts similar searches “with some frequency” when performing “criminal investigations and assessments that are unrelated to national security efforts.”

The government has attempted to downplay the effect on Americans’ privacy, asserting that back door searches rarely return information in non-national security cases. In November 2015, the FISA Court ordered the FBI to report on “[e]ach instance in which FBI personnel received and reviewed Section 702-acquired information that the FBI identified as concerning a U.S. person in response to a query that was designed to return evidence of a crime unrelated to foreign intelligence.” The FBI reported only one such instance in 2016.

But this number is almost certainly misleading. For one thing, the FBI has long claimed that it cannot ascertain how many back door searches it conducts because it often does not know, or attempt to learn, the U.S. person status of the subjects of its queries. If that is the case, limiting the reporting to cases in which the information has been affirmatively “identified as concerning a U.S. person” will result in an undercount. At a more basic level, limiting the reporting to queries “unrelated to foreign intelligence” ignores the fact that the government ordinarily must obtain an individualized order from the FISA Court in order to access Americans’ communications in foreign intelligence investigations. That requirement is being circumvented in an untold number of cases.

Compounding the constitutional harm of back door searches, the government has not fully and consistently complied with its statutory and constitutional obligation to notify criminal defendants when it uses evidence “obtained or derived from” Section 702 surveillance. Before 2013, the government interpreted “obtained or derived from” so narrowly that it notified no one.

---

46 Id. at 9.
47 PCLOB 702 Report, supra note 6, at 59.
49 Id.
In the four years since the government’s approach reportedly changed, the government has provided notification in only eight known cases, even though the PCLOB reports that the FBI searches Section 702 every time it conducts a national security investigation and there have been several hundred terrorism and national security convictions during this time.

There is reason for concern that the government is avoiding its notification requirements by engaging in “parallel construction” – i.e., recreating the Section 702 evidence using less controversial means. Attorneys have asked the Department of Justice to share its policies for determining when information is considered to be “derived from” Section 702, but the Department refuses to provide them.

Importantly, opposition to warrantless searches for U.S. person information is not a call to re-build the barriers to cooperation among agencies often attributed to “the wall.” Threat information, including threat information that focuses on U.S. persons, can and should be shared among agencies when identified, and the agencies should work together as necessary in addressing the threat. What the Fourth Amendment cannot tolerate is the government collecting information without a warrant with the intent of mining it for use in ordinary criminal cases against Americans. That is why President Obama’s Review Group on Intelligence and Communications Technologies – a five-person panel including a former acting director of the CIA (Michael J. Morell) and chief counterterrorism advisor to President George W. Bush (Richard A. Clarke) – unanimously recommended closing the “back door search” loophole by prohibiting searches for Americans’ communications without a warrant.

III. Risks and Harms of Mass Data Collection

The mass collection and storage of communications that include sensitive information about Americans carries with it significant risks and harms, which must be considered in evaluating what the appropriate scope of surveillance should be.

A. Risk of Abuse or Mishandling of Data

The substantive legal restrictions on collecting information about Americans are looser than they have been since before 1978. At the same time, the amount of data available to the government and the capacity to store and analyze that data are orders of magnitude greater than

51 DEP’T OF JUSTICE, UNITED STATES ATTORNEYS’ ANNUAL STATISTICAL REPORT FISCAL YEAR 2015 at 14; DEP’T OF JUSTICE, UNITED STATES ATTORNEYS’ ANNUAL STATISTICAL REPORT FISCAL YEAR 2014 at 12; DEP’T OF JUSTICE, UNITED STATES ATTORNEYS’ ANNUAL STATISTICAL REPORT FISCAL YEAR 2013 at 60.
they were during the period of J. Edgar Hoover’s worst excesses. History teaches us that this combination is an extraordinarily dangerous one.

To date, there is only limited evidence of intentional abuse of foreign intelligence surveillance authorities. There have, however, been multiple significant instances of non-compliance by the NSA with FISA Court orders. Notably, these include cases in which the NSA did not detect the non-compliance for years, and the agency’s overseers had no way to uncover the incidents in the meantime. Given that these incidents went unreported for years even when the agency was *not* trying to conceal them, it is not clear how overseers would learn about intentional abuses that agency officials were making every effort to hide.

Moreover, the fact that little evidence of intentional abuse has emerged to date is not a cause for complacency. Government insiders have made reference to a “culture of compliance” and professionalism that emerged in the decades following the Church Committee’s investigation. But organizational cultures change, and are highly influenced by leadership. There is simply no guarantee that the degree of institutional self-restraint exercised in the past will continue indefinitely.

In this vein, it is significant that some intelligence experts who until recently defended the wide discretion permitted by Section 702 have seemingly revisited their conclusions in light of today’s tumultuous and uncertain political landscape. Matthew Olsen, who served as NSA General Counsel and the Director of the National Counterterrorism Center, was a strong supporter of the FISA Amendments Act when it was being debated in 2008 and has often testified on its behalf. At a recent public conference, however, he stated: “I fought hard . . . for increasing information sharing . . . [and] for the modernization of FISA . . . . As I fought for these changes, I did not bargain on the current political environment. That was beyond my ability to imagine . . . [T]his is a time of . . . soul-searching for me.”

In any event, inadvertent failures to adhere to privacy protections are a concern in their own right. On multiple occasions in the past decade, the FISA Court has had occasion to rebuke the NSA for repeated, significant, and sometimes systemic failures to comply with court orders. These failures took place under multiple foreign intelligence collection authorities (including Section 702) and at all points of the programs: collection, dissemination, and retention. It is

---


instructive to review some of the Court’s comments in these cases. The following statements are excerpted from five opinions spanning the years 2009 through 2017:

- “In summary, since January 15, 2009, it has finally come to light that the FISC’s authorizations of this vast [Section 215 telephony metadata] collection program have been premised on a flawed depiction of how the NSA uses [the] metadata. This misperception by the FISC existed from the inception its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government’s submissions, and despite a government-devised and Court-mandated oversight regime. The minimization procedures proposed by the government in each successive application and approved and adopted as binding by the orders of the FISC have been so frequently and systemically violated that it can fairly be said that this critical element of the overall [bulk collection] regime has never functioned effectively.”

- “The government has compounded its non-compliance with the Court’s orders by repeatedly submitting inaccurate descriptions . . . to the FISC.”

- “[T]he NSA continues to uncover examples of systematic noncompliance.”

- “Under these circumstances, no one inside or outside of the NSA can represent with adequate certainty whether the NSA is complying with those procedures.”

- “[U]ntil this end-to-end review is completed, the Court sees little reason to believe that the most recent discovery of a systemic, ongoing violation . . . will be the last.”

- “The Court is troubled that the government’s revelations regarding NSA’s acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program.”

- “The current application [for pen register/trap and trace data] . . . raises issues that are closely related to serious compliance problems that have characterized the government’s implementation of prior FISA orders.”

- “As far as can be ascertained, the requirement was simply ignored.”

- “Notwithstanding this and many similar prior representations, there in fact had been systematic overcollection since [redacted]. . . . This overcollection . . . had occurred continuously since the initial authorization . . . .”

- “The government has provided no comprehensive explanation of how so substantial an overcollection occurred.”

- “[G]iven the duration of this problem, the oversight measures ostensibly taken since [redacted] to detect overcollection, and the extraordinary fact that the NSA’s end-to-end

---

58 In re Production of Tangible Things from [Redacted], No. BR 08-13, at 10-11 (FISA Ct. Mar. 2, 2009).
59 Id. at 6.
60 Id. at 10.
61 Id. at 15.
62 Id. at 16.
65 Id. at 19.
66 Id. at 20.
67 Id. at 21.
review overlooked unauthorized acquisitions that were documented in virtually every record of what was acquired, it must be added that those responsible for conducting oversight at NSA failed to do so effectively.”

- “The history of material misstatements in prior applications and non-compliance with prior orders gives the Court pause before approving such an expanded collection. The government’s poor track record with bulk PR/TT acquisition...presents threshold concerns about whether implementation will conform with, or exceed, what the government represents and the Court may approve.”

- “As noted above, NSA’s record of compliance with these rules has been poor. Most notably, NSA generally disregarded the special rules for disseminating United States person information outside of NSA until it was ordered to report such disseminations and certify to the FISC that the required approval had been obtained...The government has provided no meaningful explanation why these violations occurred, but it seems likely that widespread ignorance of the rules was a contributing factor.”

- “Given NSA’s longstanding and pervasive violations of the prior orders in this matter, the Court believes that it would be acting well within its discretion in precluding the government from accessing or using such information.”

- “[The] cases in which the FBI had not established the required review teams seemed to represent a potentially significant rate of non-compliance.”

- “The Court was extremely concerned about these additional instances of non-compliance.”

- “Perhaps more disturbing and disappointing than the NSA’s failure to purge this information for more than four years, was the government’s failure to convey to the Court explicitly during that time that the NSA was continuing to retain this information . . . .”

- “The Court did not find entirely satisfactory the government’s explanations of the scope of [its] segregation errors and the adequacy of its response to them . . . .”

- “[A] non-compliance rate of 85% raises substantial questions about the appropriateness of using [a redacted tool] to query FISA data.”

- “At the October 26, 2016 hearing, the Court ascribed the government’s failure to disclose those [Inspector General] and [NSA Office of Compliance for Operations] reviews at the October 4, 2016 hearing to an institutional lack of candor on NSA’s part and emphasized that this is a very serious Fourth Amendment issue.”

---

68 Id. at 22.
69 Id. at 77.
70 Id. at 95.
71 Id. at 115.
72 [Redacted], at 48-49 (FISA Ct. Nov. 6, 2015), available at www.dni.gov%2Ffiles%2Fdocuments%2F20151106-702Mem_Opinion_Order_for_Public_Release.pdf&t=MDM3MGZmYjY1ZWQ5YjUyMTQ5ZjQ1ZTA0ZDExNjY2NWU2TE1ZWJlNSxaRjRxYlRaQg%3D%3D.
73 Id. at 50.
74 Id. at 58.
76 Id. at 82.
77 Id. at 19 (internal quotation marks omitted).
The most notable recent compliance failure, discussed in the FISA Court’s April 26, 2017 opinion, is the NSA’s widespread use of U.S. person identifiers to query certain data obtained through upstream collection. The FISA Court had prohibited such queries in 2011, in response to its discovery that the NSA had for years been pulling in substantial numbers of wholly domestic communications by virtue of “about” collection. The Court had found the NSA’s handling of this data unconstitutional, and the ban on U.S. person queries of upstream data was one of the key remedies adopted to cure the constitutional defect.

In January 2016, however, the NSA Inspector General reported internally that agency analysts were not fully complying with this limitation, based on an examination of three months of audit data from early 2015. The Inspector General and the NSA’s Office of Compliance for Operations began studies of other time periods, and “preliminary results [suggested] the problem was widespread during all periods under review.”78 In other words, at no point during the operation of upstream collection – either in the years before the NSA informed the Court that it was sweeping in wholly domestic communications, or in the subsequent years when this data was supposedly off limits to U.S. person queries – had this surveillance operated within the bounds of the Constitution.

Nonetheless, the NSA waited for several months before informing the FISA Court of the problem, which it blamed on “human error” and “system design issues.”79 The Court chided the government for this “institutional lack of candor.”80 It granted short-term extensions of Section 702 surveillance authority while the government attempted to resolve the issue, but as of late January 2017, “[t]he government still had not ascertained the full range of systems that might have been used to conduct improper U.S.-person queries,”81 and as of March, “continued to . . . investigate potential root causes of non-compliant querying practices.”82 With no resolution in sight, and with the Court unwilling to certify the program for another year while the problem remained, the NSA made the only possible choice: to halt “about” collection for the time being.

The Court’s April 2017 opinion also includes a long list of other compliance failures. For instance, between November 2015 and May 2016, no less than 85 percent of queries using identifiers of U.S. persons targeted under Sections 704 and 705(b) resulted in improper querying of Section 702 data.83 The Court also found that the FBI had shared raw Section 702 information with a redacted entity “largely staffed by private contractors,” and that “the [redacted] contractors had access to raw FISA information that went well beyond what was necessary” to perform their jobs.84 And the Court noted that “[r]ecent disclosures regarding [redacted] systems maintained by the FBI suggest that raw FISA information, including Section 702 information,

---

78 Id. at 19.
79 Id. at 20.
80 Id. at 19.
81 Id. at 21.
82 Id. at 23.
83 Id. at 82.
84 Id. at 84.
may be retained on those systems in violation of applicable minimization requirements,” resulting in “indefinite retention” of some data.85

It is unclear whether these failures are occurring because the NSA is not putting sufficient effort into compliance, because the NSA lacks the technical capability to ensure compliance, or for some other reason. It may be the case that Section 702 collection has become so massive in scope, and the systems for retaining and processing the data so technically complex, that it is simply impossible to achieve consistent compliance with the rules governing its use. Whatever the explanation, the fact that the agency’s many failures to honor privacy protections were inadvertent is of limited comfort when the NSA is asking Congress and the American public to entrust it with extensive amounts of private data.

B. Chilling Effect

When Americans are aware that intelligence agencies are collecting large amounts of their data (and not just the data of suspected criminals and terrorists), it creates a measurable chilling effect on free expression and communication. After Edward Snowden’s revelations in June 2013, an analysis of Google Trends data showed a significant five percent drop in U.S.-based searches for government-sensitive terms (e.g., “dirty bomb” or “CIA”). A control list of popular search terms or other types of sensitive terms (such as “abortion”) did not show the same change.86 In 2013, PEN America surveyed 528 American writers to learn how the disclosures affected their behavior. Twenty-eight percent reported curtailing social media activities; 24 percent avoided certain topics by phone or email; 16 percent chose not to write or speak on a certain topic; and 16 percent avoided Internet searches or website visits on controversial or suspicious topics.87 These kinds of self-censorship are inimical to the robust exchange of ideas necessary for a healthy democracy.

The impact of overbroad surveillance has been particularly acute in Muslim American communities. According to one study, after the Associated Press reported on the New York City Police Department’s surveillance activities, Muslims reported a decline in mosque attendance and Muslim Student Association participation, as well as a marked reticence to speak about political matters in public places or to welcome newcomers into the community.88 Fear of surveillance, and the possibility that religious or political discussions could be misconstrued or misunderstood, has measurably impeded these communities’ ability to freely practice their faith or even to participate fully in civic life.

85 Id. at 87-89.
C. Risk of Data Theft

Any massive government database containing sensitive information about Americans also raises concerns about data theft. The disastrous 2015 attack on the Office of Personnel Management’s database, in which personal data concerning more than 21 million current and former federal employees was stolen (ostensibly by the Chinese government), illustrated how vulnerable government databases are.\(^8^9\) A few months later, hackers published contact information for 20,000 FBI employees and 10,000 Department of Homeland Security employees that they may have obtained by hacking into a Department of Justice database.\(^9^0\) The intelligence community’s data systems are not immune from being compromised, as evidenced by the theft of the NSA’s top-secret hacking tools in 2016,\(^9^1\) followed by WikiLeaks’ publication of the CIA’s hacking tools earlier this year.\(^9^2\)

The broad scope of Section 702 data, and the possibility that it could include a wealth of valuable foreign intelligence information, makes it an attractive target for hacking or data theft. Its inclusion of large amounts of information about presumptively innocent Americans significantly increases the harm that would be caused by such an event.

D. Economic Consequences

Another important concern is the negative impact of Section 702 collection on the U.S. technology industry. After Snowden’s disclosures revealed the extent of NSA collection, American technology companies reported declining sales overseas and lost business opportunities. In a survey of 300 British and Canadian businesses, 25 percent of respondents indicated they were moving their data outside of the U.S.\(^9^3\) An August 2013 study by the Information Technology and Innovation Foundation estimated that the revelations could cost the American cloud computing industry $22 to $35 billion over the coming years, representing a 10-20% loss of the foreign market share to European or Asian competitors.\(^9^4\) Another analyst found this estimate to be low, and predicted a loss to U.S. companies as high as $180 billion.\(^9^5\)

---

The economic news went from bad to worse in late 2015, when the Court of Justice of the European Union (CJEU) invalidated the “Safe Harbor” agreement – a 2000 decision of the European Commission allowing the transfer of personal data from the European Union (EU) to the United States, based on the premise that the U.S. met certain EU-law requirements about the handling of that information. The court held that EU law requires U.S. companies to give the data a level of protection that is essentially equivalent to the protections under EU law, including the Charter of Fundamental Rights of the EU – akin to an EU bill of rights. Under this standard, the court found that the European Commission had failed to ensure that EU citizens’ data was sufficiently protected within the U.S. While the court did not make express findings about Section 702, the law unquestionably loomed large in the court’s analysis, as the authority it confers is inconsistent with many of the essential rights and principles the court described. For instance, upstream surveillance is clearly implicated by the CJEU’s conclusion that “generalized” access to the content of electronic communications compromises the essence of the right to privacy.

Although the U.S. and the European Commission have devised a new arrangement, known as the “Privacy Shield,” legal challenges to that agreement are underway and recent developments have given a boost to these challenges. In particular, some of the protections U.S. officials had cited to assuage concerns about the breadth of Section 702 and other U.S. surveillance programs have been, or may soon be, eroded. The Privacy and Civil Liberties Oversight Board has lost its chairman and three other members, and is effectively dormant. A recent executive order issued by President Trump removes Privacy Act protections for foreigners. The current CIA director previously proposed revoking a directive issued by President Obama that extended some protections to foreigners’ data obtained under foreign intelligence programs.

In the absence of reforms to Section 702 and other surveillance authorities, it appears likely that the Privacy Shield will ultimately be invalidated by the CJEU or potentially even by the European Commission itself (which can suspend the arrangement unilaterally). Experts believe this would deal a massive economic blow to U.S. companies and could undermine the very structure of the Internet, which requires free data flow across borders. In the meantime, the legal limbo in which U.S. companies find themselves constrains their ability to pursue business opportunities in Europe. That is why over 30 leading technology companies, including

---

Microsoft, Google, and Facebook, recently signed a letter urging Congress to enact changes to Section 702. The reforms they propose include codifying the current prohibition against “about” collection and narrowing the definition of “foreign intelligence information” under FISA “to reduce the likelihood of collecting information about non-U.S. persons who are not suspected of wrongdoing.”

E. Potential National Security Harms

Last but clearly not least, there is a risk to national security in acquiring too much data. While computers can glean relationships and flag anomalies, they cannot replace human analysis, and human beings have limited capacity. When they are presented with an excess of data, real threats can get lost in the noise. This is not merely a theoretical concern. After the intelligence community failed to intercept the so-called “underwear bomber” (the suicide bomber who nearly brought down a plane headed to Detroit on Christmas Day 2009), an official White House review observed that a significant amount of critical information was available to the intelligence agencies but was “embedded in a large volume of other data.” Similarly, the independent investigation of the FBI’s role in the shootings by U.S. Army Major Nidal Hasan at Fort Hood concluded that the “crushing volume” of information was one of the factors that hampered accurate analysis prior to the attack.

Whatever threat information may exist amidst the 250 million Internet communications acquired yearly under Section 702, there is surely a large amount of chaff. Because this may make it more difficult to find the threats, it is important for lawmakers to examine whether the current scope of Section 702 collection may be too broad from a security standpoint as well as a privacy one.

IV. Constitutional Concerns

In addition to the practical risks and harms discussed above, the warrantless acquisition of millions of Americans’ communications presents deep Fourth Amendment concerns. The

---


102 Although a full discussion of this issue is beyond the scope of this testimony, Section 702 surveillance also raises concerns about the privacy and human rights of foreign nationals. While the Fourth Amendment might not apply to these individuals, the right to privacy is a fundamental human right recognized under international law— including treaties, such as the International Covenant on Civil and Political Rights, that the U.S. has signed. In Presidential Policy Directive 28 (PPD-28), President Obama acknowledged that “all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and . . . all persons have legitimate privacy.
communications obtained under Section 702, like any e-mails or phone calls, include not only mundane conversations, but the most private and personal confidences, as well as confidential business information and other kinds of privileged exchanges. Since the Supreme Court decided *Katz v. United States* in 1967, the government has been required to obtain a warrant to wiretap Americans’ communications. Moreover, in a subsequent case, the Court made clear that this requirement applied in domestic national security cases as well as criminal cases.

A. “Incidental” Collection

The government nonetheless justifies the warrantless collection of international communications under Section 702 on the ground that the targets themselves are foreigners overseas, and the Supreme Court has held (in a different context) that the government does not need a warrant to search the property of a non-U.S. person abroad. Although the communications obtained under Section 702 sometimes involve both foreigners and Americans, the FISA Court, along with federal courts in two circuits, have held that the authority to conduct warrantless surveillance of the foreign target entails the authority to “incidentally” collect the communications of those in contact with the target.

Outside of Section 702, however, the case law does not support the existence of a right to warrantless “incidental” collection. The courts reviewing Section 702 have relied on a line of cases dating back to the 1970s, sometimes called the “incidental overhear” cases, in which


PPD-28 requires agencies to extend certain privacy protections to foreign nationals when conducting electronic surveillance. However, the future viability of PPD-28 is uncertain, given that President Trump already has rescinded several of President Obama’s orders and CIA Director Mike Pompeo, when he served in Congress, argued that PPD-28 should be revoked. See Mike Pompeo & David B. Rivkin Jr., *Time for a Rigorous National Debate About Surveillance*, WALL ST. J. (Jan. 3, 2016), https://www.wsj.com/articles/time-for-a-rigorous-national-debate-about-surveillance-1451856106. Moreover, even if PPD-28 remains in place, it does not prevent the acquisition of information about foreign nationals who pose no threat to the United States.

A particular concern relates to the sharing of Section 702 information with foreign governments. Agencies have significant leeway to engage in such sharing. Although they should have “confidence” that the information “is not likely to be used by the recipient in an unlawful manner or in a manner harmful to U.S. interests,” OFFICE OF THE DIR. OF NAT’L INTELLIGENCE, CRITERIA FOR FOREIGN DISCLOSURE AND RELEASE OF CLASSIFIED NATIONAL INTELLIGENCE, ICPG 403.1 § (D)(2) (Mar. 13, 2013), there is no express requirement or mechanism to ensure that governments with poor or spotty human rights records will not use the information to facilitate human rights violations – for instance, to harass or persecute journalists, political dissidents, human rights activists, and other vulnerable groups whose communications may have been caught up in the Section 702 collection. See AMOS TOH, FAIZA PATEL & ELIZABETH GOITEIN, BRENNAH CTR. FOR JUSTICE, OVERSEAS SURVEILLANCE IN AN INTERCONNECTED WORLD 28-31 (2016), http://www.brennancenter.org/sites/default/files/publications/Overseas_Surveillance_in_an_Interconnected_World.pdf.

---

106 See United States v. Mohamud, 843 F.3d 420 (9th Cir. 2016); United States v. Hasbajrami, No. 11-CR-623 (JG), 2016 WL 1029500 (E.D.N.Y. Mar. 8, 2016); In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1015 (FISA Ct. Rev. 2008).
defendants challenged Title III wiretap orders on the ground that they did not name everyone whose communications might be recorded. The courts held that a warrant meets the Fourth Amendment’s “particularity” requirement as long it specifies the phone line to be tapped and the conversations to be acquired, and if the government takes reasonable steps to avoid recording “innocent” conversations. It is hard to see how these rulings on the criteria for a valid warrant could justify warrantless collection of Americans’ communications.

If, on the other hand, the courts reviewing Section 702 have correctly interpreted the rule emerging from the “incidental overhear” cases, then applying that rule in the Section 702 context would be a classic case of the law failing to keep up with technology. A blanket rule that no warrant is needed for Americans who are in contact with a lawfully surveilled target might have made sense in the 1970s, when there was almost certainly a warrant for the target himself (given the infrequency of international communication) and when government agents monitored the wiretap in real time so that they could turn off the recording equipment if “innocent conversations” were taking place. That rule does not sufficiently protect Americans’ reasonable expectation of privacy in an era where millions of Americans communicate with foreigners overseas on a routine basis, those communications can easily be intercepted in massive amounts without any warrant, and there is no mechanism for “turning off” the collection of “innocent communications.” Equating the incidental surveillance that takes place in these materially different contexts is like equating “a ride on horseback” with “a flight to the moon.”

B. The Foreign Intelligence Exception

Alternatively, the FISA Court (and, more recently, a district court following its lead) has relied on the “foreign intelligence exception” to the Fourth Amendment’s warrant requirement. The Supreme Court has never recognized this exception, and there is significant controversy over its scope. The FISA Court has construed the exception extremely broadly, stating that it applies even if the target is an American and even if the primary purpose of collection has no relation to foreign intelligence.

In the era before FISA, however, several federal courts of appeal had the opportunity to review foreign intelligence surveillance, and they articulated a much narrower version of the

---


108 See Elizabeth Goitein, The Ninth Circuit’s Constitutional Detour in Mohamud, JUST SEC. (Dec. 8, 2016), https://www.justsecurity.org/35411/ninth-circuits-constitutional-detour-mohamud/. The rulings are particularly inapt because Section 702 minimization procedures present little or no barrier to collection, and the back-end protections on retention and use are significantly weaker than those that apply in the Title III context. See Brief for Appellant at Argument I, In re Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002) (No. 02-001) (noting that “FISA’s minimization standards are more generous than those in Title III”).


111 See, e.g., In re Directives, 551 F.3d 1004; In re DNI/AG Certification [REDACTED], No. 702(i)-08-01 (FISA Ct. Sept. 4, 2008).
exception. They held that it applies only if the target is a foreign power or agent thereof, and only if the acquisition of foreign intelligence is the primary purpose of the surveillance. They also emphasized the importance of close judicial scrutiny (albeit after-the-fact) in cases where the target challenges the surveillance. While these cases addressed surveillance activities that differed in many respects from Section 702, it is clear that Section 702 surveillance would not pass constitutional muster under the standards they articulated.

A detailed analysis of the case law is beyond the scope of this testimony, but the Brennan Center’s report, *What Went Wrong With the FISA Court*, engages in such an analysis and explains why the foreign intelligence exception does not justify Section 702 surveillance in its current form.

C. The Reasonableness Test

Even if a foreign intelligence exception applied, the surveillance would still have to be “reasonable” under the Fourth Amendment. The “reasonableness” inquiry entails weighing the government’s interests against the intrusion on privacy.

In undertaking this analysis, courts generally accept that the government’s interest in protecting national security is of the highest order – as it certainly is. But to determine the reasonableness of a surveillance scheme, one must also ask whether it goes further than necessary to accomplish the desired end. For instance, how does it further national security to allow the targeting of foreigners who have no known or suspected affiliation with foreign governments, factions, or terrorist groups? How does it further national security to permit the FBI to search for Americans’ communications to use in prosecutions having nothing to do with national security?

Moreover, in assessing the impact on privacy rights, the FISA Court has focused on the protections offered to Americans by minimization procedures. As discussed above, however, these protections fall short in a number of significant respects. On their face, they allow Americans’ communications to be retained, disseminated, and used in a wide range of circumstances.

V. Reforming Section 702

There are several reforms that would go far toward mitigating the privacy risks posed by Section 702, while retaining the core functionality of the statute: the ability of the government to conduct warrantless surveillance of foreigners overseas who may pose a threat to the U.S. or its interests. These reforms would also retain the principle that communications between foreigners

---

113 GOITEIN & PATEL, *supra* note 2, at 11-12, 35-43.
115 *In re Directives*, 551 F.3d at 1015.
do not fall within FISA even if they happen to transit through or be stored within the U.S. And because they would not affect the government’s ability to collect the communications of suspected terrorists, there is no reason to believe that they would compromise Section 702’s effectiveness as a counterterrorism tool.

A. Narrowing the Scope of Collection

Congress should narrow the scope of permissible targets. Currently, the government may target anyone reasonably believed to be a foreigner overseas, as long as the purpose of collection is to acquire information “that relates to . . . the national defense or the security of the United States; or . . . the conduct of the foreign affairs of the United States.” 116 As discussed above, this language is permissive enough to allow surveillance of innocent conversations between foreigners and Americans about current events. If, in fact, the government does not condone or conduct such broad, non-threat-based surveillance, it should have no objection to statutory changes to codify a more narrow approach.

This could be accomplished through two measures. First, Congress should require the government to have a reasonable belief that the target of surveillance is a foreign power (FP) or an agent of a foreign power (AFP). The statute defines these terms quite broadly to include not only foreign governments or factions, but also private citizens who are suspected of involvement in international terrorism. The FP/AFP determination would be an internal one; it would not have to be submitted to the FISA Court for case-by-case approval or meet a “probable cause” standard. Second, Congress should narrow the permissible purposes of Section 702 surveillance so that it they are limited to protecting the U.S. against (1) actual or potential attacks or other grave hostile acts, including cyberattacks; (2) sabotage, international terrorism, or the international proliferation of weapons of mass destruction; or (3) clandestine intelligence activities. 117 It would not be sufficient that the information sought merely “relates to” the “conduct of foreign affairs.”

Limiting the scope of surveillance to those suspected of posing a threat to the U.S. would not undermine the statute’s effectiveness. The government has made public several examples of Section 702’s importance to its counterterrorism efforts; in each of these examples – including the cases of Najibullah Zazi, Khalid Ouazzani, David Headley, Agron Hasbajrami, and Jamshid Muhtorov – the targets of the Section 702 surveillance were known or suspected to have terrorist affiliations. 118 Intelligence officials have confirmed that this is the norm in cases where Section 702 surveillance has been critical – i.e., that the “typical” such case has involved “narrowly focused surveillance” targeting “a specific foreign individual overseas[,] based on the

government’s reasonable belief the individual was involved with terrorist activities.” The changes suggested here would not have prevented or limited Section 702 surveillance in those cases.

In addition, Congress should codify the current cessation of “about” collection. This type of surveillance greatly increases the chances of pulling in wholly domestic communications, not to mention other completely innocent communications between people who are not themselves permissible targets of surveillance. Moreover, although “about” collection poses uniquely significant risks to privacy, it is a relatively small part of the upstream program, which itself comprises less than one tenth of Section 702 collection. This is clearly a situation in which the privacy risks outweigh the benefits – a point the NSA effectively acknowledged when it stopped “about” collection in April.

B. Shoring Up Protections for Americans’ “Incidentally” Collected Communications

Narrowing the scope of surveillance will reduce the amount of “incidental” collection of Americans’ communications that can take place, but it will not and cannot eliminate “incidental” collection altogether. It is thus critical that Congress breathe life into its statutory command to agencies to “minimize” the retention, use, and sharing of Americans’ information acquired through Section 702 surveillance.

First, Congress should require all government agencies to obtain a warrant or an individualized FISA Court order before using U.S. person identifiers to query raw Section 702 data. This would close the loophole that currently allows the government to read Americans’ e-mails and listen to their phone calls without any factual predicate to suspect wrongdoing, let alone a warrant. What makes the warrantless surveillance lawful in the first instance is the government’s certification that it is targeting only foreigners. That representation becomes a semantic sleight of hand when the government simultaneously adopts procedures allowing it to search the data for particular Americans’ communications.

The FBI has pointed out that its databases contain information from multiple sources, and other agencies may also conduct federated searches that run against multiple data sets. In such cases, there is a simple way to implement a warrant requirement for just the Section 702 data. Such data is specially tagged to enable compliance with notification requirements as well as legal limitations on who may access it. Currently, if an FBI agent performs a query that returns Section 702 data, the agent is notified of its 702 status. The systems could instead be configured not to return Section 702 data at all, unless the agent enters a code certifying that one of two

119 See Olsen Statement, supra note 56, at 5.
121 See Statement, Nat’l Sec. Agency, NSA Stops Certain 702 “Upstream” Activities (Apr. 28, 2017), available at https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml ("NSA previously reported that, because of the limits of its current technology, it is unable to completely eliminate ‘about’ communications from its upstream 702 collection without also excluding some of the relevant communications directly ‘to or from’ its foreign intelligence targets. That limitation remains even today. Nonetheless, NSA has determined that in light of the factors noted, this change is a responsible and careful approach at this time.").
conditions is met: (1) the query term is associated with someone reasonably believed to be a
foreigner overseas, or (2) the government has obtained the required warrant or FISA Court order.

Some have suggested that agencies should be free to run U.S. person queries of Section
702 metadata, with heightened requirements in place only if the agency wishes to review content. Legal scholars and judges, however, have begun to recognize that metadata can be every bit as
revealing as content, enabling the government to piece together individuals’ beliefs, associations, habits, and other highly sensitive information.122 Even if one takes the position that metadata is
less deserving of protection, the Electronic Communications Privacy Act and Section 215 of the
USA PATRIOT Act still require the government to follow certain procedures and to meet certain
substantive standards in order to access Americans’ telephone and Internet metadata.123

Allowing unfettered access to metadata collected under Section 702 subverts those requirements,
just as allowing the unfettered review of content subverts the requirement of a warrant or FISA
Title I order.

Second, Congress should limit the permissible uses of Section 702 data about Americans,
even in cases where a warrant is obtained or the government comes across the information
without having performed a backdoor search. It is a basic tenet of privacy protection, enshrined
in the “widely accepted” Fair Information Practice Principles that are themselves “at the core of
the Privacy Act of 1974,” that the use of personal information should be limited to the purposes
for which it was collected.124 This principle has even more force when the government could not
legally have collected the information in the first place for reasons other than the stated purpose.
Obtaining evidence for use against Americans in legal proceedings unrelated to national security
or foreign intelligence is not a permissible purpose for collecting communications under Section
702. It therefore should not be a permissible use of those communications.

Third, Congress should add specificity to its definition of “minimization.” In the absence
of objective statutory criteria, there has been a predictable steady slide toward wider sharing of
raw data, greater access to the data by agency personnel, and more exceptions to retention limits.
On retention in particular, Congress should clarify that keeping Americans’ information for five
years, and for even longer in cases where that information has been reviewed and no
determination of its status has been made, is not “minimization.” Congress should specify that all
information not subject to a “litigation hold” shall be destroyed within three years of the
authorization for the acquisition, unless it has been reviewed and determined to be foreign
intelligence or evidence of a crime (where the use of that evidence would comply with applicable
use limitations).

122 See, e.g., Steven M. Bellovin, Matt Blaze, Susan Landau, & Stephanie K. Pell, It’s Too Complicated: How the
“[t]he application of traditional content/non-content distinctions leads to inconsistent and anomalous results”); Riley,
134 S. Ct. at 2490 (“Data on a cell phone can also reveal where a person has been. Historic location information is a
standard feature on many smart phones and can reconstruct someone’s specific movements down to the minute, not
only around town but also within a particular building.”).
124 Memorandum from Hugo Teufel III, Chief Privacy Officer, Dep’t of Homeland Sec., regarding The Fair
Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security (Dec. 29,
C. Increasing Transparency and Accountability

A range of other reforms would increase the transparency and accountability of Section 702 surveillance. For example, all agencies that are authorized to perform U.S. person queries, including the FBI, should be required to report how often they use U.S. person identifiers to query databases containing Section 702 data. This obligation should remain in place even if Congress enacts a warrant requirement for U.S. person queries. Lawmakers and the public need this information to understand and evaluate the impact on Americans of a surveillance authority that is nominally targeted at foreigners overseas.

Congress also should address the artificial barriers that are blocking legal challenges to Section 702 surveillance. Even though Congress clearly intended for defendants to be able to challenge the use of Section 702-derived evidence in criminal cases, the government’s notification policies are thwarting this intent. Congress should clarify that evidence is “derived” from Section 702 surveillance, for purposes of triggering the notification requirement, if the government would not otherwise have possessed this evidence. It should also specify that a person has standing to bring a civil lawsuit if she has a reasonable basis to believe her information has been (or will be) acquired, and if she has expended (or will expend) time or resources in an attempt to avoid acquisition.

An important caveat is in order. While reforms that promote transparency and accountability are critical, they are not a substitute for limiting the scope of Section 702 surveillance and shoring up privacy protections for Americans whose communications are “incidentally” collected. The most stringent of oversight provisions cannot justify amassing the personal data of ordinary, law-abiding private citizens. Nor can they legitimize the warrantless searching of Americans’ phone calls and e-mails. Procedural protections are only as good as the substantive rights and limitations they enforce. That is why Congress should reform Section 702 to bolster those rights and limitations while preserving the core of the statute: warrantless surveillance of foreigners who pose a threat to our nation.

Thank you again for this opportunity to testify.
Guide to Posted Documents Regarding Use of National Security Authorities – as of June 2017

Set forth below are links to certain officially released documents related to the use by the Intelligence Community (IC) of national security authorities. These documents have been published to meet legal requirements, as well as to carry out the Principles of Intelligence Transparency for the IC. Listed below are links to selected documents; there are many more officially released documents available for public review.

IC on the Record. IC on the Record (ICOTR) is an online platform maintained by the Office of the Director of National Intelligence (ODNI) to provide officially released information about the IC, focusing primarily on foreign intelligence surveillance activities. Hundreds of documents and thousands of pages have been posted on this platform.

- ICOTR Transparency Tracker: The ODNI’s Office of Civil Liberties, Privacy and Transparency maintains the ICOTR Transparency Tracker. This spreadsheet indexes the materials posted on IC on the Record, as well as relevant materials posted on other government sites.

General Overviews of Section 702 of the Foreign Intelligence Surveillance Act (FISA). The FISA Amendments Act – which includes Section 702 - will expire at the end of 2017 unless it is reauthorized by Congress. The government has provided general overviews of this critical national security authority:

- FISA Amendments Act: Q&A. The IC prepared a detailed Q&A document describing Section 702 and other provisions of the FISA Amendments Act. This document includes a discussion of the intelligence value of Section 702, with examples.

- Joint Unclassified Statement on Section 702. IC FISA experts testified about Section 702 before the House Judiciary Committee in March, 2017. The statement for the record provides a detailed overview of Section 702, and is posted here.

- IC Legal Reference Book. The text of FISA and other legal authorities relevant to the IC can be found in the IC Legal Reference Book, compiled by ODNI’s Office of the General Counsel.

Reports on Use of National Security Authorities. The government prepares a variety of reports detailing its use of national security authorities. These reports contain a wealth of information about how the government implements FISA and other key authorities.

- Annual Statistical Transparency Report Regarding Us of National Security Authorities. For the past four years, the ODNI has published on ICOTR annual reports that provide
important statistics on how national security authorities are used. The fourth such report, for calendar year 2016, is posted [here](#). This report includes statistics required by the USA FREEDOM Act, as well as other statistics published pursuant to the *Principles of Intelligence Transparency*.

- **Reports posted on the Privacy and Civil Liberties Oversight Board’s website** ([www.pclob.gov](http://www.pclob.gov)). The Privacy and Civil Liberties Oversight Board (PCLOB) is an independent, bipartisan agency within the executive branch. The PCLOB provides advice and oversight regarding efforts to protect the Nation from terrorism. The PCLOB has published major reports on the executive branch’s use of national security authorities.
  - PCLOB Report on the Surveillance Program Operated Pursuant to Section 702 of FISA (July 2, 2014).
  - PCLOB Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court (January 23, 2014).
  - PCLOB Update on the government’s implementation of the PCLOB Recommendations on Section 215 and Section 702 (February 5, 2016).

- **Reports posted on NSA’s Civil Liberties and Privacy Office (NSA CLPO) website** ([www.nsa.gov/about/civil-liberties](http://www.nsa.gov/about/civil-liberties)). NSA CLPO has, in the interest of transparency, prepared and published three reports describing how NSA implements key authorities, and assessing the corresponding civil liberties and privacy implications.
  - NSA CLPO Report on NSA’s implementation of Section 702.
  - NSA CLPO Transparency Report on NSA’s implementation of the new business records provisions of the USA FREEDOM Act.
  - NSA CLPO Report on civil liberties and privacy protections for targeted signals intelligence (SIGINT) activities under Executive Order 12333.

**Targeting, Minimization, and Compliance under Section 702 of FISA.** Section 702 allows for the targeting of (i) non-United States persons (ii) reasonably believed to be located abroad (iii) to acquire foreign intelligence information. To ensure that all three requirements are appropriately met, Section 702 requires targeting and minimization procedures that are reviewed and approved by the Foreign Intelligence Surveillance Court (FISC). Extensive measures are used to verify compliance with those procedures.

- **Targeting Procedures.** Targeting is effectuated by tasking communications facilities (such as telephone numbers and electronic communications accounts) to U.S. electronic communications service providers. For the first time, the government released redacted versions of targeting procedures.
  - 2016 NSA’s Section 702 Targeting Procedures dated March 30, 2017
  - 2016 FBI’s Section 702 Targeting Procedures dated September 26, 2016

- **Minimization Procedures.** Section 702 also requires minimization procedures to minimize and protect any non-public information of United States persons that may be
incidentally collected when appropriately targeting non-United States persons abroad for foreign intelligence information. The government has released several sets of minimization procedures for the past few years. The most recently released minimization procedures are set forth below.

- 2016 NSA’s Section 702 Minimization Procedures dated March 30, 2017
- 2016 FBI’s Section 702 Minimization Procedures dated September 26, 2016
- 2016 CIA’s Section 702 Minimization Procedures dated September 26, 2016
- 2016 NCTC’s Section 702 Minimization Procedures dated September 26, 2016

**Summary of Oversight Activities Conducted by DOJ and ODNI.** The National Security Division of the Department of Justice and the ODNI jointly conduct oversight of how the IC implements Section 702. These activities were officially described a filing with the FISC, which is posted [here](#).

**Semiannual Assessments of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of FISA.** Semiannual Compliance Assessments under Section 702 of FISA. These compliance assessments are jointly submitted by the Attorney General and the DNI. As of January 2017, fifteen joint assessments have been submitted. The 13th-15th Joint Assessments are posted [here](#), together with a corresponding Fact Sheet explaining joint assessments.

**Recently Posted Opinions of the Foreign Intelligence Surveillance Court (FISC) and the Foreign Intelligence Surveillance Court of Review (FISCR).** The FISC and FISCR carry out their judicial duties under FISA in a classified setting, so that they can receive and act on classified information relating to the government’s implementation of FISA authorities. Recently, a substantial number of filings, rulings, and other documents related to the FISC and FISCR have been made public, in redacted form.

- **FISC Website.** FISC rulings, filings and other documents can also be found on the FISC’s website: [http://www.fisc.uscourts.gov/](http://www.fisc.uscourts.gov/).

- **Recent Releases on ICOTR.**
  - [The FISC’s April 26, 2017 Memorandum Opinion and Order](#), addressing, among other things, the upstream compliance incident that is described by NSA [here](#).
  - [Over a dozen FISC opinions and related documents](#), recently released as part of FOIA litigation.
  - [Release of FISC Question of Law and FISCR Opinion](#), regarding collection of post-cut through digits using a pen register and trap and trace device.
  - [Release of three FISC opinions](#): June 18, 2015 Memorandum Opinion regarding appointment of amicus for a particular case; November 6, 2015 Memorandum Opinion and Order regarding the 2015 Section 702 Certifications; and December 31, 2015 Memorandum Opinion, approving the Government’s first application for orders requiring the production of call detail records under the USA FREEDOM Act.
Executive Order 12333. The IC has also released important documents related to Executive Order 12333, which establishes the Executive Branch framework for the country’s national intelligence efforts, and includes safeguards for protecting privacy and civil liberties in the conduct of intelligence activities. It was originally issued by President Ronald Reagan in 1981, was most recently revised and re-issued by President George W. Bush in 2008.

- General Documents. Executive Order 12333, as amended, is posted here. An information paper describing the 2008 revision is posted here.

- Attorney-General Approved Procedures. Section 2.3 of Executive Order 12333 provides that IC elements may collect, retain, and disseminate information concerning United States persons pursuant to procedures established by the head of the IC element and approved by the Attorney General, in consultation with the DNI.
  - DoD. The Department of Defense updated its Attorney General-approved procedures last year: Department of Defense Manual 5240.01, Procedures Governing the Conduct of DoD Intelligence Activities, with corresponding Fact Sheet. These procedures cover the IC elements that are part of DoD: DIA, NGA, NRO, NSA, and the intelligence elements of the Army, Navy, Air Force, and Marines.
  - NSA. In addition, NSA also follows United States Signals Directive (USSID) SP0018, Legal Compliance and U.S. Persons Minimization Procedures (January 25, 2011), commonly referred to as USSID 18.
  - CIA. The CIA updated its Attorney General approved procedures earlier this year: CIA’s Executive Order 12333, Attorney General Procedures, with corresponding Detailed Description.
  - Table. A table with links to IC elements’ procedures is posted here.

- Raw Signals Intelligence Availability Procedures. Section 2.3 of Executive Order 12333 also provides that raw or unminimized signals intelligence (SIGINT) information may only be disseminated or made available to Intelligence Community elements in accordance with procedures established by the DNI in coordination with the Secretary of Defense and approved by the Attorney General.
  - The Raw SIGINT Availability Procedures were finalized and released in January of this year, and are posted here, with corresponding Fact Sheet. The procedures require strict safeguards comparable to those applicable to the rigorous controls imposed by NSA for handling such information.

Presidential Policy Directive 28, Signals Intelligence Activities (PPD-28). PPD-28 was issued in January 2014 and remains in effect. It sets forth general privacy protection principles for SIGINT activities, limits the use of SIGINT collected in bulk, provides for the involvement of senior
policy makers in key SIGINT decisions, and imposes specific safeguards to protect the privacy of all individuals, regardless of nationality.

- **PPD-28.** PPD-28 is posted [here](#).

- **IC Element Policies Implementing PPD-28.** Section 4 of PPD-28 calls on each IC element to update existing or issue new policies and procedures to implement principles for safeguarding all personal information collected through SIGINT, consistent with technical capabilities and operational needs. A table with links to each IC element’s policies under PPD-28 is posted [here](#). In addition, links to two IC Standards relating to PPD-28 are posted [here](#).

- **Annual Signals Intelligence Reform Progress Report.** For the past three years, the ODNI has published an annual report outlining progress under PPD-28 and related SIGINT reform efforts. The report for calendar year 2016 is posted [here](#).
Introduction

In June 2014, the Director of National Intelligence (DNI) began releasing statistics relating to the use of critical national security authorities, including the Foreign Intelligence Surveillance Act (FISA), in an annual report called the Statistical Transparency Report Regarding Use of National Security Authorities (hereafter the Annual Statistical Transparency Report). Subsequent Annual Statistical Transparency Reports were released in 2015 and 2016.

On June 2, 2015, the USA FREEDOM Act was enacted, codifying a requirement to publicly report many of the statistics already reported in the Annual Statistical Transparency Report. The Act also expanded the scope of the information included in the reports by requiring the DNI to report information concerning United States person search terms and queries of certain FISA-acquired information, as well as specific statistics concerning information collected pursuant to call detail records. See 50 U.S.C. § 1873(b).

Today, consistent with the USA FREEDOM Act requirements to release certain statistics (codified in 50 U.S.C. § 1873(b)) and the Intelligence Community’s (IC) Principles of Intelligence Transparency, we are releasing our fourth Annual Statistical Transparency Report presenting statistics on how often the government uses certain national security authorities.

This fourth report has been reformatted to provide a description of the statistics being reported. Related definitions and additional context to the statistics included in this report are provided throughout. The order in which the statistics are presented remains consistent with last year’s report and follows the order set forth in 50 U.S.C. § 1873(b).

Additional public information on national security authorities is available at the Office of the Director of National Intelligence’s (ODNI) website, www.dni.gov, and ODNI’s public tumblr site, lContheRecord.tumblr.com.
FISA Title I -- Title III -- Title VII Sections 703 & 704

→ All of these authorities require individual court orders based on probable cause.

→ Titles I and III apply to FISA activities directed against persons within the United States.

→ Sections 703 and 704 apply to FISA activities directed against U.S. persons outside the United States.

Both FISA Title I and FISA Title III require a probable cause court order to target individuals within the United States regardless of U.S. person status. Under FISA, Title I permits electronic surveillance and Title III permits physical search in the United States of foreign powers or agents of a foreign power for the purpose of collecting foreign intelligence information. See 50 U.S.C. §§ 1804 and 1823. Title I (electronic surveillance) and Title III (physical search) are commonly referred to as “Traditional FISA.” Both require that the Foreign Intelligence Surveillance Court (FISC) make a probable cause finding, based upon a factual statement in the government’s application, that (i) the target is a foreign power or an agent of a foreign power, as defined by FISA and (ii) the facility being targeted for electronic surveillance is used by or about to be used, or the premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power. In addition to meeting the probable cause standard, the government’s application must meet the other requirements of FISA. See 50 U.S.C. §§ 1804(a) and 1823(a).

FISA Title VII Sections 703 and 704 similarly require a court order based on a finding of probable cause for the government to undertake FISA activities targeting U.S. persons located outside the United States. Section 703 applies when the government seeks to conduct electronic surveillance or to acquire stored electronic communications or stored electronic data, in a manner that otherwise requires an order pursuant to FISA, of a U.S. person who is reasonably believed to be located outside the United States. Section 704 applies when the government seeks to conduct collection overseas targeting a U.S. person reasonably believed to be located outside the United States under circumstances in which the U.S. person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted in the United States. Both Sections 703 and 704 require that the FISC make a probable cause finding, based upon a factual statement in the government’s application, that
the target is a U.S. person reasonably believed to be (i) located outside the United States and (ii) a foreign power, agent of a foreign power, or officer or employee of a foreign power; additionally, the government’s application must meet the other requirements of FISA. See 50 U.S.C. §§ 1881b(b) and 1881c(b).

- **U.S. Person.** As defined by Title I of FISA, a U.S. person is “a citizen of the United States or an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association with a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in [50 U.S.C. § 1801(a)(1), (2), or (3)].” 50 U.S.C. § 1801(i). Section 602 of the USA FREEDOM Act, however, uses a narrower definition. Since the broader Title I definition governs how U.S. person queries are conducted pursuant to the relevant minimization procedures, it will be used throughout this report.

- **Target.** Within the IC, the term “target” has multiple meanings. With respect to the statistics provided in this report, the term “target” is defined as the individual person, group, entity composed of multiple individuals, or foreign power that uses the selector such as a telephone number or email address.

**The role of the FISC.** If the FISC finds that the government’s application meets the requirements of FISA and the Constitution, the FISC must issue an order approving the requested authority.

- **Types of Orders.** There are different types of orders that the FISC may issue in connection with FISA cases, for example: orders granting or modifying the government’s authority to conduct intelligence collection; orders directing electronic communication service providers to provide any technical assistance necessary to implement the authorized intelligence collection; and supplemental orders and briefing orders requiring the government to take a particular action or provide the court with specific information.

- **Amendments and Renewals.** The FISC may amend an order one or more times after it has been issued. For example, an order may be amended to add a newly discovered account used by the target. This report does not count such amendments separately. The FISC may renew some orders multiple times during the calendar year. Each authority permitted under FISA has specific time limits for the FISA authority to continue (e.g., a Section 704 order against a U.S. person target may last no longer than 90 days.
but FISA permits the order to be renewed, see 50 U.S.C. § 1881c(c)(4)). Each renewal requires a separate application submitted by the government to the FISC and a finding by the FISC that the application meets the requirements of FISA. Thus, unlike amendments, this report does count each such renewal as a separate order. These terms will be used consistently throughout this report.

**FISA “Probable Cause” Court Orders and Targets**

<table>
<thead>
<tr>
<th>Titles I and III and Sections 703 and 704 of FISA</th>
<th>CY2013</th>
<th>CY2014</th>
<th>CY2015</th>
<th>CY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of orders</td>
<td>1,767</td>
<td>1,519</td>
<td>1,585</td>
<td><strong>1,559</strong></td>
</tr>
<tr>
<td>Estimated* number of targets of such orders</td>
<td>1,144</td>
<td>1,562</td>
<td>1,695</td>
<td><strong>1,687</strong></td>
</tr>
</tbody>
</table>


*Throughout this report, when numbers are estimated, the estimate comports with the statutory requirements to provide a “good faith estimate” of a particular number.

**How targets are counted.** If the IC received authorization to conduct electronic surveillance and/or physical search against the same target in four separate applications, the IC would count one target, not four. Alternatively, if the IC received authorization to conduct electronic surveillance and/or physical search against four targets in the same application, the IC would count four targets. Duplicate targets across authorities are not counted.

**FISA “Probable Cause” Targets – U.S. Persons**

<table>
<thead>
<tr>
<th>Titles I and III and Sections 703 and 704 -- Targets</th>
<th>CY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Estimated number of targets who are non-U.S. persons</td>
<td><strong>1,351</strong></td>
</tr>
<tr>
<td>Estimated number of targets who are U.S. persons</td>
<td><strong>336</strong></td>
</tr>
<tr>
<td>Estimated percentage of targets who are U.S. persons</td>
<td><strong>19.9%</strong></td>
</tr>
</tbody>
</table>

*While not statutorily required to publicly provide these statistics, the IC is providing them consistent with the commitment to its Principles of Intelligence Transparency.*
Section 702. Title VII of FISA includes Section 702, which permits the Attorney General and the DNI to jointly authorize the targeting of (i) non-U.S. persons reasonably believed to be (ii) located outside the United States to (iii) acquire foreign intelligence information. See 50 U.S.C. § 1881a. All three elements must be met. Additionally, Section 702 requires that the Attorney General, in consultation with the DNI, adopt targeting procedures and minimization procedures that they attest satisfy the statutory requirements and are consistent with the Fourth Amendment.

- **Section 702 Targets and “Tasking.”** Under Section 702, the government “targets” a particular non-U.S. person, group, or entity reasonably believed to be located outside the United States and who possesses, or who is likely to communicate or receive, foreign intelligence information, by directing an acquisition at – i.e., “tasking” – selectors (e.g., telephone numbers and email addresses) that are assessed to be used by such non-U.S. person, group, or entity, pursuant to targeting procedures approved by the FISC.

Before “tasking” a selector for collection under Section 702, the government must apply its targeting procedures to ensure that the IC appropriately tasks a selector used by a non-U.S. person who is reasonably believed to be located outside the United States and who will likely possess, communicate, or receive foreign intelligence information.

The FISC’s role. Under Section 702, the FISC determines whether certifications provided jointly by the Attorney General and the DNI appropriately meet all the requirements of Section 702. If the FISC determines that the government’s certifications and its targeting and minimization procedures meet the statutory requirements of Section 702 and are consistent with the Fourth Amendment, then the FISC issues an order and supporting statement approving the certifications. A recent FISC order and statement approving certifications was publicly released in April 2016 and posted on IC on the Record.
- **Certifications.** The certifications are jointly executed by the Attorney General and DNI and authorize the government to acquire foreign intelligence information under Section 702. Each annual certification application package must be submitted to the FISC for approval. The package includes the Attorney General and DNI’s certifications, affidavits by certain heads of intelligence agencies, targeting procedures, and minimization procedures. A sample of a certification application package was publicly released on *IC on the Record*. The certifications identify categories of information to be collected, which must meet the statutory definition of foreign intelligence information, through the targeting of non-U.S. persons reasonably believed to be located outside the United States. The certifications have included information concerning international terrorism and other topics, such as the acquisition of information concerning weapons of mass destruction.

- **Targeting procedures.** The targeting procedures detail the steps that the government must take before tasking a selector, as well as verification steps after tasking, to ensure that the user of the tasked selector is being targeted appropriately – specifically, that the user is a non-U.S. person, located outside the United States, who is being tasked to acquire foreign intelligence information. The IC must make individual determinations that each tasked selector meets the requirements of the targeting procedures. As part of the certification package, the FISC reviews the sufficiency of the IC’s targeting procedures, which includes assessing the IC’s compliance with the procedures.

- **Minimization procedures.** The minimization procedures detail requirements the government must meet to use, retain, and disseminate Section 702 data, which include specific restrictions on how the IC handles non-publicly available U.S. person information acquired from Section 702 collection of non-U.S. person targets, consistent with the needs of the government to obtain, produce, and disseminate foreign intelligence information. As part of the certification package, the FISC reviews the sufficiency of the IC’s minimization procedures, which includes assessing the IC’s compliance with past procedures. The 2015 minimization procedures have been released on *IC on the Record*.

The IC’s adherence to the targeting and minimization procedures is subject to robust internal agency oversight and to rigorous external oversight by the Department of Justice (DOJ), ODNI, Congress, and the FISC. Every identified incidence of non-compliance is reported to the FISC (through individual notices or in reports) and to Congress in semiannual reports. DOJ and ODNI also submit semiannual reports to Congress that assess the IC’s overall compliance efforts. Past assessments have been publicly released.
Section 702 Orders

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of orders issued</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>


Counting Section 702 orders. As explained above, the FISC may issue a single order to approve more than one Section 702 certification to acquire foreign intelligence information.

Note that, in its own transparency report, which is required pursuant to 50 U.S.C. § 1873(a), the Director of the Administrative Office of the United States Courts (AOUSC) counted each of the Section 702 certifications associated with the FISC’s order. Because the number of the government’s Section 702 certifications remains a classified fact, the government requested that the AOUSC redact the number of certifications from its transparency report prior to publicly releasing it.

In 2016, the government submitted a certification application to the FISC. Pursuant to 50 U.S.C. § 1881a(j)(2), the FISC extended its review of the 2016 certifications. The FISC may extend its review of the certifications “as necessary for good cause in a manner consistent with national security.” See 50 U.S.C. § 1881a(j)(2). Thus, because the FISC did not complete its review of the 2016 certifications during calendar year 2016, the FISC did not issue an order concerning those certifications in calendar year 2016. The 2015 order remained in effect during the extension period.

Section 702 Targets*

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Estimated number of targets of such orders</td>
<td>89,138</td>
<td>92,707</td>
<td>94,368</td>
<td>106,469</td>
</tr>
</tbody>
</table>

*While there is no statutory requirement to disclose this number, it is provided in this report to foster public understanding of the IC’s use of the Section 702 collection authority. The IC is committed to sharing as much information as possible with the public without jeopardizing mission capabilities.

Estimating Section 702 targets. The number of 702 “targets,” provided above, reflects an estimate of the number of non-United States persons who are the users of tasked selectors. This estimate is based on information readily available to the IC. Unless and until the IC has information that links multiple selectors to a single foreign intelligence target, each individual
selector is counted as a separate target for purposes of this report. On the other hand, where the IC is aware that multiple selectors are used by the same target, the IC counts the user of those selectors as a single target. This counting methodology reduces the risk that the IC might inadvertently understate the number of discrete persons targeted pursuant to Section 702.

Section 702 Search Terms Used to Query Content

<table>
<thead>
<tr>
<th>Section 702 of FISA</th>
<th>CY2015</th>
<th>CY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Estimated number of search terms concerning a known U.S. person used to retrieve the unminimized contents of communications obtained under Section 702 (excluding search terms used to prevent the return of U.S. person information)*</td>
<td>4,672</td>
<td>5,288</td>
</tr>
</tbody>
</table>


*Consistent with § 1873(d)(2)(A), this statistic does not include queries that are conducted by the Federal Bureau of Investigation (FBI).

The above is the good faith estimate of the number of search terms (e.g., email addresses and telephone numbers,) concerning known U.S. persons that the government used to query unminimized (i.e., raw) lawfully acquired Section 702 content.

Counting U.S. person search terms used to query Section 702 content. The National Security Agency (NSA) counts the number of U.S. person identifiers it uses to query the content of unminimized Section 702-acquired information. For example, if the NSA used U.S. person identifier “johndoe@XYXprovider” to query the content of Section 702-acquired information, the NSA would count it as one regardless of how many times the NSA used “johndoe@XYXprovider” to query its 702-acquired information. In calendar year 2016, the Central Intelligence Agency (CIA) adopted this same model for counting search terms. In prior calendar years, however, the CIA counted the total number of actual queries it conducted using U.S. person identifiers. For example, if the CIA used the identifier “johndoe@XYXprovider” 7 times, in prior years the CIA would count this as 7 search terms. Now, CIA the counts this as a single search term.
Section 702 Queries of Noncontents

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Estimated number of queries concerning a known U.S. person of unminimized noncontents information obtained under Section 702 (excluding queries containing information used to prevent the return of U.S. person information)*</td>
<td>9500</td>
<td>17,500</td>
<td>23,800</td>
<td>30,355</td>
</tr>
</tbody>
</table>


*Consistent with § 1873(d)(2)(A), this statistic does not include queries that are conducted by the FBI.

The above is a good faith estimate of the number of queries concerning a known U.S. person that the government conducted of unminimized (i.e., raw) lawfully acquired Section 702 metadata.

Counting queries using U.S. person identifiers of noncontents collected under Section 702.

This estimate represents the number of times a U.S. person identifier is used to query the noncontents (i.e., metadata) of unminimized Section 702-acquired information. For example, if the U.S. person identifier telephone number “111-111-2222” was used 15 times to query the noncontents of Section 702-acquired information, the number of queries counted would be 15.

As with last year’s transparency report, one IC element remains currently unable to provide the number of queries using U.S. person identifiers of unminimized Section 702 noncontent information. Under 50 U.S.C. § 1873(d)(3)(A), if the DNI concludes that this good-faith estimate cannot be determined accurately because not all of the relevant elements of the IC are able to provide this good faith estimate, then the DNI is required to (i) certify that conclusion in writing to the relevant Congressional committees; (ii) report the good faith estimate for those relevant elements able to provide such good faith estimate; (iii) explain when it is reasonably anticipated that such an estimate will be able to be determined fully and accurately; and (iv) make such certification publicly available on an Internet web site. Because one IC element remains unable to provide such information, the DNI made a certification, pursuant to § 1873(d)(3)(A) to the relevant Congressional committees.

As required by statute, this certification is being made publicly available as an attached appendix to this current report (see Appendix A).
Required Section 702 Query Reporting to the FISC

Per the FISC Memorandum Opinion and Order dated November 6, 2015: Each instance in which FBI personnel received and reviewed Section 702-acquired information that the FBI identified as concerning a U.S. person in response to a query that was designed to return evidence of a crime unrelated to foreign intelligence.

<table>
<thead>
<tr>
<th>Section 702 of FISA</th>
<th>CY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Per the FISC Memorandum Opinion and Order dated November 6, 2015: Each instance</td>
<td>1</td>
</tr>
<tr>
<td>in which FBI personnel received and reviewed Section 702-acquired information that</td>
<td></td>
</tr>
<tr>
<td>the FBI identified as concerning a U.S. person in response to a query that was</td>
<td></td>
</tr>
<tr>
<td>designed to return evidence of a crime unrelated to foreign intelligence.</td>
<td></td>
</tr>
</tbody>
</table>

On November 6, 2015, the FISC granted the government’s application for renewal of the 2015 certifications and, among other things, concluded that the FBI’s U.S. person querying provisions in its minimization procedures, “strike a reasonable balance between the privacy interests of the United States persons and persons in the United States, on the one hand, and the government’s national security interests, on the other.” Memorandum Opinion and Order dated November 6, 2015, at 44 (released on IC on the Record on April 19, 2016). The FISC further stated that the FBI conducting queries, “designed to return evidence of crimes unrelated to foreign intelligence does not preclude the Court from concluding that taken together, the targeting and minimization procedures submitted with the 2015 Certifications are consistent with the requirements of the Fourth Amendment.” Id.

Nevertheless, the FISC ordered the government to report in writing, “each instance after December 4, 2015, in which FBI personnel receive and review Section 702-acquired information that the FBI identifies as concerning a United States person in response to a query that is not designed to find and extract foreign intelligence information.” (Emphasis added). Id. at 44 and 78. The FISC directed that the report contain details of the query terms, the basis for conducting the query, the manner in which the query will be or has been used, and other details. Id. at 78. In keeping with the IC’s Principles of Transparency, the DNI declassified the number of each instance such queries occurred in calendar year 2016.
In July 2014, the Privacy and Civil Liberties Oversight Board (PCLOB or Board) issued a report on Section 702 entitled, “Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act” (PCLOB’s Section 702 Report), which contained 10 recommendations. Recommendation 9 focused on “accountability and transparency,” noting that the government should implement measures, “to provide insight about the extent to which the NSA acquires and utilizes the communications involving U.S. persons and people located in the United States under the Section 702 program.” PCLOB’s Section 702 Report at 145-146. Specifically, the PCLOB recommended that “the NSA should implement processes to annually count […] (5) the number of instances in which the NSA disseminates non-public information about U.S. persons, specifically distinguishing disseminations that includes names, titles, or other identifiers potentially associated with individuals.” Id. at 146. This recommendation is commonly referred to as Recommendation 9(5). In response to Recommendation 9(5), NSA previously publicly provided (in the Annual Statistical Transparency Report for calendar year 2015) and continues to provide the following additional information regarding the dissemination of Section 702 intelligence reports that contain U.S. person information.

NSA has been providing similar information to Congress per FISA reporting requirements. For example, FISA Section 702(l)(3) requires that NSA annually submit a report to applicable Congressional committees regarding certain numbers pertaining to the acquisition of Section 702-acquired information, including the number of “disseminated intelligence reports containing a reference to a United States person identity.” See 50 U.S.C. § 1881(l)(3)(A)(i). Additionally, NSA provides this number to Congress as part of Attorney General and Director of National Intelligence’s joint assessment of compliance. See 50 U.S.C. § 1881(l)(1).

Prior to the PCLOB issuing its Section 702 Report, NSA’s Director of Civil Liberties and Privacy Office published NSA’s Implementation of Foreign Intelligence Surveillance Act Section 702,” on April 16, 2014, (hereinafter “NSA DCLPO Report”), in which it explained NSA’s dissemination processes. NSA DCLPO Report at 7-8. NSA “only generates classified intelligence reports when the information meets a specific intelligence requirement, regardless of whether the proposed report contains U.S. person information.” NSA DCLPO Report at 7.
Dissemination. In the most basic sense, dissemination refers to the sharing of minimized information. As it pertains to FISA (including Section 702), if an agency (in this instance NSA) lawfully collects information pursuant to FISA and wants to share (i.e., disseminate) that information, the agency must first apply its minimization procedures to that information.

Section 702 only permits the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information. Such targets, however, may communicate information to, from, or about U.S. persons. NSA minimization procedures (publicly released on August 11, 2016) permit the NSA to disseminate U.S person information if the NSA masks the information that could identify the U.S. person. The minimization procedures permit NSA to disseminate the U.S. person identity only if doing so meets one of the specified reasons listed in NSA’s minimization procedures, including that the U.S. person consented to the dissemination, the U.S. person information was already publicly available, the U.S. person identity was necessary to understand foreign intelligence information, or the communication contained evidence of a crime and is being disseminated to law enforcement authorities. Even if one these conditions applies, as a matter of policy, NSA may still mask the U.S. person information and will include no more than the minimum amount of U.S. person information necessary to understand the foreign intelligence or to describe the crime or threat. Id. In certain instances, however, NSA makes a determination prior to releasing its original classified report that the U.S. person’s identity is appropriate to disseminate in the first instance using the same standards discussed above.

Masked U.S. Person Information. Information about a U.S. person is masked when the identifying information about the person is not included in a report. For example, instead of reporting that Section 702-acquired information revealed that non-U.S. person “Bad Guy” communicated with U.S. person “John Doe” (i.e., the actual name of the U.S. person), the report would mask “John Doe’s” identity, and would state that “Bad Guy” communicated with “an identified U.S. person,” “a named U.S. person,” or “a U.S. person.”

Recipients of NSA’s classified reports, such as other Federal agencies, may request that NSA provide the true identity of a masked U.S. person referenced in an intelligence report. The requested identity information is released only if the requesting recipient has a legitimate “need to know” the identity of the U.S. person and has the appropriate security clearances, and if the dissemination of the U.S. person’s identity would be consistent with NSA’s minimization procedures (e.g., the identity is necessary to understand foreign intelligence information or assess its importance). Furthermore, per NSA policy, NSA is allowed to unmask the identity for
the specific requesting recipient only where specific additional controls are in place to preclude its further dissemination and additional approval has been provided by a designated NSA official.

As part of their regular oversight reviews, DOJ and ODNI review disseminations of information about U.S. persons that NSA obtained pursuant to Section 702 to ensure that the disseminations were performed in compliance with the minimization procedures.

<table>
<thead>
<tr>
<th>Section 702 – U.S. person (USP) information disseminated by NSA</th>
<th>CY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of NSA disseminated §702 Reports containing USP identities</td>
<td>3,914</td>
</tr>
<tr>
<td>Of those NSA disseminated §702 Reports containing USP identities (from the first row in this chart), the USP identity was originally masked in this many reports</td>
<td>2,964*</td>
</tr>
<tr>
<td>Of those NSA disseminated §702 Reports containing USP identities (from the first row in this chart), the USP identity was originally revealed in this many reports</td>
<td>1,200*</td>
</tr>
<tr>
<td>Of those NSA disseminated §702 Reports containing USP identities where the USP identities was originally masked (from the second row in this chart), the number of USP identities that NSA later released in response to specific requests to unmask a USP identity**</td>
<td>1,934</td>
</tr>
</tbody>
</table>

*A single report may contain both masked and unmasked U.S. person identities.

**For this statistic, last year’s Annual Statistical Transparency Report provided the number of approved requests (i.e., 654) for unmasking of U.S. person identities, rather than the number of U.S. person identities that were released. A single request may contain multiple U.S. person identities. This year’s report provides the number of U.S. person identities referred to by name or title released in response to specific requests to unmask those identities. The number of U.S. person identities that NSA released during calendar year 2015 in response to specific requests to unmask an identity was 2,232, which was the number that should have been reported in last year’s report.
FISA Title IV – USE of PEN REGISTER and TRAP and TRACE (PR/TT) DEVICES

Commonly referred to as the “PR/TT” provision.

Bulk collection is prohibited.

Requires individual FISC order to use PR/TT device to capture dialing, routing, addressing, or signaling (DRAS) information.

Government request to use a PR/TT device on U.S. person target must be based on an investigation to protect against terrorism or clandestine intelligence activities and that investigation must not be based solely on the basis of activities protected by the First Amendment to the Constitution.

Pen Register/Trap and Trace Authority. Title IV of FISA authorizes the use of pen register and trap and trace (PR/TT) devices for foreign intelligence purposes. Title IV authorizes the government to use a PR/TT device to seek and capture dialing, routing, addressing or signaling (DRAS) information. The government may submit an application to the FISC for an order approving use of a PR/TT device (i.e., PR/TT order) for (i) “any investigation to obtain foreign intelligence information not concerning a United States person or” (ii) “to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a U.S. person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.” 50 U.S.C. § 1842(a). If the FISC finds that the government’s application sufficiently meets the requirements of FISA, the FISC must issue an order for the installation and use of a PR/TT device.
### PR/TT Statistics

<table>
<thead>
<tr>
<th>Total number of orders</th>
<th>CY2013</th>
<th>CY2014</th>
<th>CY2015</th>
<th>CY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>131</td>
<td>135</td>
<td>90</td>
<td>60</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Estimated number of targets of such orders</th>
<th>CY2013</th>
<th>CY2014</th>
<th>CY2015</th>
<th>CY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>319</td>
<td>516</td>
<td>456</td>
<td>41</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Estimated number of unique identifiers used to communicate information collected pursuant to such orders*</th>
<th>CY2013</th>
<th>CY2014</th>
<th>CY2015</th>
<th>CY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>-</td>
<td>-</td>
<td>134,987**</td>
<td>125,378</td>
</tr>
</tbody>
</table>

*Pursuant to §1873(d)(2)(B), this statistic does not apply to orders resulting in the acquisition of information by the FBI that does not include electronic mail addresses or telephone numbers.

**This number represents information the government received from provider(s) electronically for the entire 2015 calendar year. The government does not have a process for capturing unique identifiers received by other means (such as hard-copy or portable media).


---

**Counting orders.** Similar to how orders were counted for Titles I and III and Sections 703 and 704, this report only counts the orders granting authority to conduct intelligence collection -- the order for the installation and use of a PR/TT device. Thus, renewal orders are counted as a separate order; modification orders and amendments are not counted.

**Estimating the number of targets.** The government’s methodology for counting PR/TT targets is similar to the methodology described above for counting targets of electronic surveillance and/or physical search. If the IC received authorization for the installation and use of a PR/TT device against the same target in four separate applications, the IC would count one target, not four. Alternatively, if the IC received authorization for the installation and use of a PR/TT device against four targets in the same application, the IC would count four targets.

**Estimating the number of unique identifiers.** This statistic counts (1) the targeted identifiers and (2) the non-targeted identifiers (e.g., telephone numbers and e-mail addresses) that were in contact with the targeted identifiers. Specifically, the House Report on the USA FREEDOM Act states that "[t]he phrase 'unique identifiers used to communicate information collected pursuant to such orders' means the total number of, for example, email addresses or phone numbers that have been collected as a result of these particular types of FISA orders--not just
the number of target email addresses or phone numbers." [H.R. Rept. 114-109 Part I, p. 26], with certain exceptions noted.

### FISA PR/TT Targets – U.S. Persons*

<table>
<thead>
<tr>
<th>PR/TT Targets</th>
<th>CY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Estimated number of targets who are non-U.S. persons</td>
<td>23</td>
</tr>
<tr>
<td>Estimated number of targets who are U.S. persons</td>
<td>18</td>
</tr>
<tr>
<td>Estimated percentage of targets who are U.S. persons</td>
<td>43.9%</td>
</tr>
</tbody>
</table>

*While not statutorily required to publicly provide these statistics, the IC is providing them consistent with the Principles of Intelligence Transparency.

*The remainder of this page is intentionally left blank.*
FISA Title V – BUSINESS RECORDS

- Commonly referred to as “Business Records” provision.
- Bulk collection is prohibited.
- Call Detail Records (CDR) may be obtained from a telephone company if the FISC issues an individual court order for target’s records.
- Request for records in an investigation of a U.S. person must be based on an investigation to protect against terrorism or clandestine intelligence activities and provided that the investigation is not conducted solely upon activities protected by the First Amendment to the Constitution.

Business Records FISA. Under FISA, Title V authorizes the government to submit an application for an order requiring the production of any tangible things for (i) “an investigation to obtain foreign intelligence information not concerning a U.S. person or” (ii) “to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a U.S. person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.” 50 U.S.C. § 1861. Title V is commonly referred to as the “Business Records” provision of FISA.

In June 2015, the USA FREEDOM Act was signed into law and, among other things, amended Title V, including prohibiting bulk collection. See 50 U.S.C. §§ 1861(b), 1861(k)(4). The DNI is required to report various statistics about two Title V provisions – traditional business records and call detail records (discussed further below).

On November 28, 2015, in compliance with amendments enacted by the USA FREEDOM Act, the IC terminated collection of bulk telephony metadata under Title V of the FISA (the “Section 215 Program”). Solely due to legal obligations to preserve records in certain pending civil litigation, including First Unitarian Church of Los Angeles, et al. v. National Security Agency, et al., No. C 13-03287-JSW (N.D. Cal.) and Jewel, et al. v. National Security Agency, et al., No. C 08-04373-JSW (N.D. Cal.), the IC continues to preserve previously collected bulk telephony metadata. Under the terms of a FISC order dated November 24, 2015, the bulk telephony metadata cannot be used or accessed for any purpose other than compliance with preservation obligations. Once the government’s preservation obligations are lifted, the government is
required to promptly destroy all bulk metadata produced by telecommunications providers under the Section 215 Program.

As noted in last year’s Annual Statistical Transparency Report, on November 30, 2015, the IC implemented certain provisions of the USA FREEDOM Act, including the call detail records provision and the requirement to use a specific selection term. Accordingly, only one month’s worth of data for calendar year 2015 was available with respect to those provisions. Any statistical information relating to a particular FISA authority for a particular month remains classified. Therefore, the Title V data specifically associated with December 2015 was only released in a classified annex provided to Congress as part of the report for CY2015. For this CY 2016 report, statistical information was collected for an entire year under the USA FREEDOM Act Title V provisions. As a result, those statistics are included in this report.

Statistics related to traditional business records under Title V Section 501(b)(2)(B) are provided first pursuant to 50 U.S.C. § 1873(b)(4). Statistics related to call detail records under Title V Section 501(b)(2)(C) are provided second pursuant to 50 U.S.C. § 1873(b)(5).

“Traditional” Business Records – Section 501(b)(2)(B)

Business Record (BR) requests for tangible things include books, records, papers, documents, and other items pursuant to 50 U.S.C. §1861(b)(2)(B), also referred to as Section 501(b)(2)(B). These are commonly referred to as “Traditional” Business Records.

“Traditional” Business Records Statistics

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of orders issued pursuant to applications under Section 501(b)(2)(B)</td>
<td>84</td>
</tr>
<tr>
<td>Estimated number of targets of such orders</td>
<td>88</td>
</tr>
<tr>
<td>Estimated number of unique identifiers used to communicate information collected pursuant to such orders</td>
<td>81,035</td>
</tr>
</tbody>
</table>


**Estimating the number of unique identifiers.** This is an estimate of the number of (1) targeted identifiers (e.g., telephone numbers and email addresses) and (2) non-targeted identifiers that were in contact with the targeted identifiers. This metric represents unique identifiers received
electronically from the provider(s). The government does not have a process for capturing unique identifiers received by other means (i.e., hard-copy or portable media).

**Explaining how we count BR statistics.** As an example of the government’s methodology, assume that in 2016, the government submitted a BR request targeting “John Doe” with email addresses john.doe@serviceproviderX, john.doe@serviceproviderY, and john.doe@serviceproviderZ. The FISC found that the application met the requirements of Title V and issued orders granting the application and directing service providers X, Y, and Z to produce business records pursuant to Section 501(b)(2)(B). Provider X returned 10 non-targeted email addresses that were in contact with the target; provider Y returned 10 non-targeted email addresses that were in contact with the target; and provider Z returned 10 non-targeted email addresses that were in contact with the target. Based on this scenario, we would report the following statistics: A) one order by the FISC for the production of tangible things, B) one target of said orders, and C) 33 unique identifiers, representing three targeted email addresses plus 30 non-targeted email addresses.

---

**Call Detail Records – Section 501(b)(2)(C)**

Call Detail Records (CDR) – commonly referred to as “call event metadata” – may be obtained from telecommunications providers pursuant to 50 U.S.C. §1861(b)(2)(C). A CDR is defined as session identifying information (including an originating or terminating telephone number, an International Mobile Subscriber Identity (IMSI) number, or an International Mobile Station Equipment Identity (IMEI) number), a telephone calling card number, or the time or duration of a call. See 50 U.S.C. §1861(k)(3)(A). CDRs do not include the content of any communication, the name, address, or financial information of a subscriber or customer, or cell site location or global positioning system information. See 50 U.S.C. §1861(k)(3)(B). CDRs are stored and queried by the service providers. See 50 U.S.C. §1861(c)(2).

**Call Detail Record (CDR) Statistics**

<table>
<thead>
<tr>
<th>Call Detail Records “CDR” – Section 501(b)(2)(C)</th>
<th>CY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of orders issued pursuant to applications under Section 501(b)(2)(C)</td>
<td>40</td>
</tr>
<tr>
<td>Estimated number of targets of such orders</td>
<td>42</td>
</tr>
</tbody>
</table>

See 50 U.S.C. §§ 1873(b)(5) and 1873(b)(5)(A).
Estimating the number of targets of CDR orders. A “target” is the person using the selector. For example, if a target uses four selectors that have been approved, the number counted for purposes of this report would be one target, not four. Alternatively, if two targets are using one selector that has been approved, the number counted would be two targets.

The estimated number of Call Detail Records received from providers. This metric represents the number of records received from the provider(s) and stored in NSA repositories (records that fail at any of a variety of validation steps are not included in this number). CDRs covered by § 501(b)(2)(C) include call detail records created before, on, or after the date of the application relating to an authorized investigation. While the USA FREEDOM Act directs the government to provide a good faith estimate of “the number of unique identifiers used to communicate information collected pursuant to” orders issued in response to CDR applications (see § 1873(b)(5)(B)), the statistic below does not reflect the number of unique identifiers contained within the call detail records received from the providers. As of the date of this report, the government does not have the technical ability to isolate the number of unique identifiers within records received from the providers. As explained in the 2016 NSA’s public report on the USA FREEDOM Act, the metric provided is over-inclusive because the government counts each record separately even if the government receives the same record multiple times (whether from one provider or multiple providers). Additionally, this metric includes duplicates of unique identifiers – i.e., because the government lacks the technical ability to isolate unique identifiers, the statistic counts the number of records even if unique identifiers are repeated. This statistic includes records that were received from the providers in CY2016 for all orders active for any portion of the year, which includes orders that the FISC approved in 2015.

Call Detail Record (CDR) Statistics

<table>
<thead>
<tr>
<th>Call Detail Records “CDR” – Section 501(b)(2)(C)</th>
<th>CY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Estimated number of call detail records received from providers and stored in NSA repositories</td>
<td>151,230,968</td>
</tr>
</tbody>
</table>

As an example, assume an NSA intelligence analyst learns that phone number (202) 555-1234 is being used by a suspected international terrorist. This is the “specific selection term” or “selector” that will be submitted to the FISC (or the Attorney General in an emergency) for approval using the “reasonable articulable suspicion” (RAS) standard. Assume that one provider (provider X) submits to NSA a record showing (202) 555-1234 had called (301) 555-4321 on May 1, 2016. This is the “first hop” and would count as one record. If the provider submits records showing additional calls between those same telephone numbers, each would count as an
additional record. Thus, if over the course of 2016, (202) 555-1234 was in contact with (301) 555-4321 once each day, then that would count as 365 records obtained from provider X. If another provider (provider Y) also submits records showing direct contact between those two telephone numbers (assume the same number of contacts), then those would add to the count.

In turn, assume that NSA submits the “first-hop” number above – (301) 555-4321- to the providers, and finds that it was used to call (410) 555-5678. This is the “second-hop” result. Each contact between the first-hop and second-hop numbers would count as a separate record, as would each such contact submitted by other providers. More information on how NSA implements this authority can be found in the DCLPO report.

**Call Detail Record (CDR) Statistics**

<table>
<thead>
<tr>
<th>Call Detail Records “CDR” – Section 501(b)(2)(C)</th>
<th>CY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Estimated number of search terms that included information concerning a U.S. person that were used to query any database of call detail records obtained through the use of such orders*</td>
<td>22,360</td>
</tr>
</tbody>
</table>

*Consistent with § 1873(d)(2)(A), this statistic does not include queries that are conducted by the FBI.

**The number of search terms associated with a U.S. person used to query the CDR data.** Each unique query is counted only once. The same term queried 10 times, still counts as one search term. Similarly, a single query with 20 terms counts as 20.

*The remainder of this page is intentionally left blank.*
NATIONAL SECURITY LETTERS (NSLs)

→ *Not authorized by FISA but by other statutes.*

→ *Bulk collection is prohibited, however, by the USA FREEDOM Act.*

→ *FBI may only use NSLs if the information sought is relevant to international counterterrorism or counterintelligence investigation.*

**National Security Letters.** In addition to statistics relating to FISA authorities, we are reporting information on the government’s use of National Security Letters (NSLs). The FBI is statutorily authorized to issue NSLs for specific records (as specified below) only if the information being sought is relevant to a national security investigation. NSLs may be issued for four commonly used types of records:

1) telephone subscriber information, toll records, and other electronic communication transactional records, see 18 U.S.C. § 2709;  
2) consumer-identifying information possessed by consumer reporting agencies (names, addresses, places of employment, institutions at which a consumer has maintained an account), see 15 U.S.C. § 1681u;  
3) full credit reports, see 15 U.S.C. § 1681v (only for counterterrorism, not for counterintelligence investigations); and  
4) financial records, see 12 U.S.C. § 3414.

**Counting NSLs.** Today we are reporting (1) the total number of NSLs issued for all persons, and (2) the total number of requests for information (ROI) contained within those NSLs. When a single NSL contains multiple requests for information, each is considered a “request” and each request must be relevant to the same pending investigation. For example, if the government issued one NSL seeking subscriber information from one provider and that NSL identified three e-mail addresses for the provider to return records, this would count as one NSL issued and three ROIs.

- **The Department of Justice’s Report on NSLs.** In April 2017, the Department of Justice released its *Annual Foreign Intelligence Surveillance Act Report* to Congress. That report, which is available online, reports on the number of requests made for certain
information concerning different U.S. persons pursuant to NSL authorities during calendar year 2016. The Department of Justice’s report provides the number of individuals subject to an NSL whereas the ODNI’s report provides the number of NSLs issued. Because one person may be subject to more than one NSL in an annual period, the number of NSLs issued and the number of persons subject to an NSL differs.

**Why we report the number of NSL requests instead of the number of NSL targets.** We are reporting the annual number of requests for multiple reasons. First, the FBI’s systems are configured to comply with Congressional reporting requirements, which do not require the FBI to track the number of individuals or organizations that are the subject of an NSL. Even if the FBI systems were configured differently, it would still be difficult to identify the number of specific individuals or organizations that are the subjects of NSLs. One reason for this is that the subscriber information returned to the FBI in response to an NSL may identify, for example, one subscriber for three accounts or it may identify different subscribers for each account. In some cases this occurs because the identification information provided by the subscriber to the provider may not be true. For example, a subscriber may use a fictitious name or alias when creating the account. Thus, in many instances, the FBI never identifies the actual subscriber of a facility. In other cases, this occurs because individual subscribers may identify themselves differently for each account (e.g., inclusion of middle name, middle initial, etc.) when creating an account.

We also note that the actual number of individuals or organizations that are the subject of an NSL is different than the number of NSL requests. The FBI often issues NSLs under different legal authorities, e.g., 12 U.S.C. § 3414(a)(5), 15 U.S.C. §§ 1681u(a) and (b), 15 U.S.C. § 1681v, and 18 U.S.C. § 2709, for the same individual or organization. The FBI may also serve multiple NSLs for an individual for multiple facilities (e.g., multiple e-mail accounts, landline telephone numbers and cellular phone numbers). The number of requests, consequently, is significantly larger than the number of individuals or organizations that are the subjects of the NSLs.

**NSL Statistics**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of NSLs issued</td>
<td>19,212</td>
<td>16,348</td>
<td>12,870</td>
<td><strong>12,150</strong></td>
</tr>
<tr>
<td>Number of Requests for Information (ROI)</td>
<td>38,832</td>
<td>33,024</td>
<td>48,642</td>
<td><strong>24,801</strong></td>
</tr>
</tbody>
</table>

The Honorable Richard Burr  
Chairman  
Select Committee on Intelligence  
United States Senate

The Honorable Chuck Grassley  
Chairman  
Committee on the Judiciary  
United States Senate

The Honorable Devin Nunes  
Chairman  
Permanent Select Committee on Intelligence  
U.S. House of Representatives

The Honorable Robert W. Goodlatte  
Chairman  
Committee on the Judiciary  
U.S. House of Representatives

Dear Messrs. Chairmen:

Section 603(b)(2)(B) of the *Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015*, (P.L.114-23), 129 Stat. 268 (hereinafter “USA FREEDOM Act”), requires the Director of National Intelligence (“DNI”) to make publicly available for the preceding 12-month period a good faith estimate of the number of queries concerning a known United States person of unminimized non-content information relating to electronic communications or wire communications obtained through acquisitions authorized under Section 702 of the Foreign Intelligence Surveillance Act (“FISA”), excluding the number of queries containing information used to prevent the return of information concerning a United States person.

If the DNI concludes that this good faith estimate cannot be determined accurately because some, but not all, of the relevant elements of the Intelligence Community (“IC”) are able to provide such good faith estimate, the USA FREEDOM Act requires him to (i) certify that conclusion in writing to the committees identified above; (ii) report the good faith estimate for those relevant elements able to provide such good faith estimate; (iii) explain when it is reasonably anticipated that such an estimate will be able to be determined fully and accurately; and (iv) make such certification publicly available on an Internet website.

I conclude that the good faith estimate required under section 603(b)(2)(B) of the USA FREEDOM Act cannot be determined accurately because some but not all of the relevant elements of the IC are able to provide such good faith estimate. The enclosed report includes the good faith estimate for those relevant IC elements that were able to provide such good faith estimate. Based on the information provided to me by the relevant elements, I reasonably anticipate that such an estimate will be able to be determined fully and accurately by the end of calendar year 2018.
The Honorable Richard Burr  
The Honorable Chuck Grassley  
The Honorable Devin Nunes  
The Honorable Robert W. Goodlatte

If you have any questions regarding this matter, please contact the Office of DNI Director of Legislative Affairs, Deirdre M. Walsh, at (703) 275-2474.

Sincerely,

[Signature]

Daniel R. Coats

Enclosure:  
Statistical Transparency Report

cc:
IC GOVERNANCE FRAMEWORK OVERVIEW

The United States has a multi-layered framework of rules and oversight designed to ensure that we exercise our authorities and use our capabilities properly. The rules are intended to authorize – and restrict – intelligence activities. These rules are in place to ensure that intelligence agencies conduct their activities in a manner that complies with the laws and policies established by our democratic institutions.

Intelligence Community (IC) elements must satisfy their duty to uphold the Constitution by abiding by requirements imposed by the Constitution, as well as applicable statutes, executive orders, and presidential directives. Oversight, by all three branches of the government, is designed to ensure the IC’s activities are consistent with our rules and our values.

RULES

As a general matter, the U.S. has rules to ensure that intelligence agencies act within their authorities and missions, while comporting with the requirements of the Constitution and other applicable laws. The rules require a focus on national intelligence, pursuant to priorities established by the nation’s leaders.

Additionally, specific rules exist regarding the collection, retention and dissemination of foreign intelligence information. These rules are derived from different sources. For example:

- **Statutes** – Relevant statutes include the Foreign Intelligence Surveillance Act (FISA), the Privacy Act, and the Freedom of Information Act (FOIA). In turn, these statutes may call for implementing regulations, policies and procedures. For example, FISA requires that the government must have court-approved procedures governing how it will conduct the surveillance of and protect information about “United States persons.” Generally speaking, a United States person is a U.S. citizen, a Lawful Permanent Resident (LPR), a U.S. corporation, or an unincorporated association in the United States substantially composed of U.S. citizens and LPRs. Under FISA, the government may not intentionally target a U.S. person for electronic surveillance or physical search without an individualized court order, based on probable cause to believe that the target is an agent of a foreign power. If the government incidentally acquires the communications of a U.S. person who is communicating with a FISA target, the government must protect that information in accordance with court-approved “minimization procedures.”

- **Executive Orders (EO)** – EO 12333 has the force of law for intelligence agencies and imposes key restrictions on intelligence activities, including on how information concerning U.S. persons can be collected, retained and disseminated.

- **Presidential Policy Directives (PPD)** – PPDs are another mechanism by which the president establishes rules. PPD-28 regarding Signals Intelligence Activities (SIGINT) is directed at intelligence agencies. It requires that intelligence agencies develop policies to extend certain protections to all people, regardless of nationality, that are comparable to the protections required for information regarding U.S. persons.

IC GOVERNANCE FRAMEWORK HIGHLIGHTS

- Creates a set of rules to ensure that intelligence activities are conducted in a way that upholds intelligence agencies’ duties to the Constitution

- Rules regarding collection, retention, and dissemination of foreign intelligence are derived from statutes, EOs and PPDs

- All three branches of government – executive, judiciary and legislative – are involved in the oversight of intelligence activities
OVERSIGHT

We have a complex system of “many layers with many players,” involving all three branches of government, to ensure that our intelligence agencies conduct their intelligence activities in a manner that complies with the laws and policies established by our democratic institutions.

- **Executive Branch** – There are a range of organizations in the Executive Branch that carry out important advice and oversight functions to protect privacy and civil liberties. Departments and agencies have offices of general counsel to ensure that intelligence activities are conducted lawfully. In addition, offices of the inspector general independently carry out audit, investigation, and related functions to protect against fraud, waste and abuse. Agencies may also have internal compliance offices, intelligence oversight offices, and privacy and civil liberties offices. The Department of Justice also plays a key role in reviewing and approving intelligence agency procedures under EO 12333, and in providing oversight over how agencies implement FISA authorities. Additionally, the Privacy and Civil Liberties Oversight Board (PCLOB), an independent agency within the executive branch, provides advice and oversight of the government’s counterterrorism activities of the government.

- **Congress** – All of our activities are closely overseen by Congress. In particular, the House Permanent Select Committee on Intelligence (HPSCI) and the Senate Select Committee on Intelligence (SSCI) are charged with intelligence oversight. Other congressional committees are also involved, such as the judiciary committees. Congressional oversight is granular, with Congress receiving a broad range of reports pertaining to intelligence activities, including specific reports relating to implementation of FISA authorities. Additionally, Congress frequently requests specific information pertaining to topics of interest by requesting particular reports, answers to written questions, and appearances at hearings by subject matter experts and top officials.

- **Judiciary** – The Foreign Intelligence Surveillance Court strictly supervises the government’s activities concerning FISA. The Court conducts exacting reviews and has the ability to provide judicial oversight regardless of how “secret” the underlying activities may be. Many of the Court’s opinions have been publicly released. Additionally, with the June 2015 passage of the USA FREEDOM Act, the Court has now appointed the required panel of experts who can serve as amicus curiae (literally, “friend of the court”), should the Court confront significant or novel interpretations of law. The USA FREEDOM Act also requires the government to declassify or summarize to the public Court opinions that involve significant interpretations of law.
Executive Summary

The tension between a nation-state’s need to detect and interdict threats to life, safety, and property inevitably conflict with the privacy interests of its individual citizens and private sector entities. Increased flattening and convergence of global communications will continue to exacerbate this tension, as nation-states seek to pursue these twin goods within the common spaces shared by protected populations and those who would hold society at risk.

The US Constitution’s preamble calls on the government to achieve a common defense while securing the blessings of liberty. The US approach to security achieves both goals by empowering the executive branch to defend the nation while providing the legislative and judicial branches with significant oversight and meaningful involvement. This paper makes the case that the provisions of Section 702 of the FISA Amendments Act are both necessary and appropriate under the US Constitution’s mandate that the government pursue all of its aims (i.e., security and privacy). Moreover, the paper provides compelling evidence to rebut widely circulated myths regarding the actual implementation of Section 702, most notably that NSA exceeded either the intent or the letter of its authorities.

For this reason, we believe that Congress should reject calls to repeal or amend Section 702. The statute already provides a well-regulated system for intelligence agencies to collect foreign intelligence from non-US persons who are not located in the United States. The National Security Agency has stated that Section 702 is its single most significant tool for identifying terrorist threats. The program is overseen by all three branches of government and has an unprecedented system of checks and balances. In the past seven years, the program has been remarkably effective, both at protecting the privacy of US persons and
at obtaining valuable intelligence from foreign sources. Accordingly, Congress should reauthorize this valuable foreign intelligence program.

Introduction

In early June 2013, the Guardian and Washington Post newspapers released documents leaked by Edward Snowden, purporting to disclose surveillance by the National Security Agency (NSA), that were to inflame the imaginations of millions of people around the globe. Many of the disclosures by Snowden related to the Foreign Intelligence Surveillance Act’s (FISA) Section 702 (often referred to by the term PRISM).

The vast majority of Americans knew little or nothing of the inner workings of the FISA (first passed in 1978 and amended in 2008). In the days and weeks following publication of Snowden’s allegations, significant attention was given in both press accounts and congressional hearings to alleged misuse of the capability in apparent violation of the authorities conveyed by FISA and controls that had been constructed to constrain the government’s actions. Indeed, just a few weeks after the Guardian report, two law professors wrote an op-ed in the New York Times in which they boldly branded the NSA programs as “criminal,” while in the same paragraph acknowledging that they “may never know all the details of the mass surveillance programs.”

Allegations that NSA directly targeted the servers of major US telecommunication providers or had violated Section 702’s requirement for targeted collection quickly followed—based only the presumption that such abuse could have been tolerated or abetted by the controlling authorities. And that has been precisely the problem with much of the commentary about Section 702: condemnations of the program based on few actual facts and lacking the context of FISA’s purpose and the controls designed and implemented across three branches of government to constrain the government’s actions to those purposes alone.

In this paper, we seek to advance a simple policy suggestion: Congress should reauthorize this important program without any significant changes to the statute. The critics of Section 702 have not presented a compelling argument—based on how the statute actually works—that would compel Congress to make any significant changes to this program. Rather, Section 702 fully meets the Constitution’s charge: providing national security and individual privacy for all those protected by the Constitution. Put simply, there is no good case for not reauthorizing it when it comes up for renewal next year.

Indeed, the criticisms of Section 702—though often well intentioned—generally arise from widespread misunderstandings of the program’s capabilities, controls, and results. There are numerous reasons for this confusion: the complex structure of the...
program, the understandable passions provoked by the Snowden disclosures, and the inherently secret nature of classified information, to name a few. As Congress considers reauthorization of this program, we hope that legislators, the press, and the public have a full and complete understanding both of what Section 702 is, and what it is not.

In this paper, we aim to provide the facts that are necessary for a comprehensive and balanced examination of Section 702. A full understanding of government power can never be gained through an examination of a given capability alone. Rather, it is necessary to consider any capability in the context of its purpose (against which criteria should be constructed to gauge its success) and the controls imposed on it (to ensure that the capability is constrained to its intended application). In this manner, purpose and controls constitute the moral equivalent of bookends that frame and constrain the creation and employment of any government power. This is especially true in the case of government power which must always be framed in light of the constraints embodied in the Constitution, to include the limited purposes for which the government was formed and the explicit constraints upon its authorities characterized in both the articles and the first ten amendments. While less frequently showcased than its counterparts, the Tenth Amendment is perhaps the most significant in this regard: “The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.” Put another way, if a given power is not explicitly granted to the government, it cannot exercise it.

In order to place Section 702 in this context, this paper will explore the three interdependent aspects of the law. What is its purpose (and does that purpose remain true today)? What capability did the law and its attendant implementation bring into being? What are the controls imposed on the use of the authority? After describing the purpose, capability, and controls of Section 702, we examine the program’s operational results and consider Fourth Amendment concerns that some critics have raised.

A thorough examination of the purpose, capability, and controls of Section 702 paints a very different picture than the one seen in many critical accounts: the program is a limited and highly effective exercise of the executive branch’s constitutional authorities, designed to provide for a common defense while protecting individuals’ constitutional liberties. As we explain, there is no evidence of government overreach with Section 702, and a number of statutory safeguards would prevent such hypothetical abuses from occurring in the first place.

Many of the concerns that critics have raised could be addressed by a more frank and open public dialogue about the operations conducted under Section 702. But
the answer, we shall argue, does not lie in changing a law that has served the country remarkably well.

1. Purpose of Section 702

Congress passed Section 702 with a clear purpose: to effect the collection of foreign intelligence in a world that increasingly shares communications infrastructure between legitimate foreign intelligence targets and protected persons when the communications travel through the United States. As we describe in this paper, the law is carefully crafted to achieve the Constitution’s twin aims of national security and individual liberties.

While led by the law, this paper will also take care to illuminate the operational case for and use of Section 702. Like the rest of its counterpart sections within the broader Foreign Intelligence Surveillance Act of 2008, Section 702 is wholly focused on the collection and production of foreign intelligence. Moreover, Section 702 only allows the targeting of foreign persons or organizations who are themselves located outside the United States. Given those facts, the question that immediately arises is why this collection is, or should be, allowed to take place within the physical confines of the United States. The answer is straightforward. Collection within the United States, employing US infrastructure and US-based service providers, occasions three particular benefits:

1. The collection activity can be effected with greater care and attendant precision given the relative stability and safety of the domestic environment. In fact, procedures designed under certifications authorized by Section 702 must be constructed to take advantage of this opportunity for greater precision, ensuring that collection is specifically and narrowly focused on legitimate foreign intelligence targets.

2. Given the precision afforded in the selection and capture of the collected materials, Section 702 collection is therefore far more likely than its counterpart Executive Order 12333 collections (which typically take place in uncontrolled environments outside the United States) to yield pristine, intact copies of the desired communication transactions. The particular challenge of collecting unintended material adjacent to the targeted communication encountered in 702’s upstream collection will be discussed later in the paper and is addressed by imposing controls on its processing and handling.

3. FISA ensures that the collection is authorized and regulated by the combined efforts of three branches of government.
Section 702 laid in place a legal regime unique in the world that involves all three branches of government to authorize, oversee, and regulate collection effected under provisions of 702. This complex set of legal rules, however, has led to great misunderstanding of its initial purpose.

To fully understand the purpose of Section 702, it is helpful to review its history. The current framing of Section 702 is contained in the Foreign Intelligence Surveillance Act Amendments Act of 2008 (often referred to as the FISA Amendments Act or FAA). While sometimes perceived as a means to expand the capabilities of the government in effecting foreign intelligence collection, the FAA was actually designed to sustain capabilities codified in the FISA legislation of 1978, while addressing thirty years of technology modernization which had rendered both the capabilities authorized by FISA and, equally important, the controls imposed on it considerably less effective than when first implemented in the late 1970s. Two particular trends across those years warrant a more careful examination.

The first was the transformation of technology between 1978 and 2008 during which time the vast portion of international communications (between nations) made a dramatic shift to physical cables (especially high-speed fiber optic cables) and domestic communications made increasing use of wireless modes of transmission. And yet all through this period, the provisions of FISA 1978 presumed that the preponderance of communications conveyed by “wire” would be local communications and those transiting “in the air” (e.g., satellite communications in 1978) would be international in nature. As a consequence, the provisions of FISA 1978 tightly regulated NSA’s access to wireline communications with considerably less attention given to those transiting in the air. The flaw in the 1978 formulation wasn’t that its technology forecast was wrong. It was in trying to codify technology trends at all. FISA 2008 rewrote the 1978 law to sustain its provisions for both national security and privacy protections in a technology neutral context.

Second, the explosion of commercial offerings of various technologies enabled tremendous agility on the part of consumers, not only in the services they could employ but in their choice and use of selectors (e-mail address or telephone numbers) across a growing number of services. While this must be perceived for the vast majority of users as an unalloyed good, it introduced a significant challenge for intelligence services which, under FISA 1978, had to obtain explicit approval for each and every selector they wanted to target. In 2008, there was a growing body of evidence that terrorists were making effective use of this agility, acquiring and shedding e-mail addresses and telephone numbers faster than US intelligence services could prepare, submit, and obtain required selector-by-selector approvals. To address the need to equip national intelligence with an agility on par with legitimate
intelligence targets, FISA 2008 replaced the FISA 1978 selector-by-selector-based approvals with a certification approach that created and approved procedures to be followed by the executive branch for determining and employing individual selectors in foreign intelligence collections, in lieu of continuing to require selector-by-selector approvals. This compromise resulted in the creation of a requirement for “certifications” under FISA 2008, yielding both agility and accountability for the executive branch’s use of the FISA capability.

The Senate Judiciary Committee report 112-229 of September 20, 2012, noted in its introduction to the FAA Sunsets Extension Act of 2012 (which extends FAA 2008 for another three years) that:

. . . as amended, [this bill] reauthorizes Title VII of FISA for three years, enabling continued use of these important surveillance tools, while improving and clarifying the oversight and accountability provisions in Title VII to help ensure adequate protection of the privacy rights and civil liberties of persons in the United States. 4

Indeed, Congress carefully crafted Section 702 to establish an effective, but narrow, system that focuses on the acquisition of foreign intelligence information from non-US persons outside of the United States. Congress’s intentions are clear both from the plain text of the statute and from the legislative history.

Even the title of Section 702—“Procedures for targeting certain persons outside the United States other than United States persons”—indicates that Section 702 is not intended to gather information about US citizens. 5 The statute then makes clear that collection only is authorized if the targets are reasonably believed to be non-US persons located outside of the United States, and it imposes extensive limits on the collection and use of the data (described in more detail in Part 2 of this paper). The statute also requires intricate procedures “to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.” 6

Quite simply, there are few US law enforcement regimes that are subject to such a rigid set of detailed statutory and regulatory requirements. The plain language of the statute evinces Congress’s clear intent to create a program that efficiently and effectively gathers foreign intelligence information, while avoiding, to the greatest extent possible, targeting the content of communications that involve US citizens or individuals reasonably believed to be located in the United States.
Section 702’s legislative history also demonstrates the narrow purpose of the program. In its report accompanying an earlier version of the FAA, the Senate Intelligence Committee wrote that its goal “has been to develop a sound legal framework for essential intelligence activities in a manner consistent with the U.S. Constitution.”

Congress also has recognized the vital and irreplaceable national security functions of Section 702. In the House report recommending the 2012 reauthorization of FAA, legislators wrote that Section 702 information “is often unique, unavailable from any other source, and regularly provides critically important insights and operationally actionable intelligence on terrorists and foreign intelligence targets around the world.”

Despite the clear intent of Section 702 as a means of gathering foreign intelligence information on targets who are non-US persons located outside of the United States, critics are worried about the incidental interception of the communications of US persons. They raise the valid—though unsupported—concern that Section 702 is intended to be a back door around the general Fourth Amendment requirement that the government obtain a warrant before collecting the communications of US persons. This argument fails to appreciate the reason that Section 702 must allow the possibility of incidental interception: it is impossible for the government, before beginning a surveillance operation, to know with certainty the identities of every individual with whom the target might communicate. As one federal court recognized in 2000, the government “is often not in a position of omniscience regarding who or what a particular surveillance will record.” Any incidental collection of a US person’s communications is just that: incidental. To be clear, because any single communication is associated with two or more parties (a sender and one or more recipients), the “incidental communication” described here is one and the same as the communication that has been legitimately targeted and collected by the government (otherwise the legal phrasing applied to the communication would be an “unintended collection,” a subject which must not be conflated here). It is certainly possible that all parties to a given communication are legitimate targets of surveillance. But in every other case, all parties not explicitly targeted by the government will be considered as incidental to the intended collection. In this manner, an absolute prohibition on incidental collection would effectively shut down our ability to collect foreign intelligence in any case where the status of all parties in a given communication is unknown.

Critics also argue that Section 702 is merely the intelligence community’s attempt to avoid seeking Foreign Intelligence Surveillance Court approval of an order, supported by probable cause, under Title I of FISA. This argument ignores the fact that Title I is used in part to collect foreign intelligence from targets who are US persons or located in the United States, and therefore are entitled to the full panoply
of rights under the US Constitution. It would be unprecedented—and impractical—to require intelligence analysts to obtain a search warrant every time that they sought to gather information regarding a target who is neither a US person nor located in the United States. As the Public Civil Liberties Oversight Board (PCLOB) aptly concluded in its 2013 report, Section 702 “enables a much greater degree of flexibility, allowing the government to quickly begin monitoring new targets and communications facilities without the delay occasioned by the requirement to secure approval from the FISA court for each targeting decision.”11 This flexibility allows the government to more quickly learn of a terrorist plot or other national security threat that it otherwise would not have learned of if it had to comply with the full court procedures.

As we show in the next section, the program is structured to provide the government only with the capabilities to conduct these foreign intelligence operations, targeting non-US persons who are located outside of the United States.

2. Capability of Section 702

In this section, we describe the actual capability of the Section 702 program, both as stated in the law and as implemented by the NSA.12 NSA's actual surveillance capabilities under Section 702 are far narrower than many media reports would suggest.

Contrary to incomplete and inaccurate reporting shortly after the Snowden leaks, Section 702 does not provide NSA or other governments with the ability to “tap into” service providers' US servers. On June 6, 2013, the Washington Post reported that the NSA and FBI “are tapping directly into the central servers of nine leading US Internet companies, extracting audio, video, photographs, e-mails, documents, and connection logs that enable analysts to track a person’s movements and contacts over time.”13 Professor Peter Swire, who served on the President’s Review Group on Intelligence and Communications Technology, recently released a comprehensive paper that debunks that myth. He concludes that “the government does not have direct access under the PRISM program, but instead serves legal process on the providers similar to other stored records requests.”14

Section 702 focuses on ensuring that the surveillance is conducted for foreign intelligence purposes and targets non-US persons. To wit, the first two subparts of Section 702 impose a number of limitations on the collection of foreign intelligence information under the program:

- Both the attorney general and director of national intelligence must authorize any collection.15
• The collection can be authorized for no more than one year.\textsuperscript{16}

• Section 702 operations “may not intentionally target any person known at the time of acquisition to be located in the United States.”\textsuperscript{17}

• Even if the individual is reasonably believed to be located outside of the United States, the agencies cannot target that person with the ultimate purpose of targeting a person reasonably believed to be located within the United States (a prohibition against so-called “reverse targeting”).\textsuperscript{18}

• Agencies may not target a US person (such as a US citizen or permanent resident), even if that person is reasonably believed to be located outside of the United States.\textsuperscript{19} While targeting US person communications outside the United States was previously permitted by FISA 1978 under attorney general authorization, the FAA of 2008 significantly strengthened protections given to US persons by requiring that a probable-cause warrant be obtained for \textit{any} collection targeting the content of a US person’s communications, regardless of the person’s location in the world.

• Even if the target is a non-US person located outside of the United States, the agencies may not “intentionally acquire communication for which the sender and all intended recipients are known at the time of the acquisition to be located inside of the United States.”\textsuperscript{20}

• The program must be conducted “consistent” with the Fourth Amendment.\textsuperscript{21}

The entire operating structure of Section 702 is designed to satisfy these restrictions. It is important to note that the burdens imposed by these restrictions are never relieved—from the collection and processing of communications, through analysis and reporting, to dissemination and retention. To fully understand the operations of the program, it is useful to consider the process in five stages:

1. \textbf{Certification}: receiving approval from the Foreign Intelligence Surveillance Court for collecting intelligence for a foreign intelligence purpose.

2. \textbf{Targeting}: identifying targets who are non-US persons located outside of the United States and the e-mail addresses, phone numbers, and other communications facilities associated with them (known as “selectors”).

3. \textbf{Tasking}: obtaining the communications from selectors that are used by these targets.
4. **Analysis**: querying the raw data and disseminating intelligence.

5. **Retention and destruction**: ensuring that NSA does not indefinitely hold on to all raw data after tasking.

**A. Certification**

The attorney general and director of national intelligence annually certify to the Foreign Intelligence Surveillance Court a list of foreign intelligence topics for which intelligence agencies seek to collect information under Section 702. The certifications must attest that “a significant purpose of the acquisition is to obtain foreign intelligence information” and describe, in detail, the procedures that ensure that US persons are not targeted. Although the complete list of such topics is classified, the certifications are formally documented by the executive branch and must be approved by the judicial branch (i.e., the Foreign Intelligence Surveillance Court). Moreover, government officials have publicly stated that the topics include international terrorism and acquisition of weapons of mass destruction.

The Foreign Intelligence Surveillance Court’s role is to review certifications, request amendments, and determine whether the targeting procedures are reasonably designed to ensure that actions are “limited to targeting persons reasonably believed to be located outside the United States.”

**B. Targeting**

If an NSA analyst identifies a non-US person located outside of the United States as a potential target for gathering foreign intelligence for a purpose that the Foreign Intelligence Surveillance Court has certified, the analyst must follow a detailed, and FISC-approved, set of targeting procedures.

First, the analyst must determine the specific e-mail address, telephone number, or other communications facility that is used by the target (known as a “selector.”). The NSA analyst then checks multiple sources to verify both the “foreignness” of the target and the connection between the target and the selector.

After an extensive review of the NSA’s targeting procedures, the Privacy and Civil Liberties Oversight Board agreed that this foreignness determination is “not a 51% to 49% test,” and that if there is “conflicting information indicating whether a target is located in the United States or is a U.S. person, that conflict must be resolved” and the user must be determined to be a non-US person reasonably believed to be located outside the United States prior to targeting. This procedure is highly effective; in 2013, the Justice Department conducted a comprehensive review of one year of data regarding NSA’s targeting decisions and concluded 99.6 percent of the selectors that
NSA tasked under Section 702 did not have any users who were located in the United States or were US persons.²⁹

The NSA analyst also must document the specific foreign intelligence purpose for which it seeks to target an individual.³⁰ The analyst must specifically document the foreign power or foreign territory about which this surveillance will provide foreign intelligence.³¹ NSA analysts also typically include a brief statement that “further explains the analyst’s rationale for assessing that tasking the selector in question will result in the acquisition of the types of foreign intelligence information authorized by the Section 702 certifications.”³²

Upon completion of the due diligence, the analyst provides documentation of this verification to two senior NSA analysts. Only after the senior analysts approve the request may a service provider be compelled to provide the communications associated with the selector through tasking.

C. Tasking

When a selector is tasked, the NSA receives information from service providers through one of two processes.

The first process, referred to in the press as the PRISM program, requires service providers to provide NSA with communications to or from the explicitly tasked selectors. Before this data is made available to NSA analysts, it is reviewed by service provider technicians to ensure that the communications are restricted to only the types of communications that are the subject of the government’s request. This provides yet another additional limit on distribution under the program. According to data that the government provided to the Foreign Intelligence Surveillance Court, more than 90 percent of NSA’s Section 702 data came from this process.

The second process, known as upstream collection, has received the most public scrutiny and is often conflated with PRISM, though it accounts for approximately 10 percent of all Section 702 data. In the upstream process, the NSA works with telecommunications providers to obtain telephone and Internet communications that traverse US communications infrastructure.³³ The operational motivation of this capability is not intended to duplicate collections available from PRISM. Rather, it is designed to acquire targeted “in-stream” communications not under the direct control of the service providers. As with the PRISM process, electronic communications collected via the upstream process can be to or from a tasked selector. Unlike communications collected via PRISM, upstream communications also can be “about” a selector.³⁴
An “about” communication “is one in which the tasked selector is referenced within the acquired Internet transaction, but the target is not necessarily a participant in the communication.” For instance, if the selector is a target’s e-mail address, the NSA could acquire e-mail messages that contain that address in the body of the e-mail, regardless of whether the sender or recipient is a target.

NSA collects two types of Internet communications transactions through the upstream process: single communication transactions (SCTs) and multi-communication transactions (MCTs). SCTs, which comprised about 90 percent of the upstream communications that the NSA collected during a six-month sample period in 2011, are discrete communications, such as a single e-mail message. MCTs, in contrast, consist of multiple communications that are packaged and transmitted as a single entity (i.e., the inbox listing of a single communicant is often transmitted by service providers as a single intact stream of bits, even though it represents the leading edge of many individual e-mails). Due to this fact, and the ever-changing nature of service providers’ protocols and other technology, it is not always technically possible for the government to collect only the portions of MCTs that are foreign communications to, from, or about the tasked selectors. If the NSA identifies a communication within an MCT as being to, from, or about a selector, the NSA obtains the complete MCT. Accordingly, there are instances in which a discrete communication within an MCT contains a discrete domestic communication that is not to, from, or about a tasked selector.

Critics of Section 702 claim that the “about” process, when combined with the collection of discrete messages in an MCT, results in the collection of purely domestic communications, or communications that contain US person information and are not to, from, or about a tasked account. To be sure, such collection does occur, but it represents a tiny sliver of the total upstream data. A Foreign Intelligence Surveillance Court review of a sample provided by NSA found that such incidental collection only occurs for approximately 0.02 percent of upstream communications. Moreover, upstream data accounts for less than 10 percent of all communications collected under Section 702.

Even so, recognizing the possibility that MCTs might contain US person data, the FISC has imposed additional procedures to ensure due diligence in detecting their presence and effecting appropriate protections. Once the data are acquired, NSA analysts must review a sample of the communications to ensure that they are related to the target and foreign intelligence purpose that the analyst initially identified. The analyst also must review the sample to ensure that the target is a non-US person located outside of the United States. Selectors that do not meet this criteria are “de-tasked” and not available for analysis.
Moreover, NSA’s minimization procedures require the agency to acquire information in a manner that is designed “to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the acquisition.”46

The minimization procedures also take care to account for the change of a target’s location from outside of the United States to inside the United States. Even if the target is a non-US person, the NSA will cease Section 702 operations directed at that target if it reasonably believes that the target is now located in the United States. For instance, suppose that an NSA analyst uses Section 702 to lawfully obtain the e-mails of a suspected terrorist who is located in Syria. If the analyst learns that the target has since moved to New York, the acquisition “will be terminated without delay.”47 Domestic surveillance laws, under the purview of the FBI, would apply at that point.

D. Analysis

Once NSA has properly tasked selectors and obtained information from communications, it faces a series of limits on its ability to analyze this data.48 It is important to recognize that the following restrictions are applied to collected communications—specifically, those communications that have already shown themselves to be responsive to a foreign intelligence query. Put another way, the mere fact that a given communication contains a selector of legitimate interest to an NSA intelligence analyst does not relieve the burden imposed by FAA 2008 to proactively sustain protections for US persons throughout the collection-to-dissemination process.

Among the most prominent criticisms of Section 702 is that analysts could query raw communications to obtain information about US persons.49 (“Raw” means that, while each communication has already been shown to contain a targeted selector, it has not yet been reviewed to determine its actual relevance or import to the given foreign intelligence inquiry.) In other words, critics argue, this would be a back door for spying on US persons without a warrant.50

NSA’s minimization procedures, however, explicitly prevent such intentional backdoor surveillance. Analysts may only search for terms, such as phone numbers or key words, that are “reasonably likely to return foreign intelligence information.”51 As an absolute rule, however, analysts may not use an identifier of an identifiable US person to search upstream Internet communications.52 Moreover, NSA analysts generally are prohibited from using a US person’s identifier as a search term for other Section 702 data unless they justify the specific search in a written statement of facts and receive additional approval before conducting the query.53 According to PCLOB, 198 US person identifiers were approved for NSA queries in all of 2013.54
Moreover, it is important to note that the restrictions on NSA use of US person terms apply to the use of any US person term, regardless of the context. For example, an analyst pursuing a possible terrorist threat to an airline incorporated in the United States would need to follow the procedures described above before searching already collected terrorist communications for the presence of any of the following terms: “American Airlines,” “United Airlines,” or a named US person or corporation assessed to be a target of a given terrorist plot.

NSA analysts also are prohibited from using broad, overly generic search terms or conducting other similar unrestricted fishing expeditions.

The minimization procedures also recognize the legitimate concerns that MCTs may contain wholly domestic, discrete communications that are not to, from, or about the tasked selectors. The procedures require NSA to take “reasonable steps” to use technical means to segregate MCTs for which the active user—i.e., the sender or recipient—is “reasonably believed” to be located within the United States. The NSA also will segregate MCTs if the active user’s location cannot be determined. Those segregated MCTs are then reviewed by NSA analysts, who determine whether the transactions contain domestic communications. The analysts are required to document all of these determinations.

If an individual communication within an MCT is not to, from, or about a tasked selector and is to or from a US person or an individual “reasonably believed” to be in the United States, that individual communication cannot be used, except “to protect against an immediate threat to human life[.]” If the NSA uses the information for this purpose, it must report the use to the director of national intelligence and the Justice Department, which informs the Foreign Intelligence Surveillance Court.

The NSA also has imposed strict limits on its ability to share information that it has obtained under Section 702. The minimization procedures state that NSA may only disseminate data of or concerning a US person under one of a handful of limited conditions, such as the individual being an agent of a foreign power. Even when the NSA is authorized to disseminate this data, it usually masks the US person’s identity and redacts other identifying details.

### E. Retention and Destruction

Section 702 has been portrayed in some accounts as the government’s attempts to stockpile massive amounts of communications, including some involving US citizens. To be sure, Section 702, like other intelligence operations, involves vast volumes of e-mails and other communications. However, the minimization procedures prevent
NSA from holding on to these communications indefinitely, particularly if the communications are domestic.

If the NSA determines that a communication is purely domestic, the communication must be “promptly destroyed upon recognition” unless the NSA director makes the specific determination that the sender or recipient has been lawfully targeted and that the communication is reasonably believed to contain significant foreign intelligence information, evidence of a committed or planned crime, or technical information for signal exploitation or related purposes. The agency also may retain communications that contain information indicating an imminent threat of serious harm to life or property.

The NSA’s minimization procedures require all telephone and Internet transactions that the agency obtained from service providers to be destroyed within five years of the FISC certification, “unless NSA specifically determines” (1) that retention is “necessary for the maintenance of technical data bases;” (2) that the data is evidence of a past, ongoing, or future crime and has been turned over to federal law enforcement; or (3) the NSA satisfies the dissemination standards described in the previous section. Moreover, all upstream Internet transactions must be destroyed within two years of the expiration of the FISC’s certification, unless at least one communication within the transaction meets the NSA’s retention standards and is to, from, or about a tasked selector, a non-US person, or a person not located in the United States. This procedure prevents the NSA from stockpiling decades of raw data regardless of relevance.

3. Controls on Section 702

Much of the criticism of Section 702 has been premised on the assumption that a rogue NSA agent could have sweeping and unregulated access to the communications content, using the program to spy on personal enemies and commit other serious privacy violations. As with many of the criticisms surrounding Section 702, this arises largely from a misunderstanding of the complex structure of the program. An objective examination of Section 702’s intertwined network of checks and balances paints an entirely different picture. The Section 702 program has extensive oversight by the NSA, other executive branch agencies, the judicial system, and Congress.

An NSA analyst would be ill-advised to abuse the Section 702 system, particularly to gather data on a US person without proper authority. Such a move could be reviewed by numerous superiors at the NSA, the Justice Department, the Office of the Director of National Intelligence, the Inspectors General of the NSA and other agencies, four congressional committees, and the Foreign Intelligence Surveillance Court. In no case could the action be taken unilaterally without the material involvement of one
or more of the above named parties. Accordingly, it is unsurprising that the criticism of Section 702 has focused on hypothetical rather than actual abuses of Section 702 authorities; the system of safeguards across all three branches of government is carefully designed to prevent misuse of the data.

A. NSA

As discussed throughout Part 2 of this paper, analysts must produce extensive documentation of their decisions regarding targeting, tasking, querying, and retention of communications. The controls are particularly stringent when the communications may be to, from, or about a US person or person located in the United States. NSA’s Signals Intelligence Directorate regularly audits a sample of queries that include US person identifiers. This provides an additional check to ensure that analysts are not misusing the data.

NSA requires analysts to enroll in an extensive training curriculum before allowing them to access Section 702 data or other signals intelligence information. Although many of the training modules are classified, the American Civil Liberties Union obtained unclassified versions of some of the training materials via the Freedom of Information Act. A review of these materials demonstrates that the NSA not only explains the law, but also provides practical guidance as to how analysts can meet those legal requirements. For instance, the following are the NSA’s training instructions in the case of inadvertent collection of US person information:

- Stop collection immediately!
- Cancel reports based on that collect.
- Notify your supervisor or auditor.
- Write up an incident report immediately.
- Submit the incident write-up for inclusion in your organization’s IG [inspector general] Quarterly input.

If NSA employees fail to follow any of the detailed limitations on their ability to collect or use the Section 702 data, they are subject to a number of internal compliance positions, including the employees’ supervisors, NSA’s director of civil liberties and privacy, NSA’s general counsel, and NSA’s inspector general. And while concerns about potential abuse properly inform the diligence with which controls are designed and enforced, numerous and extensive investigations conducted by outside parties before and after the sensational claims of Edward Snowden in 2013 have yet
to document a single case of abuse of Section 702 data by an individual or a systemic abuse by the NSA. Indeed, as Geoffrey Stone, the Edward H. Levi Distinguished Service Professor of Law at the University of Chicago and a member of the President’s 2013 NSA Review Group, stated in an op-ed in March 2014:

From the outset, I approached my responsibilities as a member of the Review Group with great skepticism about the NSA. I am a long-time civil libertarian, a member of the National Advisory Council of the ACLU, and a former Chair of the Board of the American Constitution Society. To say I was skeptical about the NSA is, in truth, an understatement. I came away from my work on the Review Group with a view of the NSA that I found quite surprising. Not only did I find that the NSA had helped to thwart numerous terrorist plots against the United States and its allies in the years since 9/11, but I also found that it is an organization that operates with a high degree of integrity and a deep commitment to the rule of law.

Like any organization dealing with extremely complex issues, the NSA on occasion made mistakes in the implementation of its authorities, but it invariably reported those mistakes upon discovering them and worked conscientiously to correct its errors. The Review Group found no evidence that the NSA had knowingly or intentionally engaged in unlawful or unauthorized activity. To the contrary, it has put in place carefully-crafted internal procedures to ensure that it operates within the bounds of its lawful authority.67

B. Other Executive Branch Agencies

NSA’s Section 702 program also is subject to oversight by a number of other executive branch agencies, reducing the likelihood of a single department head allowing compliance to slip through the cracks.

Every other month, both the Justice Department and Office of the Director of National Intelligence review NSA analysts’ documentation of its compliance with Section 702 restrictions. Both agencies review large samples of both the tasking documentation and the report that NSA has disseminated; Justice Department attorneys determine whether the documentation meets the statutory and procedural requirements.68

The Justice Department and Office of the Director of National Intelligence receive reports of suspected noncompliance with Section 702 procedures, investigate incidents, and regularly discuss compliance issues with intelligence agencies.69 Separately, the inspectors general of other intelligence and law enforcement agencies also have the legal authority to review the NSA’s Section 702 programs.70
C. Congress

The Justice Department and the Office of the Director of National Intelligence provide the results of their routine reviews of targeting and minimization to the House and Senate Judiciary and Intelligence committees. The agencies also are required to report any compliance incidents to congressional committees in a semiannual report.

FISA requires the report to contain extensive details—many of which are classified—to ensure that members of the four committees have a complete understanding of the Section 702 programs. Among the required components of the semiannual report are the Foreign Intelligence Surveillance Court’s certifications, any compliance reviews conducted by the Justice Department or Office of the Director of National Intelligence, and descriptions of all incidents of noncompliance. The committees also hold hearings on the program.

D. Judiciary

Section 702’s operations are subject to extensive oversight by the Foreign Intelligence Surveillance Court (FISC). Although the court’s independence and transparency have been derided by critics, they ignore the fact that the court is comprised entirely of Article III, life-tenured judges who are appointed by the president and confirmed by the Senate. These are the same judges who hear the full range of civil and criminal cases over which our federal courts have jurisdiction.

As discussed in Part 2 of this paper, FISC must review and approve the Section 702 certifications and minimization procedures, ensuring that the intelligence community only operates the Section 702 program for purposes authorized by law. Moreover, FISC receives all of the reports of noncompliance, the Justice Department/director of national intelligence semiannual reports, annual Section 702 reports produced by each intelligence agency, and inspector general reports about Section 702.

Courts do more than comment on the Section 702 programs; they work with the agencies to change procedures that they do not believe satisfy the program’s statutory or constitutional mission. Consider Judge John Bates’s 2011 opinion, in which he considered the incidental collection of wholly domestic communications within MCTs.

In May 2011, the government filed a letter with the court, clarifying that MCTs may contain discrete communications that are not to, from, or about the tasked facility. Judge Bates, concluding that these acquisitions “exceeded the scope of collection previously disclosed by the government, and approved by the Court,” quickly ordered
briefings and a hearing on the issue.77 After a thorough review of the evidence, Judge Bates concluded that this acquisition complies both with the statutory requirements of Section 702 and with the Fourth Amendment.

However, Judge Bates stated that “NSA could do substantially more to minimize the retention of information concerning United States persons that is unrelated to the foreign intelligence purpose of its upstream collection.”78 Judge Bates then listed a number of additional limits the government could impose, including restricting access to upstream communications to a smaller subset of trained analysts and requiring analysts to analyze discrete communications for compliance with Section 702. Judge Bates noted that some of the steps that he suggested might be impracticable, but that “by not fully exploring such options, the government has failed to demonstrate that it has struck a reasonable balance between its foreign intelligence needs and the requirement that information concerning United States persons be protected.”79

After this opinion, the NSA revised its minimization procedures to prohibit its analysts from using discrete communications from within an MCT unless the analyst first has reviewed that specific communication to determine whether it is to or from a non-US person who is located out of the United States. If not, then the analyst may only use that communication to protect against immediate threats to life.80

Judge Bates’s opinion demonstrates Section 702’s system of effective checks and balances in action. Step back to think about the efficiency of these oversight mechanisms: in May, the government voluntarily reported new information about the program’s operations to the court; in October, the court issued an extensive examination of the program’s legal underpinnings and areas for improvement; and, by the end of the year, the government had incorporated that feedback into its operations. As intelligence officials noted in congressional testimony later that year, the court’s “exhaustive analysis of the Government’s submission, like its other decisions, refutes any argument that the court is a ‘rubber stamp,’ and demonstrates the rigorous nature of the oversight it conducts.”81

4. Results of Section 702

To fully assess a government program, it is necessary to consider not only its purpose, capability, and controls, but also the benefits that it brings to the general public. In the case of Section 702, that benefit is increased national security. Unfortunately, due to the necessarily classified nature of our national security operations, it is difficult to describe many of the specific instances in which Section 702 data has helped to protect Americans. However, the publicly reported aggregate information demonstrates the powerful and irreplaceable role that Section 702 plays in our
national security and intelligence operations. President Obama stated that after he “looked through specifically what was being done,” he determined that sections 215 and 702 “offered valuable intelligence that helps us protect the American people and they’re worth preserving.”

After its thorough review of Section 702, the independent civil liberties oversight board concluded that the statute “has enabled the U.S. government to monitor these terrorist networks in order to learn how they operate and to understand how their priorities, strategies, and tactics continue to evolve,” noting that more than a quarter of the NSA’s reports involving international terrorism are based at least partly on Section 702 data.

For instance, the oversight board cited the case of Khalid Ouazzani, who was located in Missouri and was part of a plan to bomb the New York Stock Exchange. The NSA learned of him during its surveillance of a Yemeni extremist’s e-mail address. He was apprehended and later convicted after the NSA conveyed this intelligence to the FBI. He also was a cooperating witness for the prosecution of two Al Qaeda supporters.

Similarly, the oversight board cited NSA’s surveillance of the e-mail address of an Al Qaeda courier in Pakistan that led the agency to Najibullah Zazi, a Denver man whom the courier contacted for information about bomb-making. The NSA provided this tip to the FBI, which tracked Zazi as he and collaborators drove to New York to detonate explosives on subways. Zazi learned that he was being tracked, returned to Colorado, and was soon arrested. As the oversight board correctly concluded, without the initial Section 702 information, obtained through monitoring a Pakistani, “the subway-bombing plot might have succeeded.”

Section 702 information also contributed to the arrest in Chicago of David Coleman Headley, who had planned to attack a Danish newspaper that had printed cartoons of the Prophet Muhammad. Headley also had helped to plan the 2008 terrorist attacks in Mumbai and was sentenced to thirty-five years in prison.

An expert intelligence review group, appointed by the president, concluded in 2013 that Section 702 “has clearly served an important function in helping the United States to uncover and prevent terrorist attacks both in the United States and around the world.” The record of Section 702 in supporting the collective security of nations other than the United States is particularly notable. Government officials frequently testified in open congressional session during the summer of 2013 that Section 702 had played an instrumental role in the disruption of at least fifty-four terrorist plots around the world between 2001 and 2013. Forty-one of these were described as having a nexus in a country other than the United States, of which twenty-five were
plots that were to take place in Europe. In each of these cases, information derived from Section 702 was shared by the United States with counterparts in countries believed to be under threat, leading to the application of appropriate instruments of national and international (collective) power by those nations under a rule of law consistent with both the United States and the local jurisdiction. In this manner, Section 702 contributed to the collective security of many nations under a scheme that ensured a rule of law defined by the highest common denominator between national approaches, not the lowest.

5. Constitutionality of Section 702

Since Section 702’s enactment—and especially since the 2013 Snowden disclosures—critics have asserted that the program violates the Fourth Amendment’s prohibition on unreasonable searches and seizures. However, courts have repeatedly held that Section 702—as written and implemented—complies with the Fourth Amendment. The courts’ Fourth Amendment reasoning demonstrates that Section 702 not only is constitutional, but is sound public policy that protects both national security and individual liberties. In other words, for the same reasons that Section 702 is constitutional (i.e., its minimal intrusion of privacy interests in comparison to the significant security benefits), it also is sound public policy, and Congress should reauthorize the statute without any significant revisions.

The Fourth Amendment states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

At the outset, the Fourth Amendment’s protections do not “apply to activities of the United States directed against aliens in foreign territory.” Accordingly, the Fourth Amendment concerns surround the incidental collection of US persons’ communications.

Thus, in assessing Section 702’s compliance with the Fourth Amendment, we must examine: (1) whether a warrant is required for the incidental collection of the communications of US persons; and (2) whether the process is reasonable.

A. Warrant Requirement

The Fourth Amendment’s warrant requirement does not apply to Section 702 for two reasons.
First, courts have long held that “incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful.” Section 702 is directed at intelligence from non-US persons who are located outside of the United States. Any incidental collection of US persons’ information, therefore, is not subject to the Fourth Amendment warrant requirement.

Second, Section 702 falls within the foreign intelligence exception to the warrant requirement. The Supreme Court has long recognized that the warrant requirement does not apply “when special needs, beyond the normal need for law enforcement, makes the warrant and probable-cause requirement impracticable.” Although the Supreme Court has not addressed whether foreign intelligence is a “special need” that is exempt from the warrant requirement, several other courts have held that it is. For instance, the Foreign Intelligence Surveillance Court of Review held that the special needs exception applies to foreign intelligence because the purpose “goes well beyond any garden-variety law enforcement objective.” The Foreign Intelligence Surveillance Court held that this exception applies even to the acquisition of MCTs that may contain communications of or concerning US persons. In a criminal case, a federal judge rejected the defendant’s argument that obtaining information about him through Section 702 violated the warrant clause, concluding that there “is no reasonable argument the government’s need for the acquisitions is merely routine law enforcement.” In short, courts have repeatedly held that Section 702 is exempt from the warrant requirement under the special needs exception.

B. Reasonableness

Even when a warrant is not required, the Fourth Amendment protects US persons from searches and seizures that are “unreasonable.” To determine the reasonableness of a search, courts consider the “totality of the circumstances,” in which they balance “on the one hand, the degree to which it intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.” Applying this balancing test to Section 702, the government interests in national security outweigh the privacy intrusions, when considered in light of the numerous privacy safeguards that are at the core of Section 702.

To be sure, Section 702 does implicate individual privacy due to the collection of some US persons’ communications. However, it is important to remember that this collection is only incidental, and that the Fourth Amendment does not apply to the collection of communications of non-US persons located outside of the United States.

For that small subset of information that falls within Fourth Amendment protections, the NSA and other agencies are subject to extensive restrictions on the collection,
use, and retention of the data, as described in Part 2 of this paper. In a 2014 order affirming the constitutionality of Section 702, the Foreign Intelligence Surveillance Court concluded that the combined effect of the targeting and minimization procedures “has been to substantially reduce the risk that non-target information concerning United States persons or persons inside the United States will be used or disseminated and to ensure that non-target information that is subject to protection under FISA or the Fourth Amendment is not retained any longer than is reasonably necessary.”

On the other side of the reasonableness equation, the government has a strong interest in using Section 702 to meet its national security goals. The NSA has stated that Section 702 collection “is the most significant tool in the NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the U.S. and around the world.” Indeed, the Supreme Court has held that it is “obvious and unarguable that no governmental interest is more compelling than the security of the Nation.” Section 702 does not merely provide marginal or hypothetical national security protections; it is the most essential tool that the NSA has in its arsenal. Therefore, the governmental interest is quite strong.

Gathering national security information is particularly difficult when dealing with diffuse foreign terrorist groups such as Al Qaeda and ISIS (the Islamic State). The locations, identities, and tools of the foreign targets are constantly changing, requiring intelligence agencies to be agile in their collection and analysis. In its conclusion that the core Section 702 program is constitutional, the Public Civil Liberties Oversight Board reasoned that “the hostile activities of terrorist organizations and other foreign entities are prone to being geographically dispersed, long-term in their planning, conducted in foreign languages or in code, and coordinated in large part from locations outside the reach of the United States.”

Critics challenge not only the incidental collection of US person communications, but the subsequent use of this raw data by intelligence agencies. In other words, they argue, the Fourth Amendment violation occurs not only upon collection, but also when the NSA and other agencies query the data. A federal judge in Colorado recently rejected this argument, correctly concluding that accessing data that was legitimately collected does not implicate the Fourth Amendment. For instance, the court reasoned, evidence “obtained legally by one police agency may be shared with similar agencies without the need for obtaining a warrant, even if sought to be used for an entirely different purpose.” The concerns about such backdoor searches are understandable, but an objective review of the numerous restrictions and controls on tasking can only conclude that it would be not only illegal but impossible for NSA analysts to routinely use Section 702 as a mechanism to avoid the warrant requirement for searches of US persons’ communications.
Similarly misguided are challenges to the constitutionality of the upstream collection process. In *Jewel v. NSA*,\(^{108}\) civil plaintiffs allege that upstream collection is an “illegal and unconstitutional program of dragnet surveillance” and that the government has acquired communications “of practically every American who uses the phone system or the Internet . . . in an unprecedented suspicionless general search through the nation’s communications networks.”\(^{109}\) Such concerns are misplaced for two primary reasons. Even if the upstream process were to be considered a “seizure” that is subject to the Fourth Amendment, it clearly is reasonable. As Swire concluded, the upstream process is quite limited and targeted, and “there is a strong basis for rejecting the conclusion that Upstream is ‘mass surveillance,’ given its much smaller scale.”\(^{110}\) On the other side of the reasonableness equation, the upstream program provides the government with valuable intelligence. For instance, the Senate Select Committee on Intelligence concluded in 2012 that FAA authorities “have greatly increased the government’s ability to collect information and act quickly against foreign intelligence targets.”\(^{111}\)

In sum, Section 702 is crucial for intelligence agencies to gather information about ever-evolving terrorist threats. The statute contains strong privacy protections, subject to checks and balances by all three branches of government, to minimize the harm to privacy of US persons. Accordingly, courts correctly determined that, on balance, Section 702 is reasonable and therefore does not violate the Fourth Amendment.

**Conclusion**

The debate about Section 702 likely will escalate this year as Congress considers reauthorization of the FAA. Such discussion is healthy and necessary for our democratic process. This paper is intended to help inform that debate by describing how Section 702 works in practice. A complete examination of Section 702 reveals a program that is painstakingly designed to protect the privacy of US persons to the greatest extent possible while also gathering valuable intelligence for national security. Section 702 achieves the twin goals of the Constitution’s preamble: providing for the common defense and securing the blessings of liberty.

And as noted in an extensive 2013 analysis, the United States is the only nation in the world where “. . . such surveillance is subject to review by courts presided over by federal judges, with appeals possible to the US Supreme Court. The law enforcement agencies tasked with complying with FISA are required to provide regular compliance reports to the Congressional committees with responsibility over national security.”\(^{112}\) Given the Constitution’s mandate for limited but effective government, this burden is both appropriate and well imposed. It remains the gold standard in a world searching for the means to achieve the dual aims of security and the defense of individual liberties. The critics of Section 702 have failed to provide persuasive evidence that Section 702 is either unconstitutional or bad public policy, and therefore have not
made the case for modification or repeal of the law. For that reason, Congress should reauthorize Section 702 without any significant amendments.

The biggest failure surrounding Section 702 has been the lack of clear information for the public about the actual operational details. Accordingly, although we do not believe that Section 702 should be modified, it behooves the government to have a more robust public dialogue about the operations conducted under the statute. The Privacy and Civil Liberties Oversight Board’s Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act in 2014 was the first significant step toward transparency and open debate. We hope that this paper has continued to contribute to that dialogue and that the public has a better understanding about this complex and vital national intelligence program.

NOTES


3 US Constitution, Tenth Amendment.


5 “[T]he title of a statute and the heading of a section are tools available for the resolution of a doubt about the meaning of a statute.” Almendarez-Torres v. United States, 523 US 224, 234 (1998) (internal quotation marks omitted).

6 Foreign Intelligence Surveillance Act, 50 U.S.C. 1801(h)(1).


9 United States v. Bin Laden, 126 F. Supp. 2d 264 (S.D.N.Y. 2000); see also Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans’ Privacy Rights, Hearing before the H. Judiciary Comm., 110th Cong., (2007) (statement of Rep. Randy Forbes, R-VA: “The intelligence community cannot possibly know ahead of time who these terrorists will talk to. It needs to have the flexibility to monitor calls that may occur between a foreign terrorist and a person inside the United States.”).

10 At 50 USC 1805; see Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (PCLOB Report), July 2, 2014, 6.

11 PCLOB Report, 106.

12 Due to the authors’ areas of expertise—and for the sake of brevity—this paper focuses on the NSA’s implementation of Section 702.


16 Ibid.

17 Ibid., § 1881a(b)(1).

18 Ibid., § 1881a(b)(2).

19 Ibid., § 1881a(b)(3).

20 Ibid., § 1881a(b)(4).

21 Ibid., § 1881a(b)(5).

22 Ibid., § 1881a(g).

23 Ibid., § 1881a(g)(2).

24 PCLOB Report, 25.

25 50 U.S.C. 1881a(i).


27 Ibid.

28 DCLPO Report, 4.

29 PCLOB Report, 44.

30 DCLPO Report, 4.


32 PCLOB Report, 46.


34 Ibid, 37.

35 Ibid.

36 Ibid.


38 Bates FISC Opinion, 28.

39 PCLOB Report, 39.

40 Bates FISC Opinion, 36.

FISA Amendments Act Reauthorization: Hearing Before the House Permanent Select Committee on Intelligence (Joint Statement of Lisa O. Monaco, assistant attorney general for national security; John C. Inglis, deputy director, NSA; and Robert S. Litt, general counsel, Office of the Director of National Intelligence), December 8, 2011, 7.


DCLPO Report, 6.

Ibid.


Ibid., 8.

Ibid., 4–6.


See, e.g., Laura K. Donohue, “Section 702 and the Collection of International Telephone and Internet Content,” Georgetown University Law Center, 2014, 37 (“The NSA may thus query data obtained under §702 by using the names, titles, or addresses of U.S. persons, or any other information that may be related to the individual and his or her activities. Thus, for instance, if the intelligence community would like to query the data based on membership in the Council of Foreign Relations, on the grounds that such queries are likely to yield foreign intelligence information, it may now do so.”).


DCLPO Report, 7.


PCLOB Report, 57.


Ibid.

Ibid., 1.

Ibid., 6.

Ibid., 12.


Ibid.

Ibid., 7, 11.

Ibid., 7.

DCLPO Report, 4.


68 DOJ, “Semiannual Assessment of Compliance.”

69 PCLOB Report, 74.


71 PCLOB Report, 71–74.


73 Ibid.


75 PCLOB Report, 75–76.

76 Bates FISC Opinion, 5.

77 Ibid., 7.

78 Ibid., 61.

79 Ibid., 62.

80 PCLOB Report, 65.

81 Monaco, Joint Statement.


83 PCLOB Report, 108.

84 Ibid.

85 Ibid.

86 James O’Toole, “Gov’t Claims Spying Programs Stopped Plot to Bomb New York Stock Exchange,” CNN, June 18, 2013.


89 House Committee on Intelligence, “Four Declassified Examples.”

90 See US Department of Justice, “David Coleman Headley Sentenced to 35 Years in Prison for Role in India and Denmark Terror Plots,” January 24, 2013.


92 See, e.g., Electronic Frontier Foundation, “Section 702 of the Foreign Intelligence Surveillance Act (FISA): Its Illegal and Unconstitutional Use” (“The surveillance is similar to the hated British general warrants—broad and vague warrants used against American colonists—which led to the Fourth Amendment.”).

94 US Constitution, Fourth Amendment (emphasis added).


96 In Re Directives, 551 F.3d 1004, 1015 (Foreign Intelligence Surveillance Court of Review 2008).


98 In Re Directives, 551 F.3d 1004, 1011 (Foreign Intelligence Surveillance Court of Review 2008).

99 Bates FISC Opinion, 69 (“The government’s revelation that NSA acquires MCTs as part of its Section 702 upstream collection does not disturb the Court’s prior conclusion that the government is not required to obtain a warrant before conducting acquisitions under NSA’s targeting and minimization procedures.”).


101 See Maryland v. King, 133 S.Ct. 1958, 1970 (2013) (“Even if a warrant is not required, a search is not beyond Fourth Amendment scrutiny; for it must be reasonable in its scope and manner of execution.”).


103 Opinion of Judge Hogan (internal quotations omitted).


106 PCLOB Report, 92.


108 Case No. 4:08-cv-4373 (N.D. Cal.).

109 Compl. at ¶¶ 2, 9.


Jean Perkins Foundation Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The working group's output, which includes the Aegis Paper Series, is also published on the Lawfare blog channel, “Aegis: Security Policy in Depth,” in partnership with the Hoover Institution.

Jack Goldsmith and Benjamin Wittes are the cochairs of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams/national-security-technology-law-working-group.

About the Authors

Chris Inglis is the US Naval Academy’s Robert and Mary Looker Distinguished Chair for Cyber Studies. He served at NSA from 1986–2014, including service as its deputy director from 2006–2014.

Jeff Kosseff is an assistant professor of cybersecurity law at the US Naval Academy. He practiced cybersecurity law at Covington & Burling and clerked for Judge Milan D. Smith Jr. on the Ninth Circuit and Judge Leonie M. Brinkema in the Eastern District of Virginia. He is an ex-journalist and was a finalist for the Pulitzer Prize for national reporting.
It is a strange time for national security. Beginning in 2013, Edward Snowden’s leaks caused the US government to significantly reduce the scope, and increase the transparency, of its foreign intelligence surveillance, while the president urged caution and restraint in response to the extraordinary rise of the Islamic State of Iraq and the Levant (ISIL). At the same time, US communications providers sought additional reforms and reduced their cooperation with surveillance directives in important cases. Finally, anti-surveillance politicians, on the right and left of the US political spectrum, prospered as part of a burgeoning populist movement. In Western Europe, by contrast, ISIL’s rise spurred a significant and overt expansion of surveillance authorities. European governments, particularly the United Kingdom, began making increasingly strident demands for communications data from US providers. And the European Union struck down the safe-harbor regime for trans-Atlantic data sharing on the grounds that US surveillance laws do not adequately protect privacy. Despite increased transparency, as of January 2016, the immense technical and legal complexity of US surveillance law continues to challenge informed debate across all of these fronts.

In this highly charged and confused environment, Congress will soon take up the Foreign Intelligence Surveillance Act (FISA) Amendments Act (FAA), which is set to expire at the end of 2017. I make six predictions about the issues likely to dominate that legislative process. Most of those issues concern incremental change, and a range of possible outcomes well within existing legal and policy paradigms; many are explained in a 2014 report by the Privacy and Civil Liberties Oversight Board (PCLOB). All of the following issues are important: the “upstream” collection of communications about non-US persons located abroad (less than 10 percent of FAA collection, and probably unavoidable for technical reasons); US person queries of FAA data (fewer than 200 conducted by NSA in 2013, more by other agencies); statutorily required or forbidden sharing of raw FAA data with foreign partners (now dealt with through FISA Court-approved minimization procedures); the authorized purposes of FAA collection (likely not to affect existing collection very much); and NSA compliance issues (already well publicized, dealt with by the court and congressional
oversight, and unlikely to result in significant FAA amendments, but perhaps significant for the long run as the intelligence community moves data to the cloud. But they are unlikely to have a revolutionary effect on security or privacy, except perhaps in the aggregate. The one exception concerns surveillance under Executive Order 12333, which is very likely to arise in connection with FAA renewal, but is difficult to discuss at present because it is the subject of a forthcoming report from the PCLOB.

I also make predictions about political and technological trends that I think will have the biggest impact on surveillance in the longer run. These predictions are more speculative than the ones discussed above. They include increasing pressure on FISA’s “technical assistance” provisions, partly due to challenges posed by widespread and varied encryption; two gaps in US law resulting from outdated assumptions that providers will voluntarily cooperate when surveillance requests are certified as lawful but compliance is not compelled; a growing but so far unmet need for international agreements to resolve cross-border data requests; the increasing indeterminacy of location on the Internet and the resulting foundational threat to US surveillance law; the Internet of Things and “fintech,” which promise to pose a host of practical, legal, and cultural challenges; and the increasing availability of open source and social media, which creates significant problems and opportunities for US intelligence and counter-intelligence. At present, I fear that most of these issues, with the possible exception of cross-border data requests, are not very well in focus at the highest levels of the executive and legislative branches. But I believe that they should be considered soon, either in connection with FAA renewal or in a separate process, because they have the potential to cause significant change over the next several years.

Technological and political developments in the next few years will have a major impact on US national security and the law that governs it, including surveillance law. Part 1 of this paper provides historical background for the discussion of those developments, beginning with the Foreign Intelligence Surveillance Act (FISA) Amendments Act (FAA) in 2008, but focused particularly on developments since mid-2013. Part 2 presents six issues that I think are most likely to arise in connection with a legislative extension of the FAA, which is otherwise set to expire at the end of 2017. These issues are already well in focus, largely due to reports from the Privacy and Civil Liberties Oversight Board (PCLOB), and should persist absent major disruption, such as a significant terrorist attack on the United States, or perhaps the result of our 2016 presidential election. With one possible exception, concerning Executive Order 12333, these issues concern only incremental change and fit comfortably within existing legal and policy paradigms; although important, they are unlikely to have a profound effect on security or privacy. Part 3 of the paper looks further ahead. It discusses six political and technological trends that I think will have the biggest impact on surveillance in the longer run, and explains why many of them should be considered
now. These longer-term predictions are more speculative, but they concern issues that are potentially far more significant than those addressed in part 2; I hope they will be interesting even if ultimately proven wrong. Part 4 of the paper is a short conclusion.

1. Background

The predictions discussed below make sense only when considered in historical context. Issues likely to arise in connection with the FAA’s renewal in 2017, discussed in part 2, require an understanding of the statute’s enactment in 2008 and the PCLOB’s major report on the law in 2014. The longer-term issues discussed in part 3 make sense only against the turbulent backdrop of the last two or three years, beginning with the first unauthorized disclosure from Edward Snowden in June 2013 and including the rise of the Islamic State of Iraq and the Levant (ISIL).

A. The FISA Amendments Act of 2008

The FISA Amendments Act (FAA) was enacted by Congress in 2008 to address both political and technological changes from the preceding several years. Politically, Congress passed the FAA in response to unauthorized disclosures about the Terrorist Surveillance Program (TSP) ordered by President George W. Bush shortly after the September 11, 2001, attacks. Revealed by the New York Times in December 2005, the TSP allowed the National Security Agency (NSA) to acquire the contents of international communications, to or from the United States, when one communicant was suspected of being linked to al Qaeda or related terrorist organizations. Although subject to FISA, surveillance under the TSP did not comply with the statute and generated enormous controversy, centered on the president’s power to disregard statutes under Article II of the Constitution. Roughly speaking, the FAA amended FISA to authorize the TSP, although it also reiterated that, as amended, FISA is the “exclusive” means by which such surveillance can be conducted.2

Technologically, the FAA “modernized” FISA in response to changing conditions. In particular, the rise of web-based e-mail and other developments made it more difficult to determine the location of parties to an intercepted communication. With FISA’s rules so heavily dependent on knowledge of those locations, the statute became difficult to administer; it also required a high level of legal protection for surveillance of e-mail acquired from storage in the United States, even if both sender and recipient were non-US persons, located abroad, with no other connection to this country—something the drafters of FISA clearly did not contemplate in 1978. The FAA’s central innovation, in section 702 of the law, was to reduce protections for surveillance targeting non-US persons reasonably believed to be located abroad, regardless of the location of their interlocutors. Section 702 authorized such surveillance without the FISA Court making any finding about the particular person or facility (e.g., an e-mail address) being surveilled.3
The FAA profoundly affected the scope of US foreign intelligence surveillance, at least under FISA. In 2014, 92,707 persons were targeted under section 702, up from 89,138 the year before. This compares to 1,562 persons targeted in 2014 under traditional FISA and FAA §§ 703 and 704, up from 1,144 the year before. FAA surveillance covers far more persons than does traditional FISA surveillance.4

B. The Snowden Disclosures Lead the United States to Limit Surveillance

The Edward Snowden disclosures, and the government’s response to them, had a major effect on US politics and policy, igniting debates about secret law and surveillance excesses and spurring resistance to governmental surveillance from communications providers.5 The disclosures, which began in June 2013 and continued with the assistance of some very skilled journalists, were quite significant in their own right, showing that the FISA Court had authorized NSA and the Federal Bureau of Investigation (FBI) to collect the records (but not the contents) of a huge number of telephone calls, including domestic calls. The disclosures claimed to reveal many other things, as well, not all of which have been confirmed by the US government.

The disclosures arrived at a time of post-9/11 fatigue. They were preceded, in May 2013, by a speech in which the president announced that while we were still threatened by terrorism, “[t]here have been no large-scale attacks on the United States . . . our homeland is more secure” and “the threat has shifted and evolved from the one that came to our shores on 9/11.” He declared that “this war, like all wars, must end,” that America was “at a crossroads,” and that “the future of terrorism . . . [and] the scale of this threat closely resembles the types of attacks we faced before 9/11.” The president also stated in the May 2013 speech that he was “troubled by the possibility that leak investigations may chill the investigative journalism that holds government accountable,” and he had directed the attorney general to “convene a group of media organizations to hear their concerns as part of [a] review” of Department of Justice (DOJ) guidelines governing investigations that involve reporters.6 In short, the president stated shortly before the Snowden disclosures, the terrorist threat was reduced and the government should be less aggressive in response to leaks of classified information.

The president's initial response to Snowden, in June 2013, was to dismiss him as a “twenty-nine-year-old hacker” and publicly to prioritize relations with Russia and China over demands for his extradition:

[W]e've got a whole lot of business that we do with China and Russia. And I'm not going to have one case of a suspect who we're trying to extradite suddenly being elevated to the point where I've got to start doing wheeling and dealing and trading on a whole host of other issues simply to get a guy extradited, so that he can face the Justice system here in the United States . . . And I'm sure there will be a made-for-TV movie somewhere down
the line . . . But one last thing . . . no, I’m not going to be scrambling jets to get a twenty-nine-year-old hacker.7

By August 2013, the government had affirmatively embraced the demand for greater scrutiny generated by the disclosures, with the president asserting that he had in fact “called for a thorough review of our surveillance operations before Mr. Snowden made these leaks.” The president explained that he had “never made claims that all the surveillance technologies that have developed since the time some of these laws had been put in place somehow didn’t require potentially some additional reforms.” In fact, he stated, “That’s exactly what I called for” in the May 2013 speech.8 And while “Mr. Snowden’s leaks triggered a much more rapid and passionate response than would have been the case if I had simply appointed [a] review board to go through, and I had sat down with Congress and we had worked this thing through . . . I actually think we would have gotten to the same place.”9

As those reviews were unfolding, US communications providers continued to push for additional reforms. One of the most prominent and thoughtful advocates in that area was Microsoft, which, through its then-General Counsel Brad Smith, identified a “technology trust deficit” due to the Snowden disclosures and outlined the “unfinished business” required to close it.10 In part, at least, Microsoft was understandably concerned that, in the absence of visible reform, its European counterparts were enjoying a competitive advantage in the form of perceived relative immunity from surveillance. As Smith put it, “people have real questions and concerns about how their data are protected. These concerns have real implications for cloud adoption. After all, people won’t use technology they don’t trust. We need to strike a better balance between privacy and national security to restore trust and uphold our fundamental liberties.”11

One of the key points, Smith explained, was limiting cross-border data requests: “We’re concerned about governmental attempts to use search warrants to force companies to turn over the contents of non-US customer communications that are stored exclusively outside the United States.”12 Microsoft ultimately chose to resist a directive issued under the US Stored Communications Act by the DOJ to produce e-mail of a suspected drug dealer on the grounds that the e-mail was stored in Ireland, rather than in the United States.13 The introduction to its brief in the Second Circuit used informal language capable of being understood by a broader audience than the three-judge panel hearing the case.14

By the fall of 2013, the government had made a bold decision to decrease the scope, and increase the transparency, of US foreign intelligence surveillance, recalibrating the balance between security and privacy in favor of the latter. In October, Lisa Monaco, the president’s counterterrorism adviser, wrote in USA Today of the administration’s desire to ensure that “privacy and civil liberties are appropriately protected,” promised
“even greater focus to ensuring that we are balancing our security needs with . . . privacy concerns,” and committed to “ensure we are collecting information because we need it and not just because we can.” The editorial, which noted with approval the ongoing review of the FAA by the PCLOB, was a powerful statement of the administration’s commitment to curtail perceived foreign intelligence surveillance excesses and to emphasize privacy—i.e., to do less surveillance than legally permitted based on policy preferences.

This approach found formal articulation in Presidential Policy Directive-28 (PPD-28) and a speech given by President Obama at the Department of Justice in January 2014. In essence, the government committed to (1) introduce outside advocates into the Foreign Intelligence Surveillance Court (FISC), which was later accomplished in the USA Freedom Act of 2015, (2) adopt more stringent minimization procedures for US person information incidentally collected under FAA § 702, and (3) end bulk collection of telephony metadata, also accomplished in the USA Freedom Act.

It also committed to take what the president termed “the unprecedented step” of adding new protections for non-US persons, including requirements that intelligence surveillance “take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they may reside” and recognize the “legitimate privacy and civil liberties concerns of . . . citizens of other nations.” Under PPD-28, “[p]rivacy and civil liberties shall be integral considerations in the planning of US signals intelligence activities,” including for foreign persons. This makes a stark contrast with the language of Executive Order (EO) 12333, in force since the Reagan administration, which focuses almost exclusively on the privacy interests of US persons. Implementation of PPD-28 remains ongoing as of this writing, but many steps have apparently been taken to limit surveillance and protect foreigners’ privacy rights and dignity. One recent paper identified at least two dozen measures undertaken since 2013 to reform surveillance laws and programs. In the fall of 2015, the administration also decided not to support legislation requiring providers to retain access to encrypted communications that they transmit. There is no question but that President Obama and his senior national security advisers have significantly reduced the scope, and increased the transparency, of US foreign intelligence surveillance since mid-2013: it may be their chief legacy in this area.

While the White House was curtailing surveillance and providers were pushing for even more curtailment, anti-surveillance political positions, tied to populism on both the right and the left, were on the rise in the United States. The shift was especially visible in the Republican Party, which witnessed the advent of the Tea Party soon after President Obama’s election and, at this writing, features Donald Trump as its leading presidential candidate. Trump is trailed closely by Senator Ted Cruz, despite Cruz’s
anti-surveillance positions,\textsuperscript{25} for which he has been criticized by other Republican candidates.\textsuperscript{26} Few observers during the administration of the last Republican president, George W. Bush, would have predicted this state of affairs. On the Democratic side, Bernie Sanders continues at this writing to enjoy strong standing in his race with Hillary Clinton, despite being one of only sixty-seven members of Congress to have voted against the USA Patriot Act in 2001 (and again in 2011).\textsuperscript{27} Of course, it can be difficult to separate the politics of surveillance from broader political trends, and the range of US public opinion on surveillance surely derives in some part from the recent positions of the executive branch, which is often the proponent of more rather than less surveillance. Whatever the causes, however, there is no question but that American politics has over the past few years shifted to embrace more anti-surveillance positions (although the attacks in Paris and San Bernardino have provided some recent counterweight to that shift).

\textbf{C. ISIL’s Rise Leads Europe to Increase Surveillance}

During this same period, while the United States was restricting its foreign intelligence surveillance, European governments were expanding their surveillance authorities, in response to growing concerns about ISIL and other terrorist groups. During 2013 and 2014, ISIL rose to power, taking credit for attacks killing eighty-eight people in Iraq in January 2013,\textsuperscript{28} announcing its merger with the Syrian Jabhat al-Nusra group in April,\textsuperscript{29} orchestrating a large prison break in Iraq in July,\textsuperscript{30} and capturing Syrian oil fields in November.\textsuperscript{31} In 2014, ISIL took Fallujah in January,\textsuperscript{32} directed or inspired an attack on a Jewish museum in Belgium in May,\textsuperscript{33} took Mosul and announced a caliphate in June,\textsuperscript{34} and released video of the execution of two US journalists in early September\textsuperscript{35} and of a UK humanitarian worker later that month.\textsuperscript{36} Although the president in early 2014 seemed to dismiss ISIL as unimportant,\textsuperscript{37} by later in the year he made clear that ISIL was a significant threat, at least in the Middle East,\textsuperscript{38} and focused, at least initially, on regional containment.\textsuperscript{39} By late 2015, ISIL had probably recruited at least 4,500 Westerners to its cause, many of them with European passports, and some of whom returned to Europe to conduct attacks.\textsuperscript{40}

At the same time, global instability was rising, and failed states like Yemen and Libya created more safe havens for terrorists. From 2013–2015, al Qaeda in the Arabian Peninsula (AQAP) took advantage of instability and proxy fighting between Iran and Saudi Arabia in Yemen. In December 2013, for example, AQAP attacked the Yemeni Ministry of Defense, killing fifty-six people; in September 2014, Houthi rebels took control of Sanaa; in March 2015, President Hadi was forced to flee the country (and later returned); and by April 2015, AQAP had seized the fifth-largest Yemeni city (and “emptied its bank and prison”), an oil terminal, a military base, and an airport in southern Yemen.\textsuperscript{41} AQAP also claimed credit for the January 2015 attack on \textit{Charlie Hebdo} in Paris.\textsuperscript{42} During this period, Libya also essentially fell into civil war; the United
Nations withdrew in July of that year. By 2015, ISIL had a well-established presence and was reportedly using Libya as a gateway to Europe.43

Witnessing these developments in 2014 and 2015, in contrast to the United States, European countries developed new and expanded surveillance authorities.44 The Council of Europe’s Commissioner for Human Rights aptly summarized the situation in October 2015, recounting efforts to expand surveillance authority in France, Germany, Austria, the Netherlands, and Finland (and probably having in mind similar efforts in the United Kingdom and Canada):

> When Edward Snowden disclosed details of America’s huge surveillance program two years ago, many in Europe thought that the response would be increased transparency and stronger oversight of security services. European countries, however, are moving in the opposite direction. Instead of more public scrutiny, we are getting more snooping.45

Further expansions of European surveillance are likely—such as the UK’s remarkable draft Investigatory Powers bill, discussed below.46

At this writing, in the aftermath of the Paris and San Bernardino attacks in late 2015, further attacks in the West from ISIL and other terrorist groups seem almost inevitable.47 Indeed, ISIL’s ascendency represents a significant change in paradigm due to several factors, chief among them that an international terrorist group has now become essentially a state actor, with control of significant territory, large sums of money and income (measured in the hundreds of millions or billions of dollars), and a worldwide strategy that includes a growing focus on external operations and an expanding cadre of geographically dispersed affiliates and allies.48 As such, particularly due to its oil revenue and thousands of Western recruits, ISIL clearly has far greater resources in materiel and personnel than groups like al Qaeda.49 Even if ISIL loses control of much of its territory, it is quite unlike any recent international terrorist group (and even if ultimately degraded or defeated, it will leave the Middle East more unstable).50 It is not hard to imagine ISIL and the West moving into a kind of relatively limited war, with the West bombing but not sending significant numbers of ground troops to ISIL-held territory, and ISIL directing, sponsoring, or inspiring terrorist attacks against the West, at or above the scale seen in Paris and San Bernardino.51 The wild card in that state of affairs, however, will be whether ISIL is willing and able to engage in strategic terrorism, perhaps involving attacks with weapons of mass destruction.52

2. Predictions Concerning Renewal of the FAA

As noted above, the FAA will expire, unless extended, in December 2017. Between now and then, Congress will very likely renew the statute, but only after extensive legislative debate. Many of the issues likely to arise in that debate derive from the PCLOB’s report
§ 702. The report generally found the section 702 surveillance program to be valuable, lawful, and appropriate:

Overall, the Board has found that the information the program collects has been valuable and effective in protecting the nation’s security and producing useful foreign intelligence. The program has operated under a statute that was publicly debated, and the text of the statute outlines the basic structure of the program. Operation of the Section 702 program has been subject to judicial oversight and extensive internal supervision, and the Board has found no evidence of intentional abuse.53

Based in part on this assessment, and the support for the statute from members of Congress in both political parties, there is very little doubt that the FAA will be renewed, rather than allowed to sunset, when the time comes at the end of 2017.

However, the PCLOB report also recommended several reforms based on its view that “certain aspects of the Section 702 program push the program close to the line of constitutional reasonableness. Such aspects include the unknown and potentially large scope of the incidental collection of US persons’ communications, the use of ‘about’ collection to acquire Internet communications that are neither to nor from the target of surveillance, and the use of queries to search for the communications of specific US persons within the information that has been collected.”54 Between now and the end of 2017, I think the following issues will arise in connection with the FAA’s renewal, many of them based on the PCLOB’s recommendations.55 These predictions are not necessarily normative.

A. “Upstream” and “About” Collection

The first question likely to arise in connection with FAA renewal concerns “upstream” collection under section 702, including collection of communications “about,” rather than to or from, a surveillance target. As I have explained elsewhere, collection under section 702 “occurs not only directly from Internet service providers (ISPs), but also at certain ‘upstream’ locations, like international switches or other backbone facilities, as communications transit through them.”56 In other words, section 702 surveillance comes in two varieties: “upstream” collection at the Internet backbone facilities and “downstream” or “PRISM” collection from ISPs or other communications providers. Approximately 90 percent of NSA’s FAA § 702 Internet collection is downstream/PRISM collection; less than 10 percent involves upstream.57

The “upstream” facilities involved in section 702 surveillance carry huge numbers of communications, including some domestic communications, the metadata and contents of which are scanned to determine whether they contain a targeted selector, such as an e-mail address. That is, NSA collects upstream not only the messages sent to and from
a target’s e-mail address, like BadGuy@ISP.com, but also messages sent between non-targets that mention BadGuy@ISP.com (the e-mail address, not merely the name).58 Indeed, “[b]ecause of the manner in which the NSA conducts upstream collection, and the limits of its current technology, the NSA cannot completely eliminate ‘about’ communications from its collection without also eliminating a significant portion of the ‘to/from’ communications that it seeks.”59

As an unavoidable byproduct of “to/from” collection at the upstream locations, “about” collection can be defended under two publicly available FISA Court decisions from 2011. In those decisions, the court addressed another unavoidable aspect of upstream collection—NSA’s acquisition of entire Internet “transactions,” which may contain multiple communications, including some communications that are outside the scope of section 702, but which have been bundled together by ISPs or other private-sector companies for business reasons. If an e-mail to or from a lawful surveillance target is bundled in a single transaction with other, unrelated communications, from other individuals, NSA may not be able to avoid acquiring all of the communications in the transaction, including the unrelated ones. The FISA Court initially struck down NSA’s minimization procedures governing that inevitable over-collection, but later upheld modified procedures that imposed more stringent limits on retention of the unrelated content.60 The court reached that result despite the large scale of the over-collection: NSA annually acquires “tens of thousands of wholly domestic communications, and tens of thousands of non-target communications of persons who have little or no relationship to the target but who are protected under the Fourth Amendment.”61 The PCLOB likewise found “about” collection tolerable, based primarily on its inevitability as part of “to/from” upstream collection.62

In connection with FAA renewal, I expect additional focus on the inevitability, legality, and desirability of “about” collection. The first questions likely to arise will be whether NSA now has the technical ability to parse “about” collection and “to/from” collection, and if not, whether the agency is trying to develop such an ability. (A related question will be whether NSA has developed, or is trying to develop, the ability to separate one individual communication from another within an Internet transaction.) This will be a very technical conversation, and may need to be conducted in closed session. It seems unlikely that NSA has developed such an ability since 2014, in part because one of the main challenges to doing so is the constantly changing nature of commercial Internet protocols, but the questions will need to be asked and answered.63 Given the state of confusion about the mechanics and other details of upstream collection that persist, it also may be helpful if the legislative debates can further illuminate how the collection works, without compromising national security.

Either way, and especially if “about” collection is no longer inevitable, I expect Congress to consider whether it should be permitted or forbidden by statute (perhaps
against a Fourth Amendment backdrop). Much of the prior focus on “about” collection has concerned retention of the inevitably over-collected data. In connection with FAA renewal, however, I think that Congress may focus more intensively on the collection itself—i.e., on the fact that “NSA’s machines scan the contents of all of the communications passing through the collection point, and the presence of the selector . . . that justifies the collection is not known until after the scanning is complete.” This purely legal issue, arguably involving the result of a search being used to justify the search, is both interesting and challenging.

Finally, if “about” collection is retained in the statute, Congress may ask whether it should be expanded or restricted. One possibility for expansion might be to permit “about” collection both upstream and downstream—e.g., allowing the government to direct ISPs to scan their servers for any stored e-mail mentioning BadGuy@ISP.com, as well as e-mails to or from that e-mail address. Even if it were technically feasible, this seems most unlikely. As discussed in greater detail in part 1, the Obama administration since 2013 has consistently supported less surveillance, rather than more, and I doubt that it will push for an expansion here. Nor is the new president likely to push for this after January 2017—at least absent a disruptive event of the sort described in the first paragraph of this paper. Without support from the executive branch, increased “about” collection seems very unlikely, especially given the legal questions it raises. As to further restrictions, there are always a variety of incremental changes Congress could try to legislate, particularly in the area of minimization—e.g., a one-year retention period, rather than the two-year period approved by the FISA Court in 2011.

B. Queries

A second question likely to arise in connection with FAA renewal is the government’s authority to query un-minimized FAA § 702 data with US person identifiers, or in other ways designed to return information about US persons. Attentive members of the news media have already identified querying as one of the most likely issues to be addressed. To provide a sense of scale, according to the PCLOB, in 2013, “NSA approved 198 US person identifiers to be used as content query terms” in queries of FAA § 702 data.

Querying raises concerns primarily when US persons are not surveillance targets but have their communications acquired incidentally, during collection targeting others. Roughly speaking, US persons’ communications could be collected incidentally under section 702 in any of three ways, two of which apply only to upstream collection: the US person could be the interlocutor of a target, which is inherent in any form of surveillance (including law-enforcement surveillance) that captures both sides of an intercepted conversation; the US person’s communication could be acquired upstream as part of “about” collection concerning a targeted selector; or the US person’s
communication could be acquired upstream as part of the same Internet “transaction” as a targeted communication.

Given these three possibilities, querying upstream (rather than downstream) data with US person identifiers is plainly more controversial. But NSA’s 2014 minimization procedures do not permit it, and neither the FBI nor the CIA has access to un-minimized upstream data.69 Legislative intervention to address a hypothetical concern seems relatively unlikely, unless it is in connection with broader changes to upstream collection. But it would be possible if Congress does not want to leave the matter to the other two branches of government.

With respect to downstream (PRISM) data, the PCLOB recommended that NSA and CIA minimization procedures “permit the agencies to query collected section 702 data for foreign intelligence purposes using US person identifiers only if the query is based upon a statement of facts showing that it is reasonably likely to return foreign intelligence information as defined in FISA.” The PCLOB recommended that the “NSA and CIA should develop written guidance for agents and analysts as to what information and documentation is needed to meet this standard, including specific examples.”70 It appears that the NSA and CIA have implemented this recommendation with the FISA Court’s approval,71 and it is not clear that Congress will demand more by statute.

Two members of the PCLOB recommended in addition that “[e]ach US person identifier should be submitted to the FISA court for approval before the identifier may be used to query data collected under section 702, for a foreign intelligence purpose, other than in exigent circumstances or where otherwise required by law.”72 It appears that this recommendation has not been implemented, so it likely will be discussed. It has an analog of sorts in the USA Freedom Act of 2015, which modified the prior program of bulk collection of telephony metadata in several ways, including by requiring the FISC’s approval of selectors used for searches of providers’ call detail records.73 One possible compromise would be to require FISC approval only for queries of upstream data, which has the highest risk of involving unrelated US person communications, although that would be an expansion of existing upstream querying authority.

A related question concerns the FBI’s ability to query un-minimized FAA § 702 data for evidence of a crime, particularly a crime not related to foreign intelligence.74 The government reported in 2015 that “consistent with the recommendation of the Privacy and Civil Liberties Oversight Board, information acquired under section 702 about a US person will not be introduced as evidence against that person in any criminal proceeding except (1) with the approval of the Attorney General, and (2) in criminal cases with national security implications or certain other serious crimes. This change will ensure that, if the Department of Justice decides to use information
acquired under section 702 about a US person in a criminal case, it will do so only for national security purposes or in prosecuting the most serious crimes."\textsuperscript{75} The FBI has reported that “it is extremely unlikely that an agent or analyst who is conducting an assessment of a non-national security crime would get a responsive result from the query against the section 702--acquired data."\textsuperscript{76} Two PCLOB members stated that they were “unaware of any instance in which a database query in an investigation of a non-foreign intelligence crime resulted in a ‘hit’ on 702 information, much less a situation in which such information was used to further such an investigation or prosecution."\textsuperscript{77} Recent reporting on ISIL recruits in Europe suggests this may not always be the case, however, so the issue may be worth exploring further.\textsuperscript{78}

Underlying this debate is an interesting, although somewhat technical, question of whether querying should be seen as a separate, stand-alone Fourth Amendment event, such that it must satisfy constitutional requirements on its own, or whether it is instead best seen as part of the overall Fourth Amendment event described by the FAA, which includes but is not limited to acquisition, retention, querying, and dissemination of information. The former seems to have some support in the historical position of the government going back to the 1980s,\textsuperscript{79} but the latter is at least arguably more consistent with more recent authority, particularly in the context of FAA § 702.\textsuperscript{80} It seems unlikely that Congress will tackle this technical, constitutional question in a focused manner.

\textbf{C. International Data Sharing}

At least two issues of international data sharing may arise in connection with FAA renewal. First, especially in the wake of the November 2015 Paris attacks, there will probably be some members of Congress who push for more sharing of un-minimized data with foreign partners, including but perhaps not limited to Five Eyes (France is not part of the Five Eyes). Un-minimized downstream (PRISM) data collected by NSA under FAA § 702 is routinely shared with the CIA and FBI; the argument will be that it should likewise be routinely shared with British, Canadian, or other allied intelligence services, who may be able to identify foreign intelligence information that US analysts would miss and who can be trusted to apply court-approved minimization procedures after training by NSA or the Department of Justice (DOJ). Other members of Congress, however, will raise concerns about such sharing with foreign partners, particularly because it will include incidentally collected information about US persons. Under section 8 of NSA’s 2014 standard FAA § 702 minimization procedures, the agency may share un-minimized information only for technical or linguistic assistance, subject to strict limits on analytic use by the foreign government.\textsuperscript{81} Of course, deviations from the standard procedures, allowing for more sharing in particular cases or settings, may be permitted if proposed by the government and approved on a case-by-case basis by the FISA Court.
Second, we may see discussion of data-sharing between the United States and the European Union, including the Schrems decision striking down the Data Transfer Safe Harbor, which was premised in part on European dissatisfaction with the FAA and other US surveillance practices. The Safe Harbor issue will probably be resolved before 2017; but if it is not, it will surely figure in the debates over renewal of the FAA. One interesting aspect of the Safe Harbor debates, and some related debates about cross-border data requests discussed in part 3, is the extent to which European surveillance practices may be brought to light. There is certainly an argument that European intelligence collection is conducted with far less oversight and far fewer restrictions than US collection, and it is quite clear that data is legally safest from US governmental snooping when stored here rather than abroad.

D. Technical Issues and Compliance

A fourth issue that is likely to arise needs only brief mention, even though it could be significant to the legislative debates: NSA compliance problems. These problems have been well-documented in several areas and will likely be reviewed again in connection with FAA renewal. As the PCLOB noted, “[a] failure to implement the acquisition in a manner that reasonably limits the collection to the authorized purpose of the section 702 certifications can, and has, led to incidents of noncompliance with the minimization procedures that have been reported to the FISC and Congress.”84 As it ingests more and more data, the government will be more and more dependent on data-tagging at (or just after) acquisition, in order to effectuate subsequent controls governing access, use (e.g., querying), purge, and dissemination rules and requirements.85

The compliance regime will be even more complex to administer as the intelligence community continues work on its Integrated Intelligence Enterprise (IC-ITE)—referred to by the Office of the Director of National Intelligence (ODNI) as “the largest IT transformation in the history of the intelligence community”—which would create shared cloud-type servers for multiple agencies, each of which may have different access rights and requirements.86 If the data-tagging efforts fail, the inter-agency compliance regime that rests atop it will likewise fail. Congress will likely want to explore this further in connection with FAA renewal because it is at the core of the government’s ability to comply with minimization procedures and other limits, and also critical to its ability to limit access to information and mitigate the insider threat of further unauthorized disclosures.

E. Purpose of Collection

The FAA authorizes collection only when the government has at least a significant purpose to acquire “foreign intelligence information.” That term is defined in two ways in the statute. The first part of the definition concerns what is typically referred to as
“protective” foreign intelligence, including information necessary or relevant to the ability of the United States to protect against attack, sabotage, espionage, international terrorism, or the proliferation of weapons of mass destruction by a foreign power. The second part defines “affirmative” foreign intelligence, including information concerning non-US persons that relates to the national defense or security of the United States or the conduct of the foreign affairs of the United States, but only insofar as that information concerns a foreign power or foreign territory. The PCLOB reported that the FISC has approved certifications authorizing collection under section 702 for “categories of information” that satisfy the definition of foreign intelligence information, including “information concerning international terrorism and other topics, such as the acquisition of weapons of mass destruction.” Particularly in light of PPD-28 and related statements from the Obama administration emphasizing the dignity and privacy interests of non-US persons, Congress can be expected to debate whether the FAA should continue to authorize collection of “affirmative” foreign intelligence as well as “protective” foreign intelligence.

F. Executive Order 12333

As of this writing, the PCLOB is working on a report on surveillance under Executive Order 12333, the main presidential-level directive governing the US intelligence community. Depending on the timing and nature of the report, legislative debate over FAA renewal will almost surely address surveillance under EO 12333. It seems all but inevitable that at least some members of the PCLOB will recommend a variety of measures designed to constrain EO 12333 surveillance and to make it more like surveillance under FAA § 702. Such changes might also include provisions akin to those in FAA § 702 authorizing compelled assistance from communications providers in connection with EO 12333 surveillance, although this might be opposed by US providers on the ground that it would exacerbate the perceived disparity between them and their foreign competitors in protecting privacy. Changes to the executive order in light of PPD-28 may also be called for by the PCLOB, because the two documents are significantly in tension with respect to their views concerning the privacy interests of non-US persons. It seems very probable that the Obama administration will support at least some of these measures; the next president’s views are less certain. Perhaps the debate will go even further, and address whether Congress should enact comprehensive legislation governing all intelligence surveillance, or even charter statutes for all intelligence activities, as was considered in the 1970s. Of all the issues reviewed here that might arise in connection with FAA renewal, this is the only one that I believe has the potential to result in really profound change to the status quo.

3. Longer-Term Predictions

Although I expect the FAA debate to unfold roughly as described above (absent a major disruption), it remains a very unsettled time for US national security in
general and foreign intelligence surveillance in particular. As discussed in part 1, the Snowden disclosures and the US government’s reaction to those disclosures, coupled with increasing global instability and the rise of ISIL, have created a strange political environment both here and abroad. In that environment, the increasing and varied use of encryption, the growing fragmentation and indeterminacy of location in communications networks, communications providers’ new reluctance to assist the government with surveillance requests, the expanding Internet of Things, and the explosion of open source and social media data all portend profound change. In this part of the paper, I describe these emerging political and technological developments and predict effects over the next several years. In general, the developments are presented in order, beginning with those I perceive as most likely to have the most significant, most identifiable impact in the nearest term.

A. Encryption and “Technical Assistance”

In the United States, at least, the November 2015 Paris attacks seemed to reopen a debate that previously had closed, concerning whether the government should enjoy “exceptional access” to encrypted communications and data so that it can effectuate surveillance directives.91 There is a recent and well-developed literature on that topic,92 addressing both technical and policy issues, and no need to reproduce it here. But there are two related points worth making, both of which directly concern FISA, the FAA, and foreign intelligence surveillance in general.

First, if present trends continue, in the absence of a new statute dealing expressly with encryption, there will be increasing pressure on the “technical assistance” requirements in FISA (and the Wiretap Act). Under several provisions of FISA, including the FAA, a telecommunications provider or other party may be directed to provide “technical assistance” (or simply “assistance”) to the government in implementing the authorized activity. For example, a traditional FISA order for electronic surveillance “shall direct” that

upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person . . . furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance.93

The FAA has similar language in two of its three main provisions, although it applies only to electronic communication service providers, not to custodians, landlords or other persons.94 For section 702 surveillance, targeting non-US persons
reasonably believed to be abroad, the attorney general and the director of national intelligence (DNI)

... may direct, in writing, an electronic communication service provider to... immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition.95

Indeed, section 702 surveillance may only be conducted with the assistance of a provider.96 Compelled assistance is also part of FAA § 703, which governs targeting of US persons reasonably believed to be located abroad where the surveillance would otherwise require a traditional FISA court order and is conducted in the United States.97 But there is no provision for compelled assistance in FAA § 704, which governs targeting of US persons abroad when the surveillance would not otherwise require an order and is conducted abroad: under section 704, the FISA Court does not even have “jurisdiction to review the means by which an acquisition under this section may be conducted,” let alone issue an assistance order.98 Section 704 is accomplished by the government acting alone, or with voluntary cooperation from others.

The Supreme Court addressed “technical assistance” in 1977 in US v. New York Tel. Co.,99 where it held that the All Writs Act, which allows federal courts to “issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law,”100 could be used to compel a telephone company to assist with installation of a pen register. The pen register itself was authorized under Federal Rule of Criminal Procedure 41, but the court nonetheless noted the technical assistance provision in the Wiretap Act, explaining that in light of the act’s “direct command to federal courts to compel, upon request, any assistance necessary to accomplish an electronic interception, it would be remarkable if Congress thought it beyond the power of the federal courts to exercise, where required, a discretionary authority to order telephone companies to assist in the installation and operation of pen registers, which accomplish a far lesser invasion of privacy.”101

As encryption becomes more common, both in transmission and in devices, the government may seek more in the way of technical assistance from providers or others to defeat that encryption.102 In the Eastern District of New York, the Department of Justice and Apple are at this writing engaged in a dispute about whether Apple can be compelled to unlock an iPhone for which there is a federal search warrant. The government is relying on the All Writs Act and New York Tel. Co., and Apple is claiming that the All Writs Act does not apply based on CALEA,103 a 1994 statute that requires telecommunications providers to maintain their networks in certain ways that allow for
wiretapping but does not apply to stored data on a handset. Apple’s main argument is that the All Writs Act cannot be used to compel what Congress declined to address in CALEA—i.e., that CALEA occupies the field of compelled assistance.104

There is very little publicly available law on the limits of “technical assistance” in FISA. A divided panel of the Ninth Circuit held that the Wiretap Act could not be used to compel assistance with a wiretap in ways that entirely disabled the communications system for the particular customer involved in the surveillance. The majority concluded that disabling the system was inconsistent with the statutory command that technical assistance be provided “in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier . . . is providing that target of electronic surveillance”:

... the “a minimum of interference” requirement certainly allows for some level of interference with customers’ service in the conducting of surveillance. We need not decide precisely how much interference is permitted. “A minimum of interference” at least precludes total incapacitation of a service while interception is in progress. Put another way, eavesdropping is not performed with “a minimum of interference” if a service is completely shut down as a result of the surveillance.105

The dissenting judge, Richard Tallman, concluded that the “minimum of interference” standard governed the manner in which technical assistance must be provided, not whether it must be provided. For Judge Tallman, it was enough that “the Company complied with the challenged order in the way least likely to interfere with its subscriber’s services” and that “the only method of executing the intercept order in this case” was the one used, because “even the complete shutdown of a service [for a particular user] can represent the minimum interference, so long as no lesser amount of interference could satisfy the intercept order.”106 Judge Tallman’s dissent is noteworthy, in part because he is a member of the Foreign Intelligence Surveillance Court of Review, with a term of service expiring in 2021.107

In general, the “technical assistance” requirement admits of a balancing of the provider’s costs and burdens on the one hand against governmental need and alternatives on the other. It is therefore notable that in its case in New York, one of the burdens described by Apple is the following:

... public sensitivity to issues regarding digital privacy and security is at an unprecedented level. This is true not only with respect to illegal hacking by criminals but also in the area of government access—both disclosed and covert. Apple has taken a leadership role in the protection of its customers’ personal data against any form of improper access. Forcing Apple to extract data in this case, absent clear legal authority to do so, could threaten the trust between Apple and its customers and substantially tarnish the Apple brand. This
reputational harm could have a longer term economic impact beyond the mere cost of performing the single extraction at issue.\textsuperscript{108}

Taken to its logical conclusion, this might mean that a provider could create its own undue burden by strongly and publicly opposing assistance with governmental surveillance.

A second issue concerns the difference between providing technical assistance and configuring communications networks to facilitate surveillance. As discussed above, the former is required by FISA and the Wiretap Act, while the latter is required in limited circumstances by CALEA. Absent an amendment to any of these laws, there will be at least two critical questions where CALEA by its terms does not apply. First, as a legal matter, what is the distinction between configuring “equipment, facilities, or services” under CALEA and providing “technical assistance” under FISA and the Wiretap Act? For example, is it “technical assistance” for a provider to push down to a user’s phone, with or perhaps without the user’s knowledge, a software patch or program that facilitates surveillance (e.g., by covertly disabling encryption)? Does the answer change if the software (code) is written by the government rather than the provider itself? These issues may matter more today than they did in the era in which the Wiretap Act, FISA, and CALEA were enacted, because in at least some settings, software has become more important than hardware for facilitating surveillance. Second, to what extent can uncooperative providers configure their “equipment, facilities, or services” to thwart surveillance without depriving themselves of functionality desired by themselves or their customers? For example, will providers be willing to eschew any capacity to add an invisible third party to communications on their networks? If not, the capacity may be available as technical assistance for governmental surveillance. There is enough uncertainty on these issues that Congress may want to consider some clarification.

Other countries are tackling the issue now. In the United Kingdom, for example, the November 2015 draft of a new Investigatory Powers Act is quite explicit. It deals directly with what the British call “equipment interference,” which “allows the security and intelligence agencies, law enforcement and the armed forces to interfere with electronic equipment such as computers and smartphones in order to obtain data, such as communications from a device.” Equipment interference “encompasses a wide range of activity from remote access to computers to downloading covertly the contents of a mobile phone during a search.” It is necessary to avoid “the loss of intelligence that may no longer be obtained through other techniques, such as interception, as a result of sophisticated encryption.”\textsuperscript{109}

In case the UK bill is not clear enough on its face, the Electronic Frontier Foundation (EFF) asserts in public comments on the bill that the “common term for ‘equipment interference’ is ‘hacking’: breaking into and remotely controlling devices. It permits third
parties to transform a general-purpose device such as a modern smartphone, laptop, or desktop computer into a surveillance machine.”\textsuperscript{110} Although the term “‘equipment interference’ carries with it the implication that the power is restricted to impeding normal equipment operations,” EFF asserts, it “may also include adding unexpected new functionality to a device,” such as surveillance functionality.\textsuperscript{111} The EFF comments further argue that under the UK’s bill, third parties can be compelled to assist in hacking: “a warrant might be served on British Telecom, for example, to compel them to interfere with a device they neither own nor legally control, such as a phone using their network in order to access its voicemail.”\textsuperscript{112} Indeed, EFF asserts, “[u]nder the proposed law, a British company could be compelled to distribute a [software] update in order to facilitate the execution of an equipment interference warrant and ordered to refrain from notifying their customers . . . Such an update could be targeted at an individual, an organisation, or many organisations related to a single investigation.”\textsuperscript{113} The draft IP bill also authorizes bulk collection and (in certain circumstances) equipment interference in bulk.\textsuperscript{114} Whether or not the EFF comments are completely accurate in their characterization of the UK bill, they clearly illustrate the range of issues and conduct that might be authorized or prohibited by new surveillance laws.

It would be worthwhile for Congress to consider the limits of “technical assistance” in the context of equipment interference and other techniques that might be used to defeat at least some forms of encryption. This would include legal issues as well as technical ones, depending on whether the interference action is to be accomplished by the government or the provider, and of course the relevant policy questions.

\textbf{B. Provider Cooperation}

Ironically, the government’s increasing reliance on “technical assistance” from providers will occur at a time when US providers are less inclined than they once were to cooperate with surveillance requests.\textsuperscript{115} American law, however, still assumes that providers will cooperate, at least in some cases, even when not required to do so. Coupled with the increasing storage of data abroad,\textsuperscript{116} this creates at least two significant surveillance gaps that Congress should examine.

First, whatever the merits of Microsoft’s argument in the case of the drug dealer discussed above (part 1), there is no real doubt that it would prevail if the government sought e-mail stored in Ireland under traditional FISA. That is because traditional FISA searches may only occur in the United States, and traditional FISA electronic surveillance applies to stored data only when the surveillance device is used in the United States.\textsuperscript{117} Indeed, this was part of the assessment underlying the decision by Congress to enact the FAA in 2008.\textsuperscript{118} When it comes to US persons, however, the FAA is no help in reaching e-mail stored abroad. As discussed above, section 702 does not apply to US persons; section 703 applies only when the surveillance is conducted
in the United States; and section 704 has no “technical assistance” or compelled
production provisions at all. In short, unless the provider voluntarily repatriates the
US person’s stored e-mail, its production cannot be compelled under FISA.

The same is true if the target of the surveillance or search is a non-US person located
in the United States: his e-mail in Ireland is beyond the reach of traditional FISA,
as discussed above, and his location in this country puts him outside the reach
of FAA § 702. In sum, then, when e-mail is stored abroad, neither traditional FISA
nor the FAA can be used to compel provider assistance if the target is either a US person
(in any location) or a person (of any nationality) located in the United States. This is
a potentially significant shortfall in FISA, particularly as data become more and more
mobile, subject to being stored in any location, or even fragmented and stored in
several locations at once.

A second possible gap concerns the situation in which all parties to a phone call or
e-mail are located abroad, but the communication transits a wire in the United States.
In that situation, it has long been the case that the US government generally cannot
get a FISA Court order to compel the assistance of the provider that owns the wire.119
Unless it has a valid target under FAA § 702—i.e., a non-US person located abroad—the
most the government can do is assure the provider, in the form of a certification from
the attorney general, that it may lawfully cooperate, but not that it must do so.120 If a
provider refuses, the government has very little recourse. Today, with providers more
recalcitrant than they have been, based on their public statements, voluntary assistance
may not be forthcoming.

Congress should consider these questions. Some observers will instinctively approve
of any change that reduces collection opportunities, while others will instinctively
disapprove. But Congress should approach the matter more systematically. The
alternative is effectively to delegate authority to the communications providers, who
are focused on profit and other fiduciary duties to their shareholders, rather than the
public interest, and who are reacting to events largely controlled by others with no
accountability to US voters.

C. Cross-Border Data Requests

As Europe expands surveillance authorities and the United States contracts, and as
encryption proliferates in ways that challenge surveillance without providers’ technical
assistance, there will be more focus on cross-border data requests—i.e., situations in
which a government tries to compel the production of data located outside its national
borders. Today, major US providers face escalating pressure from European governments,
asserting their own laws to require production of data stored by the providers in the
United States, in ways that violate US law. At the same time, foreign governments
also are increasingly likely to enact laws forbidding production of locally held data in response to US (and other) demands for its production, and also to enact laws requiring certain data to be held locally, creating a form of reciprocal pressure. International agreements could help reduce this dissonance and also rationalize surveillance rules to promote international commerce, law enforcement, protection of civil liberties, and the worldwide rule of law. Developing such international agreements will be challenging, but the alternative is an increasingly chaotic and dysfunctional system for cross-border data requests that benefits no one. There has been a good deal of recent scholarship on this topic, and Congress should be sure to address it soon.121

D. Location

As discussed above, cheap, user-friendly data encryption seems to have reached, or nearly reached, a tipping point, where it becomes the default instead of an esoteric option for communications and stored data. Not far behind may be location-spoofing, through technologies such as virtual private networks (VPNs). Of course, the government has been dealing with anonymity and location spoofing for some time due to TOR.122 But VPNs may be more significant because, among other things, they are more user-friendly and might be more widely adopted. Companies offering VPN service create an encrypted connection between the user’s device and their own servers, and allow the user to connect to the Internet from those servers. In doing so, the user’s apparent IP address corresponds to the VPN server, which may or may not be in the same country as the user. Ordinary persons may use VPNs to protect their privacy or their personal data from cybercrime, or perhaps to defeat geo-blocking, a location-based limit on access to content on the Internet that relies on IP addresses to filter eligible users.123 But VPNs or other technology that spoofs location to defeat geo-blocking filters could also raise problems for administration of FAA § 702. As discussed above, section 702 permits surveillance only when the government has a reasonable belief that the target is abroad, and NSA uses IP address as a means of determining location.124 Coupled with the continued growth of mobile communications at the expense of fixed-point communications, and the increasing number of people who do in fact roam across national borders, the widespread adoption of location-spoofing technology could create real problems.

It appears that ISIL has provided guidance to its members and affiliates on the use of encryption;125 if it has not already done so, ISIL also could provide guidance on the use of TOR, VPNs or similar services, or users could consult the Internet directly for instructions. To be sure, NSA almost surely has other technical or human methods at its disposal to help determine location, and it may also have lists of IP addresses associated with known VPN providers that it might be able to persuade the FISA Court to ignore as evidence of location in the court-approved targeting procedures or otherwise. But NSA’s current approach requires analysts to get to the bottom of conflicting information.
about a target’s location, rather than adopting a simple more-likely-than-not mechanical test. What this means, in practical terms, is not only that conflicts must be resolved before targeting can occur, but also that the emergence of new information about an existing target may require immediate attention and de-tasking if the discrepancy cannot be resolved. As the PCLOB explained in its report on FAA § 702:

Commentators have questioned the rigor of the agency’s “foreignness” determinations, particularly whether they rely on certain default assumptions where information about a person is lacking. The notion also has arisen that the agency employs a “51 percent test” in assessing the location and nationality of a potential target—in other words, that analysts need only be slightly more than half confident that the person being targeted is a non-US person located outside the United States.

These characterizations are not accurate. In keeping with representations the government has made to the FISA court, NSA analysts consult multiple sources of information in attempting to determine a proposed target’s foreignness; they are obligated to exercise a standard of due diligence in that effort, making their determinations based on the totality of the circumstances. They also must document the information on which they based their assessments, which must be reviewed and approved by two senior analysts prior to targeting and which are subject to further review later.126

With respect to the foreignness determination, the NSA analyst is required to assess whether the target of the acquisition is a non-US person reasonably believed to be located outside the United States based upon the totality of the circumstances available. This analysis begins with a review of the initial lead information, which must be examined to determine whether it indicates either the location or the US person status of the potential target. At times, the lead information itself will state where the target is assessed to be located and their US person status. In other instances, this information may only enable an analyst to infer location or US person status. In either case, the section 702 targeting determination may not be made upon the lead information alone. Instead, the NSA analyst must check multiple sources and make a determination based on the totality of the circumstances available to the analyst.

The government has stated that in making this foreignness determination, the NSA targeting procedures inherently impose a requirement that analysts conduct “due diligence” in identifying these relevant circumstances. What constitutes due diligence will vary depending on the target; tasking a new selector used by a foreign intelligence target with whom the NSA is already quite familiar may not require deep research into the target’s (already known) US person status and current location, while a great deal more effort may be required to target a previously unknown, and more elusive, individual. As previously discussed above, a failure by an NSA analyst to conduct due diligence in
identifying relevant circumstances regarding the location and US person status of a section 702 target is a reportable compliance incident to the FISC.

After conducting due diligence and reviewing the totality of the circumstances, the NSA analyst is required to determine whether the information indicates that the target is a non-US person reasonably believed to be located outside the United States. The government has stated, and the Board’s review has confirmed, that this is not a “51 percent to 49 percent test.” If there is conflicting information indicating whether a target is located in the United States or is a US person, that conflict must be resolved and the user must be determined to be a non-US person reasonably believed to be located outside the United States prior to targeting.127

In sum, as NSA’s director of civil liberties and privacy has explained, “[i]f the analyst discovers any information indicating the targeted person may be located in the US or that the target may be a US person, such information must be considered. In other words, if there is conflicting information about the location of the person or the status of the person as a non-US person, that conflict must be resolved before targeting can occur.”128 Given this requirement to resolve conflicting information about a target’s location, and the scale of FAA § 702 collection (probably around 100,000 targets), location-spoofing does not need to work 100 percent of the time, or even 20 percent of the time, to create significant administrative problems, delay, and uncertainty in the application of the law and repeated de-tasking and re-tasking of selectors.

It may be that NSA’s tools are so sophisticated that even a concerted effort by ISIL or others to spoof IP addresses would have negligible impact.129 But Congress should satisfy itself that this is the case in connection with FAA renewal, because if it is not, the statute might require a major overhaul. To the extent that the true locations of users of targeted selectors cannot be determined consistently, reliably, and quickly, the FAA is to that extent in deep trouble. It is not clear to me that we have the technical expertise, conceptual models, and political consensus necessary to write and enact a next generation of surveillance laws that balance privacy and security effectively and constitutionally.130

Even in the absence of intentional efforts to spoof location, increasing fragmentation of the Internet will also pressure the role of location in surveillance law. Compared to just a few years ago, global communications networks are much bigger and faster, and are likely to continue growing, whether measured by the number of users, number of web pages, or amount of data available and transmitted.131 At the same time, transmission facilities are proliferating, with more and more undersea cables being laid and planned132 and fewer chokepoints for transiting communications of all kinds. For example, Brazil is planning for an undersea cable connecting South America directly to
Europe, without transiting the United States, apparently motivated in part by desires to avoid US surveillance (although such surveillance has been publicly known since at least the 1970s).

One result, not readily amenable to legal solution, is that the US home field advantage in surveillance is receding. By one estimate, before 2001, 80 percent of the world’s communications traffic transited the United States, while now it is less than 20 percent (albeit of a much higher total number of communications). This estimate may or may not be numerically accurate, but the trend is unmistakable. On the other hand, the increase in the total amount of data also creates problems in the form of ever-larger haystacks in which the government must find the needles.

Another result of increasing fragmentation may be that there are fewer communications facilities dedicated to carrying international rather than domestic traffic, meaning that packets from domestic and international communications may increasingly be found in the same locations. That seems to be part of what has challenged NSA’s “upstream” collection, as discussed above. To the extent that is the case, however, it challenges another aspect of FISA’s basic regulatory approach: the distinctions based on where data is acquired, which were premised on the view that acquisition domestically deserved more protection because of the higher incidence of domestic communications. That is still probably true, for at least some domestic facilities, to a great extent, but it is becoming less true over time. For the long run, Congress may want to reconsider distinctions between surveillance conducted in the United States and surveillance conducted abroad.

E. Internet of Things and FinTech

It is commonplace today to acknowledge the expanding Internet of Things (IOT), in which devices ranging from toasters to air conditioners to door locks are connected to the Internet and to each other, and fintech, which involves the intersection of finance and technology. There are many interesting business issues raised by the IOT and fintech, and some very interesting operational issues relevant to national security (such as the availability and durability of what may be a host of new network access points for surveillance, and vulnerabilities for hacking, and new communications capabilities embedded in financial transactions). There are also several legal issues related to national security and surveillance. For example, the profusion of connected devices and data types will challenge existing collection paradigms, and perhaps the distinction between contents and metadata. The profusion of new “providers” may challenge existing definitions in FISA and the FAA, both as to who may be compelled to provide technical assistance and the nature of that assistance, and will certainly pose cultural challenges—e.g., if and when a manufacturer of Internet-connected door locks receives its first FISA order as part of an authorized physical search.
Finally, over time the government will need to address a series of issues arising from the increasing number of digital footprints left by almost all users of the Internet, especially users of social media. Among the issues are the following. First is the question of governmental access to this data. One perspective is that if the data are freely available on the Internet, the government also should be able to review them. A competing perspective, of course, is that the government should not be reviewing my Facebook posts without meeting some standard of suspicion. Second, of course, not all open source data is freely available to everyone—some data may require elicitation by a government agent or an agent’s undisclosed participation in a forum such as an online chat room. Is data “open source” if a government agent needs to create a false online identity (or otherwise violate a provider’s terms of service) to access it? Is it open source if the agent uses her real online identity (and doesn’t violate the terms of service)? Third, there is the question of possible bulk collection of open source data—e.g., how would Americans feel about NSA ingesting public data on all real estate transactions from Dearborn, Michigan, and then querying it selectively over time? To be sure, there are guidelines that govern access to open source data, such as the FBI’s Domestic Investigations and Operations Guide (DIOG), DOD 5240.1-R, and DOD-I 3115.12, and an inter-agency National Open Source Committee (NOSC) to consider policy issues. But it is not clear that the guidelines have kept up with recent changes. Fourth, the increasing use of social media for terrorist propaganda only complicates matters and introduces First Amendment issues as well.

There is also a series of questions from the perspective of counter-intelligence. For example, there have been concerns about the security of privately held open source data. In other words, could Facebook be the next Office of Personnel Management? Although Internet and cloud providers may have better security than most individual users, they are obviously attractive targets for hackers because they hold so much data. For example, Google revealed in 2011 that “unknown hackers likely originating from central China tried to hack into the Gmail accounts of hundreds of users, including senior US government officials, Chinese activists and journalists.” The director of the CIA’s personal e-mail account was hacked in 2015. Today, with entire digital personas available online, will terrorists and spies need to jettison their identities the way they used to dispose of mobile telephones? Will future undercover agents or NOC operatives need to do so? And if they take steps to avoid using the Internet during a period of classified training, will that gap immediately expose them as government agents? These and many related questions remain to be addressed by policymakers.

4. Conclusion

There is a significant contrast between the two analytical parts of this paper. With the possible exception of modifications to Executive Order 12333, most of the issues
discussed in part 2 are interstitial and fit within our existing paradigms. Whether to permit US person queries of upstream data, for example, is an important question, but one on which reasonably educated policymakers can make a choice without fear of truly revolutionary effects. The issues discussed in part 2 will be most significant when the solutions are considered in the aggregate, rather than individually. Death by a thousand cuts—considered from the perspective of privacy or security—is the concern here.

The issues in part 3 of the paper, by contrast, strike me as substantially more significant, and difficult. For example, if the government cannot use FISA to compel access to stored e-mail of non-US persons located in the United States, it is a big deal; if encryption makes all Western governments more reliant on provider technical assistance and providers continue to resist, and if cross-border data requests can’t be dealt with efficiently, it is a very big deal; and if the basic location-based grammar of the FAA fails because of increased location-spoofing or other developments, it is a huge deal. Debates over renewal of the FAA in the next two years will very likely include the issues set out in part 2 of this paper. I hope they will also include some of the issues set out in part 3, or that Congress and the executive branch will consider them carefully in a separate process.\(^{148}\)

**NOTES**

1 The Privacy and Civil Liberties Oversight Board (PCLOB) describes itself as follows:

The PCLOB is an independent agency within the executive branch established by the Implementing Recommendations of the 9/11 Commission Act of 2007. The bipartisan, five-member Board is appointed by the President and confirmed by the Senate. By statute, the Chairman serves full time, but the four other Board members serve in their positions part-time. The PCLOB’s mission is to ensure that the federal government’s efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties.


3 The FAA also increased protections for US persons located abroad. For a more complete discussion of the FAA, see NSIP, *supra* note 2, at chs. 16–17.

5 For a discussion of these debates, see, e.g., NSIP, supra note 2, § 19:4.50 (Supp. 2015).

6 President Barack Obama, Remarks by the President at the National Defense University (May 23, 2013), https://www.whitehouse.gov/the-press-office/2013/05/23/remarks-president-national-defense-university. The president summarized his conclusions about terrorism as follows:

So that’s the current threat—lethal yet less capable al Qaeda affiliates; threats to diplomatic facilities and businesses abroad; homegrown extremists. This is the future of terrorism. We have to take these threats seriously, and do all that we can to confront them. But as we shape our response, we have to recognize that the scale of this threat closely resembles the types of attacks we faced before 9/11.

In the 1980s, we lost Americans to terrorism at our embassy in Beirut; at our Marine barracks in Lebanon; on a cruise ship at sea; at a disco in Berlin; and on a Pan Am flight—Flight 103—over Lockerbie. In the 1990s, we lost Americans to terrorism at the World Trade Center; at our military facilities in Saudi Arabia; and at our embassy in Kenya. These attacks were all brutal; they were all deadly; and we learned that left unchecked, these threats can grow. But if dealt with smartly and proportionally, these threats need not rise to the level that we saw on the eve of 9/11.


8 The president made two references to surveillance in his May 2013 speech. First, in describing the aftermath of the 9/11 attacks, before he took office, he said: “And so our nation went to war. We have now been at war for well over a decade. . . . Meanwhile, we strengthened our defenses. . . . Most of these changes were sound. . . . But some, like expanded surveillance, raised difficult questions about the balance that we strike between our interests in security and our values of privacy.” Later in the speech, the president said:

Thwarting homegrown plots presents particular challenges in part because of our proud commitment to civil liberties for all who call America home. That’s why, in the years to come, we will have to keep working hard to strike the appropriate balance between our need for security and preserving those freedoms that make us who we are. That means reviewing the authorities of law enforcement, so we can intercept new types of communication, but also build in privacy protections to prevent abuse.

That means that—even after Boston—we do not deport someone or throw somebody in prison in the absence of evidence. That means putting careful constraints on the tools the government uses
to protect sensitive information, such as the state secrets doctrine. And that means finally having a strong Privacy and Civil Liberties Board to review those issues where our counterterrorism efforts and our values may come into tension.

Remarks by the President at the National Defense University, supra note 6.


11 Smith, supra note 10.


14 See Brief for Appellant at 1–2, In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, No. 14-2985-cv (2d Cir. Aug. 12, 2014), https://www.eff.org/document/microsofts-second-circuit-opening-brief. The Introduction to the brief begins as follows:

Imagine this scenario. Officers of the local Stadtpolizei investigating a suspected leak to the press descend on Deutsche Bank headquarters in Frankfurt, Germany. They serve a warrant to seize a bundle of private letters that a New York Times reporter is storing in a safe deposit box at a Deutsche Bank USA branch in Manhattan. The bank complies by ordering the New York branch manager to open the reporter’s box with a master key, rummage through it, and fax the private letters to the Stadtpolizei.

The U.S. Secretary of State fumes: “We are outraged by the decision to bypass existing formal procedures that the European Union and the United States have agreed on for bilateral cooperation, and to embark instead on extraterritorial law enforcement activity on American soil in violation of international law and our own privacy laws.” Germany’s Foreign Minister responds: “We did not conduct an extraterritorial search— in fact we didn’t search anything at all. No German officer ever set foot in the United States. The Stadtpolizei merely ordered a German company to produce its own business records, which were in its own possession, custody, and control. The American reporter’s privacy interests were fully protected, because the Stadtpolizei secured a warrant from a neutral magistrate.”
No way would that response satisfy the U.S. Government. The letters the reporter placed in a safe
deposit box in Manhattan are her private correspondence, not the bank’s business records. The
seizure of that private correspondence pursuant to a warrant is a law enforcement seizure by a
foreign government, executed in the United States, even if it is effected by a private party whom the
government has conscripted to act on its behalf.

This case presents a digital version of the same scenario, but the shoe is on the other foot.

Microsoft’s position was somewhat challenged when the government of Ireland filed a brief conceding that
it is “incumbent upon Ireland to acknowledge” that its own Supreme Court has “held that . . . there may be
circumstances in which an Irish court would order the production of records from an Irish entity on foreign
soil,” perhaps even if “execution of the order would violate the law of the foreign sovereign.” Brief of Amicus
Curiae Ireland at 5–6, In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft

http://www.usatoday.com/story/opinion/2013/10/24/nsa-foreign-leaders-president-obama-lisa-monaco-
editorials-debates/3183331.

16 Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over
Freedom Act are codified at 50 U.S.C. § 1803(i), and the provisions ending bulk collection are codified at

17 For a more complete discussion of the president’s speech and PPD-28, see NSIP, supra note 2, § 19:4.50
(Supp. 2015).

18 For example, in a February 2015 release, ODNI described some of the ways in which the intelligence
community has implemented PPD-28, noting that the directive “reinforces current practices, establishes
new principles, and strengthens oversight, to ensure that in conducting signals intelligence (SIGINT)
activities, the United States takes into account not only the security needs of our nation and our allies,
but also the privacy of people around the world.” Office of the Dir. of Nat’l Intelligence, Signals Intelligence
-liberties. In the same document, the DNI described himself as being “pleased to report that, as required
by PPD-28, all Intelligence Community elements have reviewed and updated their existing policies and
procedures, or have issued new policies or procedures, to provide safeguards for personal information
collected through SIGINT, regardless of nationality and consistent with national security, our technical
capabilities, and operational needs.” For a more complete discussion of PPD-28, see NSIP, supra note 2,
§ 19:4.50 (Supp. 2015).


20 See Ellen Nakashima and Andrea Peterson, Obama Administration Opted Not to Force Firms to Decrypt
/obama-administration-opted-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1da6a012-6dca
-11e5-aa5b-f78a98956699_story.html. By contrast, some of the 2016 presidential contenders, such as
Hillary Clinton, are keeping options open on encryption and urging providers and the government to work
together to find solutions. See Hillary Clinton on National Security and the Islamic State, Council on Foreign
-islamic-state/p37266. In her CFR speech, Clinton said:

Another challenge is how to strike the right balance of protecting privacy and security.
Encryption of mobile communications presents a particularly tough problem. We should take the
concerns of law enforcement and counterterrorism professionals seriously. They have warned that impenetrable encryption may prevent them from accessing terrorist communications and preventing a future attack. On the other hand, we know there are legitimate concerns about government intrusion, network security, and creating new vulnerabilities that bad actors can and would exploit. So we need Silicon Valley not to view government as its adversary. We need to challenge our best minds in the private sector to work with our best minds in the public sector to develop solutions that will both keep us safe and protect our privacy. Now is the time to solve this problem, not after the next attack.

In a speech at the University of Minnesota in mid-December 2015, Clinton said this:

Now, encryption of mobile devices and communications does present a particularly tough problem with important implications for security and civil liberties. Law enforcement and counterterrorism professionals warn that impenetrable encryption may make it harder for them to investigate plots and prevent future attacks. On the other hand, there are very legitimate worries about privacy, network security, and creating new vulnerabilities that bad actors can exploit.

I know there’s no magic fix to this dilemma that will satisfy all these concerns. But we can’t just throw up our hands. The tech community and the government have to stop seeing each other as adversaries and start working together to keep us safe from terrorists. And even as we make sure law enforcement officials get the tools they need to prevent attacks, it’s essential that we also make sure jihadists don’t get the tools they need to carry out attacks.


21 Of course, some observers presumably believe the Obama administration did not go far enough in advancing reforms, while others may believe it went too far. An interesting question, which may be answered during calendar year 2016, is the extent to which the US intelligence community will depart, in public or in private, from the Obama administration’s official positions on national security issues. There are certainly at least pockets of resentment against the administration within the community, and serious disagreement with some of its policies. See, e.g., Adam Entous & Danny Yadron, Some Senior U.S. Officials Not Comfortable with Obama’s Curbs on NSA Spying on Leaders, WALL STREET JOURNAL (Dec. 30, 2015), http://www.wsj.com/articles/some-senior-u-s-officials-not-comfortable-with-obamas-curbs-on-nsa-spying-on-leaders-1451506801. With respect to encryption, for example, FBI Director Comey called publicly for legislation to address the issue in 2014, and then, after the administration decided not to seek such legislation, the FBI in 2015 apparently continued to meet with congressional staff about the topic. See James Comey, Keynote Address at Going Dark: Are Technology, Privacy and Public Safety on a Collision Course?, BROOKINGS INST. (Oct. 16, 2014) (transcript available at http://www.brookings.edu/~media/events/2014/10/goingdark20technologyprivacycomey_fbi_20141016_fbi_comey_transcript.pdf) at 14; David Perera, Terror Fears Don’t Budge Obama on Encryption, POLITICO (Dec. 17, 2015), http://www.politico.com/story/2015/12/obama-resists-calls-for-encryption-shift-216920 (“After warning in 2014 that encryption was hamstringing the FBI, Comey launched a yearlong campaign to persuade Congress to act. Even after being warned off earlier this year by the White House, FBI officials continued meeting with lawmakers and congressional staffers.”).


Ingrid Melander & Adrian Croft, France Arrests Suspect in Brussels Jewish Museum Shooting, REUTERS (June 1, 2014), http://www.reuters.com/article/2014/06/01/us-belgium-shooting-france -idUSB5BN0EC17P20140601.


37 David Remnick, *Going the Distance*, The New Yorker (Jan. 27, 2014), http://www.newyorker.com/magazine/2014/01/27/going-the-distance-david-remnick. The New Yorker article was the one in which the president referred to ISIL as a “jayvee” group:

> The analogy we use around here sometimes, and I think is accurate, is if a jayvee team puts on Lakers uniforms that doesn’t make them Kobe Bryant,” Obama said, resorting to an uncharacteristically flip analogy. “I think there is a distinction between the capacity and reach of a bin Laden and a network that is actively planning major terrorist plots against the homeland versus jihadists who are engaged in various local power struggles and disputes, often sectarian.

In his May 2013 speech, the president gave a more nuanced assessment, without mentioning ISIL by name:

> Unrest in the Arab world has also allowed extremists to gain a foothold in countries like Libya and Syria. But here, too, there are differences from 9/11. In some cases, we continue to confront state-sponsored networks like Hezbollah that engage in acts of terror to achieve political goals. Other of these groups are simply collections of local militias or extremists interested in seizing territory. And while we are vigilant for signs that these groups may pose a transnational threat, most are focused on operating in the countries and regions where they are based. And that means we’ll face more localized threats like what we saw in Benghazi, or the BP oil facility in Algeria, in which local operatives—perhaps in loose affiliation with regional networks—launch periodic attacks against Western diplomats, companies, and other soft targets, or resort to kidnapping and other criminal enterprises to fund their operations.

Remarks by the president at the National Defense University, *supra* note 6.


39 Arlette Saenz, *President Obama Vows to ‘Completely Decapitate’ ISIS Operations*, ABC News (Nov. 13, 2013), http://abcnews.go.com/Politics/president-obama-vows-completely-decapitate-isis-operations/story?id=35173579 (“From the start our goal has been first to contain, and we have contained them.”).


51 See McLaughlin, supra note 40.

I am not aware of any credible, public reporting that ISIL has so far developed a meaningful capability in either biological or nuclear weapons.

53 *PCLOB 702 Report, supra* note 1, at 2.

54 *Id.* at 9.


57 See *PCLOB 702 Report, supra* note 1, at 33–34, 84.

58 See *id.* at 37.

59 *Id.* at 10; see *id.* at 38 (“There are technical reasons why ‘about’ collection is necessary to acquire even some communications that are ‘to’ and ‘from’ a tasked selector. In addition, some types of ‘about’ communications actually involve internet activity of the targeted person. The NSA cannot, however, distinguish in an automated fashion between ‘about’ communications that involve the activity of the target from communications that, for instance, merely contain an email address in the body of an email between two non-targets.” (footnotes omitted)).

60 For a detailed discussion of the two FISA Court decisions from 2011, see *NSIP, supra* note 2, § 17:5 (Supp. 2015).

61 *Id.* (quoting [REDACTED], 2011 WL 10945618, at *13 (FISA Ct. Oct. 3, 2011)).

62 See *id.* (citing *PCLOB 702 Report, supra* note 1, at 84–86).

63 See *PCLOB 702 Report, supra* note 1, at 143–145 (“To build on current efforts to filter upstream communications to avoid collection of purely domestic communications, the NSA and DOJ, in consultation with affected telecommunications service providers, and as appropriate, with independent experts, should periodically assess whether filtering techniques applied in upstream collection utilize the best technology consistent with program needs to ensure government acquisition of only communications that are authorized for collection and prevent the inadvertent collection of domestic communications . . . . The NSA periodically should review the types of communications acquired through ‘about’ collection under Section 702, and study the extent to which it would be technically feasible to limit, as appropriate, the types of ‘about’ collection.”); *PCLOB 1-29-15 RAR, supra* note 55, at 21–24.

64 *NSIP, supra* note 2, § 17:5 (Supp. 2015). As the PCLOB explained in its report on FAA § 702,

    In a still-classified September 2008 opinion, the FISC agreed with the government’s conclusion that the government’s target when it acquires an “about” communication is not the sender or recipients of the communication, regarding whom the government may know nothing, but instead the targeted user of the Section 702–tasked selector. The FISC’s reasoning relied upon language in a congressional report, later quoted by the FISA Court of Review, that the “target” of a traditional FISA electronic surveillance “is the individual or entity . . . about whom or from whom information is sought.”

*PCLOB 702 Report, supra* note 1, at 29–30. It is certainly true that the “target” of surveillance is the person from or about whom the government is seeking information, as discussed in *NSIP, supra* note 2, §§ 7:13, 8:1, 17:5. But that does not resolve the question whether the government can review the contents of an unlimited number of e-mails from unrelated parties in its effort to find information “about” the target.
65 The Obama administration certainly has described itself as restricting surveillance in favor of privacy. See, e.g., ODNI SIGNALS INTELLIGENCE REFORM 2015 ANNIVERSARY REPORT, http://icontherecord.tumblr.com/pdp-28/2015/privacy-civil-liberties. For a more complete discussion of PPD-28, see NSIP, supra note 2, § 19.4.50 (Supp. 2015).

66 Under current law, queries of FAA § 702 data are governed by minimization procedures approved by the FISA Court. As explained in the PCLOB’s report on Section 702:

Each agency that receives communications under Section 702 has its own minimization procedures, approved by the FISA court, that govern the agency’s use, retention, and dissemination of Section 702 data. Among other things, these procedures include rules on how the agencies may “query” the collected data. The NSA, CIA, and FBI minimization procedures all include provisions permitting these agencies to query data acquired through Section 702, using terms intended to discover or retrieve communications content or metadata that meets the criteria specified in the query. These queries may include terms that identify specific U.S. persons and can be used to retrieve the already acquired communications of specific U.S. persons. Minimization procedures set forth the standards for conducting queries. For example, the NSA’s minimization procedures require that queries of Section 702—acquired information be designed so that they are “reasonably likely to return foreign intelligence information.”

67 See Charlie Savage, New York Times, statement at The Second Annual Cato Surveillance Conference, After FREEDOM: A Dialogue on NSA in the Post-Snowden Era (Oct. 21, 2015) (“the FISA Amendments Act come [sic] up for renewal in 2017, and . . . there is an effort already in Congress to require warrants before the government can look at already-collected information that it gathered without a warrant for an American’s identifier, which is something the intelligence community has been resisting. But we’ll see—that, I imagine, is the next battle”).

68 PCLOB 702 Report, supra note 1, at 7–8 (footnotes omitted). For a discussion of the mechanics of querying, see id. at 55–60.

69 See Minimization Procedures used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, § 3(b)(5) (Oct. 31, 2011), http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf; PCLOB 702 Report, supra note 1, at 7 (“Data from upstream collection is received only by the NSA: neither the CIA nor the FBI has access to unminimized upstream data.”); PCLOB 702 Report, supra note 1, at 35, 161 n.571.

70 PCLOB 702 Report, supra note 1, at 12; see also id. at 137–138.

71 In February 2015, ODNI reported that

FBI, CIA, and NSA each are instituting new requirements for using a U.S. person identifier to query information acquired under Section 702. As recommended by the Privacy and Civil Liberties Oversight Board, NSA’s minimization procedures will require a written statement of facts showing that a query is reasonably likely to return foreign intelligence information. CIA’s minimization procedures will be similarly amended to require a statement of facts for queries of content. In
addition, FBI’s minimization procedures will be updated to more clearly reflect the FBI’s standard for conducting U.S. person queries and to require additional supervisory approval to access query results in certain circumstances.

ODNI Signals Intelligence Reform 2015 Anniversary Report, http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties; see also PCLOB 1-29-15 RAR at 19–20. Other possibilities are set out in NSIP:

As to querying of downstream data, there are several options available in devising the new restrictions. Substantively, the government could simply forbid querying altogether, or forbid it when motivated by an affirmative (rather than protective) foreign intelligence purpose. Alternatively, or in addition, it could adopt a procedural approach, requiring a finding of reasonable articulable suspicion (RAS), or even probable cause, that the U.S. person is associated in some way with an international terrorist group, or perhaps another foreign power. Such a finding could be made either by the Executive Branch unilaterally, or be subject to approval by the FISA Court (perhaps with an emergency exception), before querying may occur.

NSIP, supra note 2, § 19:4.50 (Supp. 2015).

72 PCLOB 702 Report, supra note 1, at 14. For more detail on how querying works under Section 702, see id. at 55–60.


74 See PCLOB 702 Report, supra note 1, at 137–138.

75 ODNI Signals Intelligence Reform 2015 Anniversary Report, http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties. In particular, according to Robert Litt, the General Counsel of ODNI:

Under the new policy, in addition to any other limitations imposed by applicable law, including FISA, any communication to or from, or information about, a U.S. person acquired under Section 702 of FISA shall not be introduced as evidence against that U.S. person in any criminal proceeding except (1) with the prior approval of the Attorney General and (2) in (A) criminal proceedings related to national security (such as terrorism, proliferation, espionage, or cybersecurity) or (B) other prosecutions of crimes involving (i) death; (ii) kidnapping; (iii) substantial bodily harm; (iv) conduct that constitutes a criminal offense that is a specified offense against a minor as defined in 42 USC 16911; (v) incapacitation or destruction of critical infrastructure as defined in 42 USC 5195c(e); (vi) cybersecurity; (vii) transnational crimes; or (viii) human trafficking.


76 PCLOB 702 Report, supra note 1, at 97 n.438.

77 Id. at 162.

See NSIP, supra note 2, § 19:4.50 (Supp. 2015) and sources cited therein. Even if some querying of data collected under EO 12333 were subject to a probable-cause or other requirement, it is not clear that the same requirement would apply to data collected under FAA § 702 because of the higher standards and requirements for collection under Section 702.

Cf. United States v. Ramirez, 523 U.S. 65, 71 (1998) (“This is not to say that the Fourth Amendment speaks not at all to the manner of executing a search warrant. The general touchstone of reasonableness which governs Fourth Amendment analysis, governs the method of execution of the warrant. Excessive or unnecessary destruction of property in the course of a search may violate the Fourth Amendment, even though the entry itself is lawful and the fruits of the search are not subject to suppression.” (citation omitted)). In its decision upholding “upstream” collection, discussed above, the FISA Court relied in part on strong minimization procedures to uphold very broad acquisition of information. See NSIP, supra note 2, § 17:5 (Supp. 2015); see also United States v. Mohamud, No. 10-475, 2014 WL 2866749, at *26 (D. Or. June 24, 2014) (“Thus, subsequent querying of a § 702 collection, even if U.S. person identifiers are used, is not a separate search and does not make § 702 surveillance unreasonable under the Fourth Amendment.”). The analysis under the FAA may not be the same as earlier analysis governing EO 12333 surveillance, in part because of the role of the FISA Court in the former.


PCLOB 702 Report, supra note 1, at 52.

See id. at 55–56 (“The NSA . . . often stores data acquired from multiple legal authorities in a single data repository. Instead of limiting access to whole databases, the NSA tags each acquired communication with the legal authority under which it was acquired, and then has systems that prevent an analyst from accessing or querying data acquired under a legal authority for which the analyst does not have the requisite training”).


The IC ITE [Intelligence Community Integrated Intelligence Enterprise] represents a strategic shift from agency-centric information technology (IT) to a common enterprise platform where the IC can easily and securely share technology, information, and capabilities across the Community. To enable this change, the Director of National Intelligence (DNI), in consultation with the applicable IC element head, has designated IC elements as Service Providers, who assume the responsibility for developing and maintaining IC ITE services of common concern. IC ITE Services are the capabilities and shared solutions that are being delivered across the IC to help complete the vision of IC ITE. These services currently include: a common desktop environment; a joint cloud environment; an applications mail; an enterprise management capability; identification, authentication, and authorization capabilities; network requirements and engineering services; and a security coordination service.
Working with the IC under the IC ITE Strategy, the IC CIO is facilitating the development, implementation, and adoption of seamless and secure enterprise solutions that promote trusted collaboration—connecting people to people, people to data, and data to data. The strategy enhances the IC’s ability to securely discover, access, and share information across agencies and ultimately enables greater mission success.

IC ITE Implementation is an evolving process of consolidating and adopting Community capabilities. With the adoption of IC ITE Services, users will have broader and faster access to data and an increased ability to collaborate on common systems across the IC in ways that enhance mission integration and optimize mission success.

Id.

87 See 50 U.S.C. §§ 1801(e)(1)–(2), 1881a(a), 1881a(g)(2)(A)(v).

88 For a discussion of “foreign intelligence information” including both “protective” and “affirmative” intelligence, see NSIP, supra note 2, §§ 8:29–8:36. For a discussion of PPD-28, see NSIP, supra note 2, § 19:4.50 (Supp. 2015).


90 For a discussion of this possibility, and how it influenced the adoption of the first executive order comprehensively regulating the Intelligence Community, an antecedent to EO 12333, see id. §§ 1:4, 2:7. More recently, in December 2014, in Section 309 of the Intelligence Authorization Act for Fiscal Year 2015, Pub. L. No. 113-293, 128 Stat. 3998 (codified at 50 U.S.C. § 1813 (Supp. II 2014)), Congress required by statute procedures governing retention of communications acquired under EO 12333. To my knowledge, this is the first direct statutory regulation of such surveillance.


92 Much of the most sophisticated and thoughtful material on encryption is available on or through LAWFARE, www.lawfareblog.com.

93 50 U.S.C. § 1805(c)(2)(B); see also id. §§ 1802(a)(4)(A), 1822(a)(4)(A)(i), 1842(d)(2)(B)(i); 50 U.S.C.A. 1861(c)(2)(F)(vii). The language in FISA is very similar to that in a 1970 amendment to the Wiretap Act, which provides that an order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information,
facilities, and technical assistance necessary to accomplish the interception unobtrusively and
with a minimum of interference with the services that such service provider, landlord, custodian,
or person is according the person whose communications are to be intercepted.

18 U.S.C. § 2518(4); see also id. § 2511(2)(a)(ii).

94 The term is defined in 50 U.S.C. § 1881(b)(4) to include:

(A) a telecommunications carrier, as that term is defined in [section 3 of the Communications Act
of 1934 (47 U.S.C. 153)];

(B) a provider of electronic communication service, as that term is defined in section 2510 of title
18, [United States Code];

(C) a provider of a remote computing service, as that term is defined in section 2711 of title 18,
[United States Code];

(D) any other communication service provider who has access to wire or electronic communications
either as such communications are transmitted or as such communications are stored; or

(E) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).


95 Id. § 1881a(h)(1)(A).

96 See id. § 1881a(g)(2)(A)(vi).

97 See id. § 1881b(a)(1). A Section 703 order “shall direct . . . if applicable, an electronic communication
service provider to provide to the Government forthwith all information, facilities, or assistance necessary
to accomplish the acquisition authorized under such order in a manner that will protect the secrecy of the
acquisition and produce a minimum of interference with the services that such electronic communication
service provider is providing to the target of the acquisition.” Id. § 1881b(c)(5)(B).

98 See id. § 1881c(c)(3)(A).


101 New York Tel. Co., 434 U.S. at 176–177. The Supreme Court elaborated on this point in a footnote:

We reject the Court of Appeals’ suggestion that the fact that Congress amended Title III [the
Wiretap Act] to require that communication common carriers provide necessary assistance in
connection with electronic surveillance within the scope of Title III reveals a congressional “doubt
that the courts possessed inherent power to issue such orders” and therefore “it seems reasonable
to conclude that similar authorization should be required in connection with pen register
orders. . . .” The amendment was passed following the decision of the Ninth Circuit in Application
of United States, 427 F.2d 639 (1970), which held that absent specific statutory authority, a United
States District Court was without power to compel a telephone company to assist in a wiretap
conducted pursuant to Title III. The court refused to infer such authority in light of Congress’ silence
in a statute which constituted a “comprehensive legislative treatment” of wiretapping. We think
that Congress’ prompt action in amending the Act was not an acceptance of the Ninth Circuit’s
view but “more in the nature of an overruling of that opinion.” The meager legislative history of
the amendment indicates that Congress was only providing an unequivocal statement of its intent
under Title III. See 115 Cong. Rec. 37192 (1969) (remarks of Sen. McClellan). We decline to infer from
a congressional grant of authority under these circumstances that such authority was previously
lacking.
Moreover, even if Congress’ action were viewed as indicating acceptance of the Ninth Circuit’s view that there was no authority for the issuance of orders compelling telephone companies to provide assistance in connection with wiretaps without an explicit statutory provision, it would not follow that explicit congressional authorization was also needed to order telephone companies to assist in the installation and operation of pen registers which, unlike wiretaps, are not regulated by a comprehensive statutory scheme. In any event, by amending Title III Congress has now required that at the Government’s request telephone companies be directed to provide assistance in connection with wiretaps. It is plainly unlikely that Congress intended at the same time to leave federal courts without authority to require assistance in connection with pen registers.

Id. at 177 n.25 (some citations omitted).

102 This is in one sense the continuation of a trend revealed publicly by the US government before the FAA. See NSIP, supra note 2, § 16:5 (quoting remarks by Ken Wainstein).

103 The Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001–1010. Under one provision of CALEA, a “telecommunications carrier shall not be responsible for decrypting, or ensuring the government’s ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.” Id. § 1002(b)(3).


105 In re U.S. for an Order Authorizing Roving Interception of Oral Communications, 349 F.3d 1132, 1145 (9th Cir. 2003).

106 Id. at 1147–48 (Tallman, J., dissenting) (citations omitted).


111 Id., Comment 27.

112 Id., Comment 24. This possibility raises an interesting question that Congress may want to consider with respect to the technical assistance provisions of the FAA. As noted above, traditional FISA allows compelled assistance from “a specified communication or other common carrier, landlord, custodian, or
other specified person,” while FAA § 702 applies only to an “electronic communication service provider” (ECSP). The question is whether an ECSP is subject to the compelled assistance provisions of FAA § 702 where it is not directly involved in facilitating the communications to be monitored—e.g., if Microsoft were compelled to push down a Windows software update to facilitate surveillance of a person who was sending encrypted emails on a Dell personal computer using a Comcast connection to the Internet and Gmail. For a discussion of a more extreme scenario, in which a Verizon employee is compelled to assist in a physical search under FAA § 702 by disabling a home alarm system, see NSIP, supra note 2, § 17:8.

113 EFF UK Comments, supra note 109, Comment 33.


In describing their compliance qualitatively, however, these providers are often quite explicit in their efforts to provide as little data as possible to the government, and only when compelled to do so. Apple reports its approach to compliance as follows:

Any government agency demanding customer content from Apple must get a search warrant. When we receive such a demand, our legal team carefully reviews it. If there’s a question about the legitimacy or scope of the request we challenge it, as we have done as recently as this year. We only comply with information requests once we are satisfied that the request is valid and appropriate, and then we deliver the narrowest possible set of information.

Facebook describes itself as follows:

We have strict processes in place to handle these government requests. Every request we receive is checked for legal sufficiency. We require officials to provide a detailed description of the legal and factual basis for their request, and we push back when we find legal deficiencies or overly broad or vague demands for information. We frequently share only basic subscriber information.

Yahoo! uses similar language to describe its approach:

We carefully scrutinize each request to make sure that it complies with the law, and we push back on those requests that don’t satisfy our rigorous standards. When we are compelled to disclose data, consistent with our Global Principles for Responding to Government Requests, we disclose only as much data as is necessary to comply with the request.

Yahoo! also highlights on its transparency web site a quote from its general counsel: “We fight any requests that we deem unclear, improper, overbroad, or unlawful.”
Finally, Twitter reports this:

We may not comply with requests for a variety of reasons. For example:

We do not comply with requests that fail to identify a Tweet or Twitter account.

We may seek to narrow requests that are overly broad.

In other cases, users may have challenged the requests after we’ve notified them.

On the other hand, it is reasonably clear from these reports that the providers have not decided to resist government directives wholesale or to engage in broad civil disobedience of court orders. According to their latest published data, Google, Apple, Facebook, Yahoo! and Twitter all currently provide at least some information in response to approximately 80 percent of US government law enforcement requests. The companies do not appear to publish data on their compliance with US national security requests, although 50 U.S.C. § 1874 as amended by the USA Freedom Act has expanded reporting options.


In September 2010, Microsoft began to store data for certain web-based email accounts in a datacenter in Dublin, Ireland, which is leased and operated by Microsoft’s wholly owned Irish subsidiary. The addition of the Dublin datacenter boosted the quality of service to numerous users because it reduces “network latency”—i.e., the inverse ratio between quality of service and the distance between a user and the datacenter where that user’s account is hosted. Maximizing quality of service by minimizing network latency is critical to Microsoft’s business. The Dublin datacenter allows Microsoft to reduce network latency and improve the quality of service for users located closer to Ireland than to the United States. For Outlook.com accounts stored in Dublin, the users’ content resides on a specific server in the Dublin datacenter. It does not exist in any form inside the United States. Certain non-content information and address book data, in contrast, is stored in the United States.

For its part, the government says that “[a]ccording to Microsoft, it stores email content in a foreign datacenter when a subscriber claims to be physically present in an overseas location, but it takes no steps to confirm whether the subscriber is, in fact, logging in from a foreign location.” Government’s Memorandum of Law in Opposition to Microsoft’s Motion to Vacate Email Account Warrant at 2, In re a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, No. 13-MAG-2814; M9-150 (S.D.N.Y., April 20, 2014), http://digitalconstitution.com/wp-content/uploads/2014/11/government-warrant.pdf

117 For a more complete discussion of these points, see NSIP, supra note 2, at §§ 7:12, 7:16, 7:18.

118 See NSIP, supra note 2, § 16:5 (quoting remarks by Ken Wainstein).

119 See NSIP, supra note 2, § 7:29. As a former assistant attorney general for national security (Ken Wainstein) explained in 2008 in a slightly different context, “We rely on the communications providers to do our intelligence surveillances. We can’t do [the surveillances] without them because . . . we . . . don’t own the communications systems. We need to rely on their assistance.” Cited in NSIP, supra note 2, § 16:5. The full quotation from Wainstein reflects the fact that in some cases (but not in all), the government can obtain a FISA Court order.

A good deal of high-quality scholarship, and also a short piece that I wrote on the subject, can be found on Lawfare, https://lawfareblog.com/search/node/cross-border%20data%20requests.


For a discussion of the efforts of Netflix and Hulu to defeat VPN-spoofed IP addresses, see, e.g., Thorin Klosowski, Get Around Location Restrictions on Netflix or Hulu with a Private VPN IP Address, LIFEHACKER (Jan. 20, 2016), http://lifehacker.com/get-around-location-restrictions-on-netflix-or-hulu-wit-175403343.

See PCLOB 702 Report, supra note 1, at 38 (“NSA is required to use other technical means, such as Internet protocol (‘IP’) filters, to help ensure that at least one end of an acquired Internet transaction is located outside the United States.”), 120 (“In part to compensate for this problem, the NSA takes additional measures with its upstream collection to ensure that no communications are acquired that are entirely between people located in the United States. These measures can include, for instance, employing Internet protocol filters to acquire only communications that appear to have at least one end outside the United States.”); 132 n.544 (NSA masks U.S. person identities in its FAA § 702 reporting in certain circumstances, and unmasking can include IP addresses as well as names). See also NSA Director of Civil Liberties and Privacy Office Report, NSA’s Implementation of Foreign Intelligence Surveillance Act Section 702, at 5–6 (April 16, 2014) (“For example, in certain circumstances NSA’s procedures require that it employ an Internet Protocol filter to ensure that the target is located overseas”), http://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf.

Margaret Coker, Sam Schechner and Alexis Flynn, How Islamic State Teaches Tech Savvy to Evade Detection, WALL STREET JOURNAL (Nov. 16, 2015) (“Islamic State, for its part, has built a tech-savvy division of commanders who issue tutorials to sympathizers about the most secure and least expensive ways of communicating”), http://www.wsj.com/articles/islamic-state-teaches-tech-savvy-1447720824.

PCLOB 702 Report, supra note 1, at 117–118 (footnotes omitted).

PCLOB 702 Report, supra note 1, at 43–44 (emphasis and footnotes omitted).


According to one study from June 2015, VPNs are used by approximately 20 percent of European Internet users, but 11 out of 14 VPN providers studied leaked information about users because of the “IPv6 leakage.” See Science Daily, Most Internet Anonymity Software Leaks Users’ Details (June 29, 2015), http://www.sciencedaily.com/releases/2015/06/150629210621.htm.


The Internet can be measured by number of users, amount of data, or number of web sites, among other things. Precise measurements can be difficult, but the trends are unmistakable. See, e.g., Internet World Stats, Internet Growth Statistics, http://www.internetworldstats.com/emarketing.htm; Internet Live Stats, Internet Users, http://www.internetlivestats.com/internet-users.


See NSIP, supra note 2, § 16:12; Church Report Book III at 741.


137 See NSIP, supra note 1, Chapters 7, 16, 17.


142 See, e.g., the reference to “common carrier” in 50 U.S.C. §§ 1801(l), 1802(a)(4), and 1805(c)(2)(B), and the definition and reference to “electronic communication service provider” in 50 U.S.C. § 1881(b)(4) and, e.g., 50 U.S.C. § 1881a(g)(2)(A)(vi).


144 In a November 2015 speech, for example, Hillary Clinton said: “Radicalization and recruitment also is happening online. There’s no doubt we have to do a better job contesting online space, including websites and chat rooms, where jihadists communicate with followers. We must deny them virtual territory just as we deny them actual territory. . . Social media companies can also do their part by swiftly shutting down terrorist accounts so they’re not used to plan, provoke, or celebrate violence.” *Hillary Clinton on National Security and the Islamic State*, COUNCIL ON FOREIGN RELATIONS (Nov. 19, 2015), http://www.cfr.org/radicalization-and-extremism/hillary-clinton-national-security-islamic-state/p37266. President Obama addressed the nation from the Oval Office in early December 2015. According to an article in Politico, a “senior administration official speaking ahead of Obama’s speech Sunday told reporters the president’s speech would include a discussion about encryption and the social media fight, but the president left that out of the version of the speech that he delivered. (The White House said Monday that the efforts to address this issue are underway.)” Edward-Isaac Dovere, *This Time, Clinton’s Closer to the Public Mood than Obama*, POLITICO (Dec. 8, 2015), http://www.politico.com/story/2015/12/hillary-clinton-obama-national-security-216523. See also Nicole Perlofth & Mike Isaac, *Terrorists Mock Bids to End Use of Social Media*, N.Y. TIMES (Dec. 7, 2015) (“As soon as Twitter suspends one account, a new one is created. After the group’s 99th account was suspended, it taunted Twitter by creating @IslamicState100, posting images of birthday candles, cake, trophies and fireworks”), http://www.nytimes.com/2015/12/08/technology/terrorists-mock-bids-to-end-use-of-social-media.html; Scott Shane, Matt Apuzzo & Eric Schmitt, *Americans Attracted to ISIS Find an “Echo Chamber” on Social Media*, N.Y. TIMES (Dec. 8, 2015), http://www.nytimes.com/2015/12/09/us/americans-attracted-to-isis-find-an-echo-chamber-on-social-media.html; Scott Shane, *Internet Firms


146 Reuters, Google: Gmail Hack Likely From China Cyberattackers, HUFFINGTON POST (June 1, 2011), http://www.huffingtonpost.com/2011/06/01/google-gmail-hack-china_n_869995.html.


148 The question whether the issues discussed in part 3 should be considered as part of FAA renewal, or separately, is one that may depend on legislative tactics and other considerations. I am largely indifferent as to whether these issues are addressed as part of FAA renewal or in a separate process.
About the Author

DAVID S. KRIS

David S. Kris is general counsel of Intellectual Ventures. From 2009 to 2011, he was assistant attorney general for national security at the US Department of Justice. From 2003 to 2009 he held various positions at Time Warner, including deputy general counsel and chief ethics and compliance officer. From 1992 to 2003, he was an attorney and then associate deputy attorney general at the Department of Justice. He is the author of several papers on national security and coauthor of the treatise National Security Investigations and Prosecutions. He graduated from Harvard Law School in 1991.

Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group’s output will also be published on the Lawfare blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation’s laws and legal institutions.

Jack Goldsmith and Benjamin Wittes are the cochairs of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams/national-security-technology-law-working-group.
The Fourth Amendment in the Information Age

Robert S. Litt

To badly mangle Marx, a specter is haunting Fourth Amendment law—the specter of technological change. In a number of recent cases, in a number of different contexts, courts have questioned whether existing Fourth Amendment doctrine, developed in an analog age, is able to deal effectively with digital technologies. Justice Sotomayor, for example, wrote in her concurrence in United States v. Jones, a case involving a GPS tracking device placed on a car, that “the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties . . . is ill suited to the digital age.” And in Riley v. California, the Chief Justice more colorfully rejected the government’s argument that a search of a cell phone was equivalent to a search of a wallet:

That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.

I intend to discuss the application of the Fourth Amendment in the information age, and I want to start with two important caveats.

First, I am not proposing a comprehensive theory of Fourth Amendment law. Rather, I want to offer some tentative observations that might be explored in shaping a productive response to the challenges that modern technology poses.

2. Id. at 957 (Sotomayor, J., concurring).
4. Id. at 2488-89.
creates for existing legal doctrine. In particular, I would like to suggest that the concept of “reasonable expectation of privacy” as a kind of gatekeeper for Fourth Amendment analysis should be revisited.

Second, these thoughts are not informed by deep research into the intent of the Framers, or close analysis of case law or academic scholarship. Rather, they derive from almost forty years of experience in law enforcement and intelligence. But, despite Justice Oliver Wendell Holmes’s adage about the life of the law, I hope that they have some foundation in logic as well.\(^5\)

I want to approach this complicated issue by focusing on two intelligence activities that have been the subject of recent litigation, partly because they will help illuminate the Fourth Amendment issue, and partly because I know them well. The first is the formerly secret, but now well-known, bulk telephone metadata collection program conducted under the business records provision of the Foreign Intelligence Surveillance Act (FISA).\(^6\) Although this program has now ended, it provides a good starting point for this discussion.

Telephone metadata is information about a telephone call such as the number calling, the number being called, the date, time and duration of the call, and so on—the same sort of information that those of us old enough to remember long-distance toll calls used to get each month on our itemized telephone bills. Metadata does not include the content of the calls or the identity of the callers.

For several years, and with judicial authorization, the NSA collected metadata in bulk about U.S. phone calls from telephone companies for counterterrorism purposes. The metadata was kept in secure databases. It could only be accessed by a few specially trained NSA analysts, and then only to identify telephone numbers in contact with so-called “seed” numbers as to which there was a reasonable and articulable suspicion of an association with terrorism—such as, for example, a number used by a suspected terrorist.\(^7\) The standard of “reasonable articulable suspicion” is derived from *Terry v. Ohio*,\(^8\) which held that police stops that did not amount to an arrest could be made on reasonable suspicion. Although this program was approved numerous times by

---

5. See Oliver Wendell Holmes, Jr., *The Common Law* 1 (1881) (“The life of the law has not been logic: it has been experience.”).


judges of the Foreign Intelligence Surveillance Court, the Second Circuit has held that it was not authorized by FISA’s business records provision.  

Here, however, I want to focus on the litigation in the District of Columbia in which Judge Leon enjoined the bulk collection of metadata on the ground that it violated the Fourth Amendment. The plaintiffs’ constitutional challenge in that case faced a substantial hurdle in the form of Smith v. Maryland, a 1979 Supreme Court decision holding that obtaining telephone metadata is not a search for Fourth Amendment purposes because people lack a reasonable expectation of privacy in information they voluntarily expose to the telephone company. If the so-called “third-party doctrine” of Smith governed this case, then there was no search at all, and hence no violation of the Fourth Amendment.

In his lengthy and somewhat colorful opinion, Judge Leon tried to distinguish the bulk collection program from Smith because the metadata in the case before him was collected about millions of people rather than about a single individual; because it was collected on a rolling basis and covered several years’ worth of metadata, rather than just a few days; and because, in the modern age, cellphones are ubiquitous and contain vast amounts of information. According to Judge Leon, metadata “that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic—a vibrant and constantly updating picture of the person’s life.” Judge Leon went on to hold that the electronic search of this metadata without a warrant likely violated the Fourth Amendment.

I do not think that Judge Leon’s efforts to distinguish Smith were successful. First, while Judge Leon is certainly right that metadata can be very revealing of personal activities, there is nothing new about that insight. Justice Stewart dissented from the decision in Smith itself in part because he recognized that metadata “easily could . . . reveal the most intimate details of a person’s life.” The point of Smith was not that metadata is innocuous, but that you have chosen to reveal it to a third party. To use an analogy, if you give a document to a third party, you have lost your expectation of privacy in that document, whether it is a laundry ticket or a confession of mortal sin. Moreover, the fact that cell phones today contain a lot of information beyond metadata does not seem relevant when the government did not actually search or collect any of that other information.

---

9. ACLU v. Clapper, 785 F.3d 787, 792 (2d Cir. 2015).
13. Id. at 42.
It is also true that the government collected lots of metadata about lots of people under this program. But it is a well-established principle that one person cannot assert the Fourth Amendment rights of someone else. The Court has long held that “Fourth Amendment rights are personal rights which . . . may not be vicariously asserted.”

My right to privacy is not violated when the government collects your metadata.

Finally, I find it hard to understand the alchemy by which information that you choose to disclose to a third party develops an expectation of privacy because you have chosen to disclose a lot of that information. That seems counter-intuitive to say the least. For all of these reasons, if you accept Smith’s holding that there was no expectation of privacy in the telephone metadata in that case because it had been voluntarily exposed to a third party, you can’t conclude there was an expectation of privacy in the metadata in this case.

I am not alone in thinking that Judge Leon did not correctly apply existing Fourth Amendment doctrine. Every other judge to rule on the constitutionality of the bulk metadata program has disagreed with him. Most recently, his injunction was immediately stayed by the D.C. Circuit, and in an opinion concurring in the denial of rehearing en banc, Judge Kavanaugh pointedly noted that Smith remained controlling. Although I think Judge Leon’s dismissal of Smith was wrong, it is nevertheless worth considering his analytic framework.

Judge Leon’s decision, and the arguments of the parties, followed traditional Fourth Amendment doctrine. First, he considered whether or not there was a “search” for Fourth Amendment purposes, by determining whether plaintiffs had a reasonable expectation of privacy in the information obtained by the government, including whether any expectation of privacy was defeated by the fact that they had voluntarily disclosed the information to the telephone companies. After finding that plaintiffs had a reasonable expectation of privacy in the metadata, he went on to analyze whether the search of that data was “reasonable” under the Fourth Amendment, using the well-established rubric that warrantless searches are unreasonable unless they fall within one of a number of established exceptions. That’s the way cases like this have been approached since Katz v. United States, but I’m not sure that the framework is entirely satisfying in the context of digital data.

To help illustrate why, let’s turn to another factual scenario: the recent case of *Jewel v. National Security Agency*, in which plaintiffs challenged the government’s surveillance of internet communications under Section 702 of the Foreign Intelligence Surveillance Act. Section 702 authorizes the government to collect foreign intelligence information, without an individualized warrant or probable cause, by targeting non-U.S. persons outside the United States. Persons inside the United States, or Americans anywhere in the world, can only be targeted with probable cause.

However, plaintiffs in *Jewel* claimed that the warrantless collection of Internet communications even of foreigners violated the Fourth Amendment rights of Americans, because it involved the search of communications of U.S. persons as well as the foreign targets. According to the plaintiffs’ motion for partial summary judgment, the government accomplishes one type of collection under Section 702—so-called “upstream” collection of emails—by first copying all internet traffic flowing across certain switches and storing it briefly; then electronically scanning the contents of the communications as well as the metadata to determine which communications contain certain “selectors” such as email addresses that have been determined to be likely to produce foreign intelligence; and finally pulling out those communications and ignoring the rest. The plaintiffs allege that this process constitutes an unconstitutional search of everyone’s email communications and that, just as the Supreme Court in *Katz* recognized that people have a reasonable expectation of privacy in telephone communications that could not be invaded without a warrant, this electronic scanning constitutes an invasion of people’s reasonable expectation of privacy in Internet communications.

The description set out above is drawn from the plaintiffs’ allegations. I am not confirming or denying their accuracy, or indeed saying anything about the means by which the government collects Internet communications. In fact, the court in *Jewel* never reached the merits of the Fourth Amendment argument, holding that the plaintiffs lacked standing because they could not establish that their communications were actually searched in this manner. Assume,

---

21. Motion for Partial Summary Judgment at 1, Jewel, No. 4:08-cv-04373-JSW, ECF No. 261.
22. Id. at 6–9.
23. Id. at 17.
24. See Jewel v. Nat’l Sec. Agency, 810 F.3d 622, 625 (9th Cir. 2015) (discussing the district court’s dismissal of the plaintiffs’ Fourth Amendment internet surveillance claim for lack of standing, and dismissing the plaintiffs’ appeal for lack of jurisdiction).
however, that the plaintiffs’ description is accurate, and consider how the Fourth Amendment should apply to this hypothetical scenario.

The *Jewel* case involved the content of communications rather than metadata. It is significant that the government did not argue in *Jewel* that the plaintiffs had no reasonable expectation of privacy in the content of the communications even though that content was exposed to a third party, although the government did advance other arguments that there was no search for purposes of the Fourth Amendment. Yet, in important respects, this hypothetical Internet collection program looks like the real bulk metadata program. In both situations, the government is obtaining large quantities of digital data and scanning that data electronically using specific selectors such as telephone numbers and email addresses to look for specific relevant information that is found in only a small percentage of communications. In both cases, no human being ever sees the vast majority of information that never passes through that filter. Yet because our analytical framework makes application of Fourth Amendment protections turn upon whether there is a “reasonable expectation of privacy,” and thus distinguishes metadata from content, one of these might be a search subject to the Fourth Amendment, and the other might not be.

This strikes me as both unrealistic and undesirable. I suggest that—at least in the context of government acquisition of digital data—we should think about eliminating the separate inquiry into whether there was a “reasonable expectation of privacy” as a gatekeeper for Fourth Amendment analysis. In an era in which huge amounts of data are flowing across the Internet; in which people expose previously unimagined quantities and kinds of information through social media; in which private companies monetize information derived from search requests and GPS location; and in which our cars, dishwashers, and even light bulbs are connected to the Internet, trying to parse out the information in which we do and do not have a reasonable expectation of privacy strikes me as a difficult and sterile task of line-drawing. Rather, we should simply accept that any acquisition of digital information by the Government implicates Fourth Amendment interests.

After all, the concept of a “reasonable expectation of privacy” as a talisman of Fourth Amendment protection is not found in the text of the Fourth Amendment itself, which says merely that “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.” It was only in 1967, in *Katz*, that the Supreme Court defined a search as the invasion of a “reasonable expectation of privacy.” *Katz* revisited *Olmstead v. United States* after 40 years.

25. *U.S. CONST.* amend. IV.
years; the accelerating pace of modern technological change suggests to me that fifty years is not too soon to revisit Katz. My proposal is that the law should focus on determining what is unreasonable rather than on what is a search.

Of course, this approach would mean that courts would assess the reasonableness of government activity in cases where today they simply find that the Fourth Amendment does not apply. But before the privacy advocates start popping the champagne corks, I want to make clear that I believe the inquiry into reasonableness should focus on actual harms, rather than theoretical ones. It should involve a realistic assessment of privacy rights and governmental needs, one that looks at not only the act of collection but also at the use that is made of the data and the processes that exist to regulate that use. Just as the changing technological environment should affect how we view the interests of individuals, it should affect how we evaluate the governmental interests at stake.

Let’s return to the metadata program. Every bit of the data that the government collected in the bulk metadata program was data that the telephone companies collected and retained for their own purposes. In fact, the government got the data from the telephone companies, not individuals. Once the government got the data, it remained unseen and unknown unless it proved to be connected to a terrorist “seed” number, and, as noted above, only an infinitesimal fraction of the data was ever seen by any human being. And while Congress last summer ordered the bulk collection program stopped, it authorized a mechanism allowing the government to get the exact same information—phone numbers in contact with potential terrorist phone numbers—directly from the telephone companies, based on the exact same showing of a reasonable articulable suspicion of a connection to terrorism.

In the bulk collection program, digital data was moved from one set of computer servers owned by telephone companies to another set of computer servers owned by the government. No person in the government ever saw this data, except under circumstances that Congress, at least, appears to have agreed are reasonable. What is the actual harm to an individual for constitutional purposes if information about her telephone calls sits on two computers instead of one? Indeed, despite a great deal of overheated rhetoric about “mass surveillance,” the criticism of the bulk metadata program invariably focused on speculation about what the government could do with bulk metadata, rather than what it did do, and on the chilling effect that hypothetical activity might produce. There’s no question that one could use

27. 277 U.S. 438 (1928).
28. See supra note 22 and accompanying text.
bulk telephone metadata to do a lot of big data analysis and find out a lot of personal information. But that’s not what this program ever did.

Similarly, in the hypothetical Internet case, if the government electronically scans electronic communications, even the content of those communications, to identify those that it is lawfully entitled to collect, and no one ever sees a non-responsive communication, or even knows that it exists, where is the actual harm? Indeed, while I am no expert, I believe that this scanning is similar to what private companies and government agencies already do on their networks for the purposes of identifying and stopping malware.30

In both of these situations, while government computers may electronically touch information about you contained in a digital database, the government actually knows nothing more about you than it did before—unless and until it has a valid purpose for learning that information. Fourth Amendment analysis should be based on that reality, rather than on hypotheticals.

Of course, the nature of the information the government collects, and the privacy interests that attach to that data, will still have an important role to play in assessing reasonableness. To this extent, I agree with those who criticize the broad proposition that any information that is disclosed to third parties is outside the protection of the Fourth Amendment. Courts can appropriately take into account whether information is content or non-content information, whether it is publicly disclosed through social media or is stored in the equivalent of the cloud, or whether its exposure is “voluntary” only in the most technical sense because of the demands of modern technology. But we should not be viewing this analysis of privacy interests as an on/off switch to determine whether or not the Fourth Amendment applies, as today’s third-party doctrine does, but as more of a rheostat to identify the degree of protection that would ensure that the collection and use of that data is reasonable.

So the flip-side of my argument is that even where there is a substantial privacy interest in digital data, we should not default immediately to the rule that a warrant is required unless we can fit the collection of such data into one of the twentieth-century exceptions to the warrant requirement. Instead, at least while the courts are feeling their way through the new legal challenges of the digital age, they should look at all such activity through the prism of a reasonableness inquiry that takes into account not only the nature of the data the government is collecting, but the use the government is going to make of

---

that data. And just as the assessment of privacy interests should be concerned with real harms rather than theoretical ones, the assessment of government use must take account of the very real government interests at stake. Protection of the public is one of the most important functions of government, and the kinds of digital data we are talking about can be of immense benefit to both law enforcement and the national security community, not to mention the potential victims of terrorist attacks or other crimes—if we can be comfortable with the manner in which the government collects and uses that data.

Turning back to my two examples, I noted in my description of the bulk metadata program that the data was used only to help determine, under carefully controlled and supervised conditions, whether a U.S. telephone number had a connection with a number associated with terrorism. There has been a lot of debate about the utility of this program, with people arguing that the program, by itself, never stopped a terrorist attack. But that is the wrong way to assess the value of an intelligence program; you do not get rid of a fire insurance policy that has never paid off because your house has never burned down. The bulk metadata program was developed to fill a real gap that was identified after the 9/11 attacks as one of the factors contributing to our failure to prevent those attacks. And in light of the ongoing efforts of terrorists to recruit Westerners to conduct attacks, and recent horrific events in Paris and Brussels, it’s not hard to see how the information obtained from this program—information about potential contacts between terrorists abroad and people in the US—could be useful. In other words, the bulk metadata program was narrowly focused on a legitimate counterterrorism purpose.

Similarly, Section 702, the Internet program, was specifically authorized by Congress to allow the collection of information for important foreign intelligence purposes, including counterterrorism, by targeting foreigners outside the United States,31 and is one of our most valuable intelligence collection programs. Moreover, while I do not have the technical knowledge necessary to speak authoritatively on this point and my analysis is therefore purely hypothetical, I find it at least plausible that there would often be no effective way to collect targeted communications from the Internet without scanning other communications as well. So in both the telephone metadata and the Internet cases, one can make a strong case that the use of the data was reasonable.

Our legal framework already accepts the concept that restrictions on the use of data can be an important way to protect privacy interests. Congress has required that a variety of government activity authorized under the Foreign Intelligence Surveillance Act be conducted pursuant to so-called “minimization procedures,” which are designed, among other things, to limit the retention

and dissemination of private information acquired through surveillance. Executive Order 12,333 imposes a similar requirement for all intelligence activities collecting information about United States persons. Minimization procedures generally identify permitted uses of information the government collects, including sharing of information between agencies when appropriate, and provide rules and procedures to ensure that those limitations are adhered to. They are a form of use restriction that helps ensure that data collection is consistent with the protection of privacy.

And this is similar to how privacy is protected today in the private sector. A company’s privacy policies typically tell you that the company will keep only certain kinds of information about you, and make use of that information only for certain specified purposes. In other words, your privacy is protected through use restrictions. Corporate privacy policies are not universally applauded, but the principal criticism is that they are frequently contracts of adhesion, not that use restrictions are inadequate to protect privacy. So, in assessing the reasonableness of the government’s collection of data, courts should look at the back end — whether the retention, use, and dissemination are reasonable — as well as the front end — whether the collection itself is reasonable in light of its purpose.

Let me now address several questions that this approach raises. One objection is obvious: once the government gets hold of information, how can we be sure that it is only used appropriately? This concern is both justified and substantial. We care more about government collection of data than private collection because of the government’s power to make use of data in ways that adversely affect us and could infringe upon our privacy and liberties. We must always be alert to the possibility of government overreach, and attentive to ways to prevent it. As President Obama said, “Given the unique power of the state, it is not enough for leaders to say: Trust us: we won’t abuse the data we collect . . . . Our system of government is built on the premise that our liberty cannot depend on the good intentions of those in power, it depends on the law to constrain those in power.”

Three related concepts can provide the necessary assurance: oversight, technology, and transparency.

Oversight — and accountability through the mechanisms of oversight — is a critical way to ensure compliance with reasonable restrictions on collection and use. At least in the area of intelligence, we have robust oversight, involving a variety of agencies and offices, congressional committees, and, in the case of

activities under FISA, the courts. In addition, the independent Privacy and Civil Liberties Oversight Board provides both oversight and guidance on counterterrorism policies. This multi-level oversight should play a role in any assessment of the reasonableness of data collection. The more people who have eyes on a particular activity, the less likely it is to be abused, and the more likely it is that privacy protections will be observed.

Technology is a critical adjunct to oversight. When people talk about technology in the context of surveillance, they tend to talk either about the awful ways in which technology enables the government to spy on us, or about the ways in which we can use technology to protect ourselves from that awful government spying. But technology can play an important role as well in protecting privacy while enabling lawful collection of information by the government. I mentioned above that the bulk telephone metadata was kept in special secure databases, with access limited to only a few people with special training. Software also tracked every query that was made of the database so that the queries could be audited for compliance. I am no computer scientist, but I have to think that there are additional ways that we could use technology to buttress our oversight mechanisms. I’ve been told, for example, that there are systems that permit queries of data in such a fashion that the person making the query never sees the data but sees only the response, and that the holder of the data doesn’t see the actual query or the response but is able to ascertain that the query is authorized. Surely our extraordinarily capable technologists can develop other techniques to provide assurance that data the government collects is being used only as appropriate.

The fact is, in the context of the activities I discussed above—the bulk metadata program and collection under Section 702 of FISA—the combination of oversight mechanisms and technology worked effectively. In all the information that has come out about these two programs, there has not been a single instance of intentional violation of the law or other deliberate abuse. There were unquestionably mistakes made, which is not surprising given the complexity of the systems involved, and they were discovered, reported, and remedied. But there is a difference between a mistake and an abuse: to quote Justice Holmes again, “[e]ven a dog distinguishes between being stumbled over and being kicked.”

Where we fell short was on the third leg of the stool, transparency. There would have been less damage to the Intelligence Community from the disclosures of the last couple of years had we been more forthcoming about our activities before those leaks. Obviously, intelligence activities have to be conducted with some degree of secrecy, and the same is true of some law enforcement activities. Specific methods and targets of surveillance have to be protected. But if we don’t discuss what we are doing and how we are

35. Holmes, supra note 5, at 3.
regulating it even in general terms, we cede the field to those who are hostile to intelligence activities.

Our actions in the last two and a half years, including the DNI’s promulgation of principles of transparency to govern the Intelligence Community, demonstrate that we are internalizing this lesson. And the availability of public information about intelligence programs, along with the extent of oversight and the nature of technological controls, should factor into the analysis of whether those activities are reasonable. The more transparent we can be about collection activity and its oversight, the more confident the public can be that the appropriate limits on that activity will be respected. And the more the public understands and has confidence in what our law enforcement and intelligence agencies are actually doing, the less likely it is to be “chilled” by fears about what they could be doing.

A second question is how broadly I would extend my suggested framework. In these remarks I have suggested that it apply to “digital data.” Generally speaking, this is information, of any nature, that is transmitted or stored electronically. My discussion of the Fourth Amendment is limited to digital data because it most starkly illustrates the problems technology poses for existing doctrine. However, I have not considered whether my suggestions could or should serve as the basis for a broader Fourth Amendment jurisprudence.

Third, the idea of balancing the invasion of privacy and the government’s purpose looks very much like the existing test used by courts to determine whether a warrantless search is “reasonable” under the Fourth Amendment. As the Supreme Court said in Maryland v. King,36 “[a] pplication of ‘traditional standards of reasonableness’ requires a court to weigh ‘the promotion of legitimate governmental interests’ against ‘the degree to which [the search] intrudes upon an individual’s privacy.’”37 In particular, the courts have upheld much warrantless foreign intelligence collection activity under the doctrine of “special needs.” To that extent, I am proposing nothing new.

What I have suggested, however, is that—at least in the area of government collection of digital data—we eliminate the preliminary analysis of whether someone has a reasonable expectation of privacy in the data and proceed directly to the issue of whether the collection is reasonable; that the privacy side of that analysis should be focused on concrete rather than theoretical invasions of privacy; and that courts in evaluating reasonableness should look at the entirety of the government’s activity, including the “back end” use, retention restrictions, and the degree of transparency, not just the “front end” activity of collection.

37. Id. at 1970 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).
This approach would present a challenge for our legal system. We would be abandoning a set of fixed rules and a body of case law that have guided law enforcement and the courts for half a century, in favor of a less predictable analysis. But it is time we stopped trying to hammer twenty-first century pegs into mid-twentieth-century holes. It may be that over time a new series of rules would emerge to provide more certainty. But it is equally likely that technology will continue to change so rapidly that the legal system will constantly be struggling to catch up. Application of the general standard of reasonableness to judge the legality of government collection of digital data is a better way to hit that constantly moving target than trying to define more specific rules that may promptly be overtaken by new technologies.

This leads me to one final important point, which is to emphasize that Congress, rather than the judiciary, is in the best position to articulate the rules that should apply to collection activities of the government. A decision by Congress to authorize certain activities under certain controls, made after discussion and debate, should be a strong factor in support of the reasonableness of those activities. Congress is going to have a number of opportunities to address these issues. For example, Section 702 expires at the end of 2017, and there are continued efforts to modernize the Stored Communications Act. It may be too much to hope that in the current political environment, Congress could have a dispassionate and comprehensive discussion about such weighty issues, but the Executive Branch would welcome such a discussion.

These are important issues. They implicate, on the one hand, the privacy and civil liberties of Americans and of others around the world, and, on the other hand, the safety and security of Americans and of others around the world. It is important that we get them right. I hope that the thoughts expressed here can be viewed as a constructive contribution to this effort.

Robert S. Litt is General Counsel, Office of the Director of National Intelligence. This Essay is adapted from a speech delivered to the American Bar Association’s Standing Committee on Law and National Security on February 16, 2016. The views above are entirely the author’s and do not reflect the position of the United States government, the Obama Administration, the Intelligence Community, or even the Office of General Counsel for the Office of the Director of National Intelligence.


(U) SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE

Reporting Period: June 1, 2015 – November 30, 2015

November 2016
(U) SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE

November 2016

TABLE OF CONTENTS

(U) Executive Summary 3

(U) Section 1: Introduction 4

(U) Section 2: Oversight of the Implementation of Section 702 6

(U) I. Joint Oversight of NSA 7
(U) II. Joint Oversight of CIA 9
(U) III. Joint Oversight of FBI 10
(U) IV. Joint Oversight of NCTC 13
(U) V. Interagency/Programmatic Oversight 13
(U) VI. Training 13
(U) VII. The Privacy and Civil Liberties Oversight Board 14

(U) Section 3: Trends in Section 702 Targeting and Minimization 16

(U) I. Trends in NSA Targeting and Minimization 16
(U) II. Trends in FBI Targeting 21
(U) III. Trends in CIA Minimization 23

(U) Section 4: Compliance Assessment – Findings 27

(U) I. Compliance Incidents – General 27
(U) II. Review of Compliance Incidents – NSA Targeting and Minimization Procedures 34
(U) III. Review of Compliance Incidents – CIA Minimization Procedures 48
(U) IV. Review of Compliance Incidents – FBI Targeting and Minimization Procedures 48
(U) V. Review of Compliance Incidents – Provider Errors 51

(U) Section 5: Conclusion 51

(U) Appendix A A-1
(U) **Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence**

November 2016

**Reporting Period: June 1, 2015 – November 30, 2015**

(U) **EXECUTIVE SUMMARY**

(U) The FISA Amendments Act of 2008 (hereinafter “FAA”) requires the Attorney General and the Director of National Intelligence (DNI) to assess compliance with certain procedures and guidelines issued pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 et seq., as amended, (hereinafter “FISA” or “the Act”) and to submit such assessments to the Foreign Intelligence Surveillance Court (FISC) and relevant congressional committees at least once every six months. Section 702 authorizes, subject to restrictions imposed by the statute and required targeting and minimization procedures, the targeting of non-United States persons reasonably believed to be located outside the United States in order to acquire foreign intelligence information. The present assessment sets forth the fifteenth joint compliance assessment of the Section 702 program. This assessment covers the period from June 1, 2015 through November 30, 2015 (hereinafter the “reporting period”) and accompanies the Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of the Foreign Intelligence Surveillance Act as required by Section 707(b)(1) of FISA (hereinafter “the Section 707 Report”). The Department of Justice submitted the Section 707 Report on March 3, 2016; it covers the same reporting period as the Joint Assessment.

(U) This Joint Assessment is based upon the compliance assessment activities that have been jointly conducted by the Department of Justice’s National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI).

(U) This Joint Assessment finds that the agencies have continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702. The personnel involved in implementing the authorities are appropriately focused on directing their efforts at non-United States persons reasonably believed to be located outside the United States for the purpose of acquiring foreign intelligence information. Processes are in place to implement these authorities and to impose internal controls for compliance and verification purposes. The compliance incidents that occurred during this reporting period represent a very small percentage (0.52%) of the overall collection activity. While this represents an increase from the last Joint Assessment’s rate of 0.35%, as well as from the other previous joint assessments’ rates, it still remains well below 1%. Individual incidents, however, can have broader implications, as further discussed herein and in the Section 707 Report. Based upon a review of these compliance incidents, the joint oversight team believes that none of these incidents represent an intentional attempt to circumvent or violate the Act, the targeting or minimization procedures, or the Attorney General’s Acquisition Guidelines.
(U) SECTION 1: INTRODUCTION

(U) The FISA Amendments Act of 2008 (hereinafter, “FAA”) requires the Attorney General and the Director of National Intelligence (DNI) to assess compliance with certain procedures and guidelines issued pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 et seq., as amended (hereinafter, “FISA” or “the Act”), and to submit such assessments to the Foreign Intelligence Surveillance Court (FISC) and relevant congressional committees at least once every six months. As required by the Act, a team of oversight personnel from the Department of Justice’s National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) have conducted compliance reviews to assess whether the authorities under Section 702 of FISA (hereinafter, “Section 702”) have been implemented in accordance with the applicable procedures and guidelines, discussed herein. This report sets forth NSD and ODNI’s fifteenth joint compliance assessment under Section 702, covering the period June 1, 2015 through November 30, 2015 (hereinafter, the “reporting period”).

(U) Section 702 requires that the Attorney General, in consultation with the DNI, adopt targeting and minimization procedures, as well as guidelines. A primary purpose of the guidelines is to ensure compliance with the limitations set forth in subsection (b) of Section 702, which are as follows:

An acquisition authorized under subsection (a)—

(1) may not intentionally target any person known at the time of acquisition to be located in the United States;
(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;
(3) may not intentionally target a United States person reasonably believed to be located outside the United States;
(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and
(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

The Attorney General’s Guidelines for the Acquisition of Foreign Intelligence Information Pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended (hereinafter “the Attorney General’s Acquisition Guidelines”) were adopted by the Attorney General, in consultation with the DNI, on August 5, 2008.

1 (U) This report accompanies the Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of the Foreign Intelligence Surveillance Act, which was previously submitted on March 3, 2016, as required by Section 707(b)(1) of FISA (hereafter Section 707 Report). This fifteenth Joint Assessment covers the same reporting period as the fifteenth Attorney General’s Section 707 Report.
During this reporting period, the Government acquired foreign intelligence information under Attorney General and DNI authorized Section 702(g) certifications that targeted non-United States persons reasonably believed to be located outside the United States in order to acquire different types of foreign intelligence information. Three agencies are primarily involved in implementing Section 702: the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and the Central Intelligence Agency (CIA). An overview of how these agencies implement the authority appears in Appendix A of this assessment. The other agency involved in implementing Section 702 is the National Counterterrorism Center (NCTC), which has a limited role, as reflected in the “Minimization Procedures Used by NCTC in connection with Information Acquired by FBI pursuant to Section 702 of FISA, as amended.”

Section Two of this Joint Assessment provides a comprehensive overview of oversight measures the Government employs to ensure compliance with the targeting and minimization procedures, as well as the Attorney General’s Acquisition Guidelines. Section Two also discusses the July 2014 Section 702 Report by the Privacy and Civil Liberties Oversight Board. Section Three compiles and presents data acquired from the joint oversight team’s compliance reviews in order to provide insight into the overall scope of the Section 702 program, as well as trends in targeting, reporting, and the minimization of United States person information. Section Four describes compliance trends. All of the specific compliance incidents for the reporting period have been previously described in detail in the Section 707 Report. As with the prior Joint Assessments, some of those compliance incidents are analyzed here to determine whether there are patterns or trends that might indicate underlying causes that could be addressed through additional measures, and to assess whether the agency involved has implemented processes to prevent recurrences.

In summary, the joint oversight team finds that the agencies have continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702 during this reporting period.
reporting period. As in the prior Joint Assessments, the joint oversight team has not found indications in the compliance incidents that have been reported or otherwise identified of any intentional or willful attempts to violate or circumvent the requirements of the Act. The number of compliance incidents remains small, particularly when compared with the total amount of targeting and collection activity. In its ongoing efforts to reduce the number of future compliance incidents, the Government will continue to focus on measures to improve (a) inter and intra-agency communication, (b) training, and (c) systems used in the handling of Section 702-acquired communications, including those systems needed to ensure that appropriate purge practices are followed and that certain disseminated reports are withdrawn as required. Further, the joint oversight team will also continue to monitor agency practices to ensure appropriate remediation steps are taken to prevent, whenever possible, reoccurrences of the types of compliance incidents discussed herein and in the Section 707 Report. As appropriate, this Joint Assessment provides updates on these on-going efforts.

(U) SECTION 2: OVERSIGHT OF THE IMPLEMENTATION OF SECTION 702

(U) The implementation of Section 702 is a multi-agency effort. As described in detail in Appendix A, NSA and FBI each acquire certain types of data pursuant to their own Section 702 targeting procedures. NSA, FBI, and CIA\(^4\) each handle Section 702-acquired data in accordance with their own minimization procedures.\(^5\) There are differences in the way each agency implements its procedures resulting from unique provisions in the procedures themselves, differences in how these agencies utilize Section 702-acquired data, and efficiencies from using preexisting systems to implement Section 702 authorities. Because of these differences in practice and procedure, there are corresponding differences in each agency’s internal compliance programs and in the external NSD and ODNI oversight programs.

(U) A joint oversight team has been assembled to conduct compliance assessment activities, consisting of members from NSD, ODNI’s Office of Civil Liberties, Privacy and Transparency (ODNI CLPT),\(^6\) ODNI’s Office of General Counsel (ODNI OGC), and ODNI’s Office of the Deputy Director for Intelligence Integration/Mission Integration Division (ODNI DD/II/MID). The team members play complementary roles in the review process. The following describes the oversight activities of the joint oversight team, the results of which, in conjunction with the internal oversight conducted by the reviewed agencies, provide the basis for this Joint Assessment.

---

\(^4\) (U) As discussed herein, CIA receives Section 702-acquired data from NSA and FBI.

\(^5\) (U) Each agency’s targeting and minimization procedures are approved by the Attorney General and reviewed by the Foreign Intelligence Surveillance Court. In 2015, the DNI released, in redacted form, NSA’s, FBI’s, and CIA’s 2014 minimization procedures on ODNI’s IC on the Record website as part of its SIGINT Intelligence Reform 2015 Anniversary Report (hereinafter the “2015 Anniversary Report”). Most recently, on August 11, 2016, the DNI released, in redacted form, NSA’s, FBI’s, and CIA’s (as well as NCTC’s) 2015 minimization procedures on ODNI’s IC on the Record website as part of DNI’s commitment to the IC’s Principles of Transparency.

\(^6\) (U) CLPT was formerly called the Civil Liberties and Privacy Office (CLPO). Its name was changed to CLPT in June 2016. Although outside the reporting period for this current assessment, the name has nonetheless been updated herein.
(U) **I. Joint Oversight of NSA**

(U) Under the process established by the Attorney General and Director of National Intelligence’s certifications, all Section 702 targeting is initiated pursuant to the NSA’s targeting procedures. Additionally, NSA is responsible for conducting post-tasking checks of all Section 702-tasked communication facilities (also referred to as selectors) once collection begins. NSA must also minimize its collection in accordance with its minimization procedures. Each of these responsibilities is detailed in Appendix A. Given its central role in the Section 702 process, NSA has devoted substantial oversight and compliance resources to monitoring its implementation of the Section 702 authorities. NSA’s internal oversight and compliance mechanisms are further described in Appendix A.

(U) NSD and ODNI’s joint oversight of NSA’s implementation of Section 702 consists of periodic compliance reviews, which the NSA targeting procedures require,\(^8\) as well as the investigation and reporting of specific compliance incidents. During this reporting period, NSD and ODNI conducted the following onsite reviews at NSA:

**Figure 1: (U) NSA Reviews**

<table>
<thead>
<tr>
<th>Date of Review</th>
<th>Taskings/Minimization Reviewed</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 28, 2015</td>
<td>June 1, 2015 – July 31, 2015</td>
</tr>
<tr>
<td>October 30, 2015</td>
<td>August 1, 2015 – September 30, 2015</td>
</tr>
<tr>
<td>December 16 and 22, 2015</td>
<td>October 1, 2015 – November 30, 2015</td>
</tr>
</tbody>
</table>

(U) Reports for each of these reviews document the relevant time period of the review, the number and types of communication facilities tasked, and the types of information that NSA relied upon, as well as provide a detailed summary of the findings for that review period. These reports have been provided to the congressional committees with the Section 707 Report, as required by Section 707(b)(1)(F) of FISA.

(U) The joint oversight review process for NSA targeting begins well before the onsite review. Prior to each onsite review, NSA electronically sends the tasking record (known as a tasking sheet) for each facility tasked during the review period to NSD and ODNI.\(^9\) Members of the joint oversight team initially review the tasking sheets, with ODNI team members sending any questions they may have concerning the tasking sheets to NSD, who then prepare a detailed report.

\(^7\) (U) Section 702 authorizes the targeting of non-United States persons reasonably believed to be located outside the United States. This targeting is effectuated by tasking communication facilities (i.e. selectors), including but not limited to telephone numbers and electronic communications accounts, to Section 702 electronic communication service providers. The oversight review process, which is described within this joint assessment, applies to the targeting of every communication facility regardless of the type of facility. A fuller description of the Section 702 targeting process may be found in the Appendix. This assessment uses the terms facilities and selectors interchangeably and is not attempting to make a substantive distinction between the two terms.

\(^8\) (U) NSA’s targeting procedures require that the onsite reviews occur approximately every two months.

\(^9\) (U) During this reporting period, NSA discovered that it had mistakenly not provided some of the required tasking documentation (i.e. tasking sheets) to NSD and ODNI, thereby resulting in compliance incidents, which are discussed below.
of the findings, including any questions and requests for additional information. NSD shares this report with the ODNI members of the joint oversight team. During this initial review, the joint oversight team determines whether the tasking sheets meet the documentation standards required by NSA’s targeting procedures and provide sufficient information for the reviewers to ascertain the basis for NSA’s foreignness determinations. For those tasking sheets that, on their face, meet the standards and provide sufficient information, no further supporting documentation is requested. The joint oversight team then identifies the tasking sheets that did not provide sufficient information and requests additional information.

(U) During the onsite review, the joint oversight team examines the cited documentation underlying these identified tasking sheets, together with NSA Signals Intelligence Directorate (SID) Oversight and Compliance personnel, NSA attorneys, and other NSA personnel as required. The joint oversight team works with NSA to answer questions, identify issues, clarify ambiguous entries, and provide guidance on areas of potential improvement. Interaction continues following the onsite reviews in the form of electronic and telephonic exchanges to answer questions and clarify issues.

(U) The joint oversight team also reviews NSA’s minimization of Section 702-acquired data. NSD reviews all of the serialized reports (with ODNI reviewing a sample) that NSA has disseminated and identified as containing Section 702-acquired United States person information. The team also reviews a sample of serialized reports that NSA has disseminated and identified as containing Section-702 acquired non-United States person information. NSD and ODNI also review a sample of NSA disseminations to certain foreign government partners made outside of its serialized reporting process. These disseminations consist of information that NSA has evaluated for foreign intelligence and minimized, but which may not have been translated into English.

(U) With respect to queries of Section 702-acquired content using a United States person identifier, the joint oversight team reviews all approved United States person identifiers to ensure compliance with the minimization procedures. For each approved identifier, NSA also provides information detailing why the proposed use of the United States person identifier would be reasonably likely to return foreign intelligence information, the duration for which the United States person identifier has been authorized to be used as a query term, and any other relevant information. In addition, with respect to queries of Section 702-acquired metadata using a United States person identifier, NSA’s internal procedures require that NSA analysts document the basis for each metadata query prior to conducting the query. NSD reviews the documentation for 100% of the metadata queries that NSA provides to NSD.

10 (U) Although outside this Joint Assessment’s reporting period, on May 2, 2016, the DNI publicly released ODNI’s third annual Transparency Report[s]: Statistical Transparency Report Regarding Use of National Security Authorities for calendar year 2015 (hereafter the 2015 Transparency Report). Pursuant to reporting requirements proscribed by the USA FREEDOM Act (see 50 U.S.C. § 1873(b)(2)(A)), the 2015 Transparency Report provided the “estimated number of search terms concerning a known U.S. person used to retrieve the unminimized contents of communications obtained under Section 702” (emphasis added) for the entire calendar year of 2015.

11 (U) Also pursuant to reporting requirements proscribed by the USA FREEDOM Act (see 50 U.S.C. § 1873(b)(2)(B)), the 2015 Transparency Report provided the “estimated number of queries concerning a known U.S. person used to retrieve the unminimized noncontents [(i.e. metadata)] information obtained under Section 702” (emphasis added) for the entire calendar year of 2015.
Additionally, the joint oversight team investigates and reports incidents of noncompliance with the NSA targeting and minimization procedures, as well as with the Attorney General Acquisition Guidelines. While some of these incidents may be identified during the reviews, most are identified by NSA analysts or by NSA’s internal compliance program. NSA is also required to report certain events that may not be incidents of non-compliance. For example, NSA is required to report all instances in which Section 702 acquisition continued while a targeted individual was in the United States, whether or not NSA had any knowledge of the target’s travel to the United States. The purpose of such reporting is to allow the joint oversight team to assess whether a compliance incident has occurred and to confirm that any necessary remedial action is taken. Investigations of all of these incidents sometimes result in requests for supplemental information. All compliance incidents identified by these investigations are reported to the congressional committees in the Section 707 Report and to the FISC through quarterly reports or individualized notices.

II. Joint Oversight of CIA

As further described in detail in Appendix A, although CIA does not directly engage in targeting or acquisition, it does nominate potential Section 702 targets to NSA. Because CIA nominates potential Section 702 targets to NSA, the joint oversight team conducts onsite visits at CIA and the results of these visits are included in the bimonthly NSA review reports discussed above. CIA has established internal compliance mechanisms and procedures to oversee proper implementation of its Section 702 authorities.

The onsite reviews also focus on CIA’s application of its Section 702 minimization procedures. For this reporting period, NSD and ODNI conducted the following onsite reviews at CIA:

Figure 2: CIA Reviews

<table>
<thead>
<tr>
<th>Date of Visits</th>
<th>Minimization Reviewed</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 11, 2015</td>
<td>June 1, 2015 – July 31, 2015</td>
</tr>
<tr>
<td>November 4 and 17, 2015</td>
<td>August 1, 2015 – September 30, 2015</td>
</tr>
<tr>
<td>January 6 and 8, 2016</td>
<td>October 1, 2015 – November 30, 2015</td>
</tr>
</tbody>
</table>

Reports for each of these reviews have previously been provided to the congressional committees with the Section 707 Report, as required by Section 707(b)(1)(F) of FISA.

As a part of the onsite reviews, the joint oversight team examines documents related to CIA’s retention, dissemination, and querying of Section 702-acquired data. The team reviews a
sample of communications acquired under Section 702 and identified as containing United States person information that have been minimized and retained by CIA. Reviewers ensure that communications have been properly minimized and discuss with personnel issues involving the proper application of CIA’s minimization procedures. The team also reviews all disseminations of information acquired under Section 702 that CIA identified as potentially containing United States person information. NSD and ODNI also review CIA’s written foreign intelligence justifications for all queries using United States person identifiers of the content of unminimized Section 702-acquired communications.

(S//NF) CIA may receive §unminimized§ Section 702-acquired communications. Such communications must be minimized pursuant to CIA’s minimization procedures. As further described in detail in Appendix A, CIA nominates potential Section 702 targets to NSA. The joint oversight team conducts onsite visits at CIA to review CIA’s original source documentation. The results of these visits are included in the bimonthly NSA review reports discussed above. CIA has established internal compliance mechanisms and procedures to oversee proper implementation of its Section 702 authorities. These processes are further described in Appendix A.

(U) In addition to the bimonthly reviews, the joint oversight team also investigates and reports incidents of noncompliance with CIA’s minimization procedures, the Attorney General Acquisition Guidelines, or other agencies’ procedures in which CIA is involved. Investigations are coordinated through the CIA FISA Program Office and CIA’s Office of General Counsel (CIA OGC), and when necessary, may involve requests for further information, meetings with CIA legal, analytical, and/or technical personnel, or the review of source documentation. All compliance incidents identified by these investigations are reported to the congressional committees in the Section 707 Report and to the FISC through quarterly reports or individualized notices.

(U) III. Joint Oversight of FBI

(U) FBI fulfills various roles in the implementation of Section 702. First, FBI is authorized under the certifications to acquire foreign intelligence information. These acquisitions must be conducted pursuant to FBI’s Section 702 targeting procedures.

(S//NF) Second, FBI also provides_____.

Pursuant to its own authority, FBI is authorized from electronic communication

13 (S//NF) This footnote carried a different portion marking in prior joint assessments.

14 (U) Insofar as CIA nominates facilities for tasking and reviews content that may indicate that a target is located in the United States or is a United States person, some investigations of possible noncompliance with the NSA targeting procedures can also involve CIA.
service providers by targeting facilities that NSA designates (hereinafter “Designated Accounts”). FBI conveys [REDACTED] from the electronic communications service providers for processing in accordance with the agencies’ FISC-approved minimization procedures.

(S//NF) Third, [REDACTED] FBI may receive [REDACTED] unminimized Section 702-acquired communications. Such communications must be minimized pursuant to FBI’s Section 702 minimization procedures. Like CIA, FBI has a process for nominating to NSA new facilities to be targeted pursuant to Section 702.

(U) FBI’s internal compliance program and NSD and ODNI’s oversight program are designed to ensure FBI’s compliance with statutory and procedural requirements for each of these three roles. Each of the roles discussed above, as well as FBI’s internal compliance program, are set forth in further detail in Appendix A.

(U) NSD and ODNI generally conduct monthly reviews of FBI’s compliance with its targeting procedures and bimonthly reviews of FBI’s compliance with its minimization procedures. For this reporting period, onsite reviews were conducted on the following dates:

Figure 3: (U) FBI Reviews

<table>
<thead>
<tr>
<th>Date of Visit</th>
<th>Targeting and Minimization Reviewed</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 19, 2015</td>
<td>June 2015 targeting decisions</td>
</tr>
<tr>
<td>September 16, 2015</td>
<td>July 2015 targeting decisions</td>
</tr>
<tr>
<td>November 9 and 10, 2015</td>
<td>August 2015 targeting decisions and June 1 through August 31, 2015, minimization decisions</td>
</tr>
<tr>
<td>November 17 and 18, 2015</td>
<td>September 2015 targeting decisions</td>
</tr>
<tr>
<td>December 10 and 11, 2015</td>
<td>October 2015 targeting decisions and September 1 through November 30, 2015, minimization decisions</td>
</tr>
<tr>
<td>January 11 and 12, 2016</td>
<td>November 2015 targeting decisions</td>
</tr>
</tbody>
</table>

Reports for each of these reviews have previously been provided to the congressional committees with the Section 707 Report, as required by Section 707(b)(1)(F) of FISA.

(U) In conducting the targeting review, the joint oversight team reviews the targeting checklist completed by FBI analysts and supervisory personnel involved in the process, together with supporting documentation. The joint oversight team also reviews a sample of other files to identify any other potential compliance issues. FBI analysts, supervisory personnel, and attorneys from FBI’s Office of General Counsel (FBI OGC) are available to answer questions, and provide supporting documentation. The joint oversight team provides guidance on areas of potential improvement.

15 (S//NF) Supporting document includes, among other things, [REDACTED] The joint oversight team reviews every file identified by FBI
(U) With respect to minimization, the joint oversight team reviews documents related to FBI’s application of its Section 702 minimization procedures. The team reviews a sample of communications that FBI has marked in its systems as both meeting the retention standards and containing United States person information. The team also reviews all disseminations of information acquired under Section 702 that FBI identified as potentially containing non-publicly available information concerning unconsenting United States person information. In addition, during reviews at individual FBI field offices, NSD reviews FBI’s use of identifiers to query raw FISA-acquired data, including Section 702-acquired data.

(U) During this reporting period, NSD continued to conduct minimization reviews at FBI field offices in order to review the retention and dissemination decisions made by FBI field office personnel with respect to Section 702-acquired data. During these field office reviews, NSD also audits a sample of FBI personnel queries in systems that contain unminimized Section 702 collection. As detailed in the attachments to the Attorney General’s Section 707 Report, NSD conducted minimization reviews at 15 FBI field offices during this reporting period and reviewed cases involving Section 702-tasked facilities. ODNI joined NSD at a subset of these reviews; ODNI receives written summaries regarding all the reviews from NSD regardless of whether ODNI was in attendance or not. These reviews are further discussed in Section IV below.

(S/NF) Separately, in order to evaluate the FBI’s acquisition and provision of FBI has established internal compliance mechanisms and procedures to oversee proper implementation of its Section 702 authorities. These processes are further described in Appendix A.

(U) The joint oversight team also investigates potential incidents of noncompliance with the FBI targeting and minimization procedures, the Attorney General’s Acquisition Guidelines, or other agencies’ procedures in which FBI is involved. These investigations are coordinated with FBI OGC and may involve requests for further information, meetings with FBI legal, analytical, and/or technical personnel, or review of source documentation. All compliance incidents identified by these investigations are reported to the congressional committees in the Section 707 Report and to the FISC through quarterly reports or individualized notices.

16 (S/NF) During these field office reviews, NSD reviewed involving Section 702-tasked facilities.

17 (U) Insofar as FBI nominates facilities for tasking and reviews content that may indicate that a target is located in the United States or is a United States person, some investigations of possible noncompliance with the NSA targeting procedures can also involve FBI.
IV. Joint Oversight of NCTC

As noted above, NCTC is also involved in implementing Section 702, albeit in a limited role, as reflected in the “Minimization Procedures Used by NCTC in connection with Information Acquired by the FBI pursuant to Section 702 of FISA, as amended.” Under these limited minimization procedures, NCTC is not authorized to receive unminimized Section 702 data, but NCTC has been provided access to certain FBI systems containing minimized Section 702 information. As part of the joint oversight of NCTC to ensure compliance with these procedures, NSD and ODNI conduct reviews of NCTC’s access, receipt, and processing of Section 702 information received from FBI. The most recent review occurred in May 2016, which is outside this current joint assessment’s reporting period.

V. Interagency/Programmatic Oversight

Because the implementation and oversight of the Government’s Section 702 authorities are a multi-agency effort, investigations of particular compliance incidents may involve more than one agency. The resolution of particular compliance incidents can provide lessons learned for all agencies. Robust communication among the agencies is required for each to effectively implement its authorities, gather foreign intelligence, and comply with all legal requirements. For these reasons, NSD and ODNI conduct twice monthly telephone calls and quarterly meetings (in addition to ad hoc calls and meetings on specific topics as needed) with representatives from all agencies implementing Section 702 authorities to discuss and resolve interagency issues affecting compliance with the statute and applicable procedures.

NSD and ODNI’s programmatic oversight also involves efforts to proactively minimize the number of incidents of noncompliance. For example, NSD and ODNI have required agencies to demonstrate to the joint oversight team new or substantially revised systems involved in Section 702 targeting or minimization prior to implementation. NSD and ODNI personnel also continue to work with the agencies to review, and where appropriate seek modifications of, their targeting and minimization procedures in an effort to enhance the Government’s collection of foreign intelligence information, civil liberties protections, and compliance. As discussed below, beginning in this reporting period, the Government proposed modifications to the agencies’ targeting and minimization procedures, as well as to some related internal guidance, based on recommendations made by the Privacy and Civil Liberties Oversight Board.

VI. Training

In addition to specific instructions to personnel directly involved in certain incidents of noncompliance discussed in Section 4, the agencies and the joint oversight team have also continued their training efforts to ensure compliance with the targeting and minimization procedures. NSA continued to administer the compliance training course implemented in the prior reporting period. All NSA personnel are required to complete this course on an annual basis in order to gain access to raw Section 702 acquisitions. Additionally, NSA continued providing training on a more informal and ad hoc basis by issuing training reminders to analysts concerning new or updated guidance to maintain compliance with the Section 702 procedures. NSA also began designing new training reminders, in November 2015, on an internal agency website where

13
personnel could obtain information about specific types of Section 702-related issues and compliance matters. CIA continues to provide regular FISA training at least twice a year to all of the attorneys it embeds with CIA operational personnel. Additionally, CIA has a training program that provides hands-on experience with handling and minimizing Section 702-acquired data. During the previous reporting period, CIA centralized its FISA training to provide greater consistency and added a program that provides greater depth on the Section 702 nomination process; during this reporting period, the CIA continued to implement this training required for all personnel who nominate facilities to NSA and/or minimize Section 702-acquired communications. FBI has similarly continued implementing its online training programs regarding nominations, minimization, and other requirements. Completion of these FBI online training programs is required of all FBI personnel who request access to Section 702 information. NSD and FBI have also conducted in-person trainings at multiple FBI field offices. For example, during this current reporting period, NSD and FBI continued to provide additional focused training at FBI field offices on the Section 702 minimization procedures, including training FBI field personnel, such as field office attorneys, on the attorney-client privileged communication provisions of FBI’s minimization procedures.\footnote{This specific training began before and continued after the current reporting period of June 1, 2015 – November 30, 2015.} NSD’s training at FBI field offices also included training on the new reporting requirement from the FISC’s \textit{November 6, 2015 Memorandum Opinion and Order} regarding the 2015 FISA Section 702 Certifications.\footnote{On April 19, 2016, the DNI, in consultation with the Attorney General, released in redacted form, the FISC’s \textit{November 6, 2015 Memorandum Opinion and Order} on the ODNI’s public website \textit{IC on the Record}.} This new reporting requirement applies to queries conducted after December 4, 2015, that were conducted solely for the purpose of returning evidence of a crime and returned Section 702-acquired information of or concerning a U.S. person that was reviewed by FBI personnel.

(U) VII. Privacy and Civil Liberties Oversight Board

(U) In July 2014, the Privacy and Civil Liberties Oversight Board (PCLOB or Board) issued a report on the Section 702 program entitled, “Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act” (PCLOB’s \textit{Section 702 Report}). According to page 2 of the \textit{PCLOB’s Section 702 Report}:

\begin{quote}
The Section 702 program is extremely complex, involving multiple agencies, collecting multiple types of information, for multiple purposes. Overall, the Board has found that the information the program collects has been valuable and effective in protecting the nation’s security and producing useful foreign intelligence. The program has operated under a statute that was publicly debated, and the text of the statute outlines the basic structure of the program. Operation of the Section 702 program has been subject to judicial oversight and extensive internal supervision, and the Board has found no evidence of intentional abuse.
\end{quote}
The Board has found that certain aspects of the program’s implementation raise privacy concerns. These include the scope of the incidental collection of U.S. persons’ communications and the use of queries to search the information collected under the program for the communications of specific U.S. persons. The Board offers a series of policy recommendations to strengthen privacy safeguards and to address these concerns.

(U) Specifically, the Board determined that PRISM collection (where the government sends a selector to a United States-based electronic communications service provider) and upstream collection are authorized by the statutory language of Section 702, and further concluded “that the core of the Section 702 program – acquiring the communications of specifically targeted foreign persons who are located outside the United States, upon a belief that those persons are likely to communicate foreign intelligence […] – fits within the “totality of the circumstances” standard for reasonableness under the Fourth Amendment.” PCLOB’s Section 702 Report at 8-9. However, the Board also found that “[o]utside of this fundamental core, certain aspects of the Section 702 program push the program close to the line of constitutional reasonableness.” Id. It enumerated specific areas “where operations of the Section 702 program could strike a better balance between privacy, civil rights, and national security” and recommended three revisions to the targeting and minimization procedures governing the Section 702 program. See id. at 134.

(U) In response to the PCLOB’s Section 702 Report, the Government adopted all three recommended revisions to the relevant 2015 targeting and minimization procedures, which are detailed below. Subsequently, the FISC, after the appointment of an amicus curiae, found, in an opinion, that those revised procedures complied with Section 702 and were consistent with the requirements of the Fourth Amendment.20

(U) The PCLOB recommended that NSA’s targeting procedures be “revised to (a) specify criteria for determining the expected foreign intelligence value of a particular target, and (b) require a written explanation of the basis for that determination sufficient to demonstrate that the targeting of each selector [i.e. facility] is likely to return foreign intelligence information relevant to the subject of one of the certifications approved by the FISA court.” PCLOB’s Section 702 Report at 134 (Recommendation 1). The joint oversight team worked with NSA to appropriately modify its targeting procedures, including engaging with the PCLOB regarding the proposed revisions, which resulted in those recommendations being implemented in revised targeting procedures that were submitted to the FISC. Additionally, the joint oversight team advised NSA on appropriate supplemental written guidance and training for its personnel, which will continue to be the subject of continued oversight by NSA’s internal compliance personnel and the joint oversight team.

(U) The PCLOB also recommended that FBI’s procedures “be updated to more clearly reflect the actual practice for conducting U.S. person queries, including the frequency with which Section 702 data may be searched when making routine queries as part of FBI assessments and investigations. Further, some additional limits should be placed on the FBI’s use and dissemination

20 (U) These procedures were filed with the FISC as part of the 2015 Certifications renewal application, which the FISC approved on November 6, 2015. As noted above, the FISC’s November 6, 2015 Memorandum Opinion and Order was publicly released on ODNI’s IC on the Record website in April 2016.
of Section 702 data in connection with non-foreign intelligence criminal matters.”  
PCLOB’s Section 702 Report at 137 (Recommendation 2).  Again, the joint oversight team worked with FBI to implement this recommendation and engaged with the PCLOB regarding the proposed revisions.  These revisions were submitted to the FISC in the form of revised minimization procedures.  As discussed above, in its November 6, 2015 Memorandum Opinion and Order, the FISC imposed a reporting requirement for queries conducted after December 4, 2015, that were conducted solely for the purpose of returning evidence of a crime and returned Section 702-acquired information of or concerning a U.S. person that was reviewed by FBI personnel.

(U)  Additionally, the PCLOB also recommended that “[t]he NSA and CIA minimization procedures should permit the agencies to query collected Section 702 data for foreign intelligence purposes using U.S. person identifiers only if it is based upon a statement of facts showing that the query is reasonably likely to return foreign intelligence information as defined in FISA.”  
PCLOB’s Section 702 Report at 139 (Recommendation 3).  The joint oversight team worked with the relevant agencies to implement this recommendation and engaged the PCLOB regarding the proposed revisions.  The revisions to these agencies’ minimization procedures were submitted to, and approved by the FISC, and will continue to be the subject of oversight by the joint oversight team.

(U)  SECTION 3:  TRENDS IN SECTION 702 TARGETING AND MINIMIZATION

(U)  In conducting the above-described oversight program, NSD, ODNI, and the agencies have collected a substantial amount of data regarding the implementation of Section 702.  In this section, a comprehensive collection of this data has been compiled in order to identify overall trends in the agencies’ targeting, minimization, and compliance.

(U)  I.  Trends in NSA Targeting and Minimization

(U)  NSA provides to the joint oversight team the average approximate number of facilities that were under collection on any given day during the reporting period.  Because the actual number of facilities tasked remains classified, the figure charting the average number of facilities under collection is classified as well.  Since the inception of the program, the total number of facilities under collection during each reporting period has steadily increased with the exception of two reporting periods that experienced minor decreases.

---

21 (U) The provided number of facilities on average subject to acquisition during the reporting period remains classified and is different from the unclassified estimated number of targets affected by Section 702 released by ODNI, most recently in its 2015 Transparency Report.  Previously, ODNI released transparency reports on June 26, 2014, (the 2013 Transparency Report) and on April 22, 2015 (the 2014 Transparency Report).  The classified numbers estimate the number of facilities subject to Section 702 acquisition, whereas the unclassified number provided in the Transparency Reports estimate the number of Section 702 targets.  As noted in the Transparency Reports, the number of 702 ‘targets’ reflects an estimate of the number of known users of particular facilities subject to intelligence collection under those Certifications.  Furthermore, the classified numbers of facilities account for the number of facilities subject to Section 702 acquisition during the current six month reporting period, whereas the Transparency Reports estimate the number of targets affected by Section 702 during the calendar year.

22 (U) One of the reporting periods in which the total number of facilities under collection decreased occurred prior to 2010 and is not reflected in the below chart.
More specifically, NSA reports that, on average, approximately [redacted] facilities were under collection pursuant to the applicable certifications on any given day during the reporting period. This represents a 2.9% increase from the approximately [redacted] facilities under collection on any given day in the last reporting period.

The above statistics describe the average number of facilities under collection at any given time during the reporting period. The total number of newly tasked facilities during the reporting period provides another useful metric. Classified Figure 5 charts the total monthly numbers of newly tasked facilities since September 2010.

---

23 (S//NF) The applicable certifications for this reporting period were [redacted].

24 (U) The term newly tasked facilities refers to any facility that was added to collection under a certification. This term includes any facility added to collection pursuant to the Section 702 targeting procedures; some of these newly tasked facilities are therefore facilities that had been previously tasked for collection, were detasked, and now have been retasked.
Figure 5: (TS//SI//NF) New Taskings by Month (Yearly Average for 2010 through 2014)

Specifically, NSA provided documentation of [redacted] new taskings during the reporting period. This represents a 14.0% increase in new taskings from the previous reporting period.

NSA tasked an average of [redacted] telephony facilities each month in 2014. During the first eleven months of 2015, NSA has tasked an average of [redacted] telephony facilities. This represents a [redacted] increase in the average monthly telephony facilities in the first eleven months of 2015 compared to 2014.

NSA tasked an average of [redacted] electronic communications accounts each month in 2014. During the first eleven months of 2015, NSA tasked an average of [redacted] electronic communication accounts (a [redacted] increase from 2014’s monthly average).
(U) With respect to minimization, NSA identified to the joint oversight team the number of serialized reports NSA generated based upon minimized Section 702-acquired data, and provided NSD and ODNI access to all reports NSA identified as containing United States person information. 26 Figure 6 contains the classified number of serialized reports and reports identified as containing United States person information over the last seven reporting periods. NSD and ODNI’s review revealed that the United States person information was at least initially masked in the vast majority of circumstances. 27 The number of serialized reports NSA has identified as containing United States person information slightly decreased this reporting period, compared to the prior reporting period. 28

26 (U) Previous joint assessments referred to these reports containing minimized Section 702- or Protect America Act (PAA)-acquired information. However, given that Section 702 of FAA replaced the PAA in 2008, the government no longer disseminates minimized information that was previously acquired pursuant to PAA. However, Figure 6 provides a trend analysis over a longer period of time and may include reports containing minimized PAA-acquired information in addition to minimized Section 702-acquired information.

27 (U) NSA generally “masks” United States person information by replacing the name or other identifying information of the United States person with a generic term, such as “United States person #1.” Agencies may request that NSA “unmask” the United States person identity. Prior to such unmasking, NSA must determine that the United States person’s identity is necessary to understand the foreign intelligence information.

28 (U) In the 2015 Transparency Report, in response to the PCLOB’s 702 Report Recommendation 9(5), NSA publicly released the number of Section 702 reports that contained U.S. person information for calendar year 2015, including delineating the number of times the U.S. person information was masked versus unmasked in those disseminated reports.
Figure 6: (S//NF) Total Disseminated NSA Serialized Reports Based Upon Section 702-Acquired Data and Number of Such Reports NSA Identified as Containing USP Information

Specifically, in this reporting period NSA identified to NSD and ODNI serialized reports based upon minimized Section 702-acquired data. This represents a 6.2% increase from the such serialized reports NSA identified in the prior reporting period. Figure 6 reflects NSA reporting over the last nine reporting periods; the fact that reporting based on Section 702-acquired data increased is consistent with prior reporting periods.

Figure 6 also shows the number of these serialized reports that NSA identified as containing United States person information. During this reporting period, NSA identified serialized reports as containing United States person information derived from Section 702-acquired data. The percentage of reports containing United States person information was lower this reporting period (9.0%), than the 9.7% and 9.8% reported in the two prior reporting periods.

---

29 (C//NF) NSA does not maintain records that allow it to readily determine, in the case of a report that includes information from several sources, from which source a reference to a U.S. person was derived. Accordingly, the references to U.S. person identities may have resulted from collection pursuant to Section 702 or from other authorized signals intelligence activity conducted by NSA that was reported in conjunction with information acquired under Section 702. Thus, the number provided above is assessed to likely be over-inclusive. NSA has previously provided this explanation in its Annual Review pursuant to Section 702(l)(3) that is provided to Congress.
II. Trends in FBI Targeting

(U) Under Section 702, NSA designates and submits facilities to FBI for acquisition of communications from certain facilities that have been previously approved for Section 702 acquisition under the NSA targeting procedures. FBI applies its own targeting procedures with regard to these designated accounts. FBI reports to the joint oversight team the specific number of facilities designated by NSA and the number of NSA designated-facilities that FBI approved. As detailed below, the number of facilities designated for acquisition has increased from the past reporting period, which is consistent with the general trend in prior reporting periods.

(U) As classified Figure 7 details, FBI approves the vast majority of NSA’s designated facilities and this percentage has been consistently high. The high level of approval can be attributed to the fact that the NSA-designated facilities have already been evaluated and found to meet NSA’s targeting procedures. FBI may not approve NSA’s request for acquisition of a designated facility for several reasons, including withdrawal of the request because the potential data to be acquired is no longer of foreign intelligence interest, or because FBI has uncovered information causing NSA and/or FBI to question whether the user or users of the facility are non-United States persons located outside the United States. Historically, the joint oversight team notes that for those accounts not approved by FBI, only a small portion were rejected on the basis that they were ineligible for Section 702 collection.

(U) Between 2010 and December 2014, the yearly average of designated facilities approved by FBI steadily increased. Between January and November 2015, the number of designated facilities approved by FBI each month has varied. NSD and ODNI have continued to track the number of facilities approved by FBI in 2015 and will incorporate this information into future Joint Assessments.
Specifically, FBI reports that NSA designated  accounts during the reporting period – an average of  designated accounts per month. This is an increase from the  accounts designated in the prior six-month reporting period.

FBI approved requests for
As indicated in the prior Joint Assessment, the Government was previously able to provide figures regarding the number of reports FBI had identified as containing minimized Section 702-acquired United States person information. However, in 2013, FBI transitioned much of its dissemination of Section 702-acquired information from FBI Headquarters to FBI field offices. NSD conducts oversight reviews at multiple FBI field offices each year, some of which ODNI attends, and during those reviews, NSD reviews a sample of the Section 702 disseminations issued by the respective field office. Because every field office is not reviewed every six months, NSD no longer has comprehensive numbers on the number of disseminations of Section 702-acquired United States person information made by FBI. FBI does, however, report comparable information on an annual basis to Congress and the FISC pursuant to 50 U.S.C. § 1881a(l)(3)(i).

III. Trends in CIA Minimization

CIA only identifies for NSD and ODNI disseminations of Section 702-acquired United States person information. Classified Figure 8 compiles the number of such disseminations of reports containing United States person information identified in the last nine reporting periods (June-November 2011 through the current period of June-November 2015). In the first six reporting periods, the number of CIA-identified disseminations containing United States person information, while always low, decreased. In the seventh, the number of CIA-identified disseminations containing United States person information, while still low, increased. In the last two reporting periods, the number of CIA-identified disseminations containing United States person information again decreased.
During this reporting period, CIA identified disseminations of Section 702-acquired data containing minimized United States person information. This is a decrease from the such disseminations CIA made in the prior reporting period. SD and ODNI, however, review all containing Section 702-acquired information that CIA has identified as potentially containing United States person information to ensure compliance with CIA’s minimization procedures.

CIA also tracks the number of files its personnel determine are appropriate for broader access and longer-term retention. CIA’s minimization procedures must be applied to these files before they are retained or transferred to systems with broader access. Classified Figure 9 details the total number of files that were either retained or transferred, as well as the number of those

In making these retention decisions, CIA personnel are required to identify any files potentially containing United States person information.
retained or transferred files that contain identified United States person information.\textsuperscript{35} Beginning in the middle of the reporting period covered by the thirteenth Joint Assessment (dated September 2015), CIA began reporting the number of files CIA transferred to systems with broader access, instead of the number of files retained in systems of limited access, as the number of transferred files provides a more accurate portrayal of CIA’s use of Section 702-acquired information. This current assessment reports the total number of files CIA transferred from June 2015 through November 2015. For reference, however, the number of files retained from prior assessment periods is also displayed in the Figure below.\textsuperscript{36} In all reporting periods, the number of retained or transferred files identified by CIA as potentially containing United States person information has been consistently a very small percentage of the total number of retained or transferred files.

\textsuperscript{35} (U) As reported in the eleventh Joint Assessment (October 2014), CIA determined in September 2014 that characterizations in prior assessments of the number of files having been “transferred” was not the most appropriate term as some files had been retained for long term retention but had not been transferred to systems of broader access. Consequently, the numbers of files for which CIA had made a retention decision were re-characterized as having been “retained.” Because the terms transferred and retained attempt to describe the same authorized actions under CIA’s Minimization Procedures, this Joint Assessment just refers to retention decisions.

\textsuperscript{36}
Figure 9: (S//NF) Total CIA Files Retained or Transferred and Total CIA Files that were Retained or Transferred Files Which Contained Potential United States Person Information

(S//NF) For this reporting period, CIA analysts transferred or retained [REDACTED] of which were identified by CIA as containing a communication with potential United States person information. This is a [REDACTED] decrease in the number of files transferred or retained, when compared to the previous reporting period when [REDACTED] of which contained potential United States person information.
(U) SECTION 4: COMPLIANCE ASSESSMENT – FINDINGS

(U) The joint oversight team finds that during this reporting period, the agencies have continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702. The personnel involved in implementing the authorities are appropriately directing their efforts at non-United States persons reasonably believed to be located outside the United States for the purpose of acquiring foreign intelligence information. Processes have been put in place to implement these authorities and to impose internal controls for compliance and verification purposes.

(U) The compliance incidents during the reporting period represent a very small percentage of the overall collection activity. Based upon a review of the reported compliance incidents, the joint oversight team does not believe that these incidents represent an intentional attempt to circumvent or violate the procedures required by the Act.

(U) As noted in prior reports, in the cooperative environment the implementing agencies have established, an action by one agency can result in an incident of noncompliance with another agency’s procedures. It is also important to note that a single incident can have broader implications.

(U) Each of the compliance incidents for this current reporting period are described in detail in the corresponding Section 707 Report. The Joint Assessment provides NSD and ODNI’s analysis of these compliance incidents in an effort to identify existing patterns or trends that might identify the underlying causes of those incidents. The joint oversight team then considers whether and how those underlying causes could be addressed through additional remedial or proactive measures and assesses whether the agency involved has implemented appropriate procedures to prevent recurrences. The joint oversight team continues to assist in the development of such measures, some of which are detailed below, especially as it pertains to investigating whether additional and/or new system automation may assist in preventing compliance incidents.

(U) I. Compliance Incidents – General

(U) A. Statistical Data Relating To Compliance Incidents

(S//NF) As noted in the Section 707 Report, there were a total of compliance incidents that involved noncompliance with NSA’s targeting or minimization procedures and compliance incidents involving noncompliance with FBI’s targeting and minimization procedures, for a total of incidents involving NSA and/or FBI procedures. During this reporting period, there was one identified incident of noncompliance with CIA’s minimization procedures, and no identified instances of noncompliance by an electronic communication service provider issued a directive pursuant to Section 702(h) of FISA.

37 (U) As is discussed in the Section 707 report and herein, some compliance incidents involve more than one element of the Intelligence Community. Incidents have therefore been grouped not by the agency “at fault,” but instead by the set of procedures with which actions have been noncompliant.
(U) The following table puts these compliance incidents in the context of the average number of facilities subject to acquisition on any given day\(^{38}\) during the reporting period:

**Figure 10: (TS//SI//NF) Compliance Incident Rate**

| Compliance incidents during reporting period (June 1, 2015 – November 30, 2015) |   |
| Number of facilities on average subject to acquisition during the reporting period |   |
| Compliance incident rate: number of incidents divided by average facilities subject to acquisition | 0.53% |

(U) The compliance incident rate continues to remain low, well below one percent. The compliance incident rate of 0.53% represents an increase from the 0.35% compliance incident rate in the prior reporting period, however, this increase is largely attributable to two types of errors discussed further below.\(^{39}\) The number of notification delays remained low during this reporting period. If the notification delays incidents are not included in the calculation, the overall compliance incident rate for this reporting period is actually 0.50% which is still higher than the prior period’s 0.32%. This information is explained below and detailed in Figure 11.

(U) While the incident rate remains low, this percentage in and of itself does not provide a full measure of compliance in the program. A single incident, for example, may have broad ramifications and may involve multiple facilities. Other incidents, such as notification delays (described further below) may occur with frequency, but have limited significance with respect to United States person information.\(^{40}\)

---

\(^{38}\) (S//NF) He Attorney General’s Section 707 report provides further details with respect to any particular incident.

\(^{39}\) The Joint Assessment has traditionally compared the number of compliance incidents to the number of average tasked facilities. Using the number of average facilities subject to acquisition as the denominator provides a general proxy for an activity level that is relevant from a compliance perspective. That is, the joint oversight team believes that the number of targeted facilities generally comports with the number of activities that could result in compliance incidents (e.g. taskings, detaskings, disseminations, and queries). Tracking this rate over consecutive years allows one to discern general trends as to how the Section 702 program is functioning overall from a compliance standpoint.
The joint oversight team assesses that another measure of substantive compliance with the applicable targeting and minimization procedures is to compare the compliance incident rate excluding these notification delays. The following Figure 11 shows this adjusted rate:

**Figure 11: (U) Compliance Incident Rate (as the number of incidents divided by the number of average facilities tasked), Not including Notification Delays**

(U) As Figure 11 demonstrates, the adjusted compliance incident rate calculated without the notification delays is 0.50%, which is higher than what was reported in the prior reporting period (0.32%) but still well below 1%. The joint oversight team assesses that the consistently low compliance incident rate of less than 1% is a result of training, internal processes designed to identify and remediate potential compliance issues, and a continued focus by internal and external oversight personnel to ensure compliance with the applicable targeting and minimization procedures. In addition, although there was an increase in the compliance incident rate this period, NSA has taken steps to address some of the causes of these incidents, which are discussed further below.
(U) **B. Categories of Compliance Incidents**

(U) Most of the compliance incidents occurring during the reporting period involved non-compliance with the NSA’s targeting or minimization procedures. This largely reflects the centrality of NSA’s targeting and minimization efforts in the Government’s implementation of the Section 702 authority. The compliance incidents involving NSA’s targeting or minimization procedures have generally fallen into the following categories:

- **(U) Tasking Issues.** This category involves incidents where noncompliance with the targeting procedures resulted in an error in the initial tasking of the facility.

- **(U) Detasking Issues.** This category involves incidents in which the facility was properly tasked in accordance with the targeting procedures, but errors in the detasking of the facility caused noncompliance with the targeting procedures.

- **(U) Notification Delays.** The category involves incidents in which a facility was properly tasked in accordance with the targeting procedures, but a notification requirement contained in the targeting procedures was not satisfied.

- **(U) Documentation Issues.** This category involves incidents where the determination to target a facility was not properly documented as required by the targeting procedures.\(^41\)

- **(U) Minimization Issues.** This category involves NSA’s compliance with its minimization procedures.

- **(U) Other Issues.** This category involves incidents that do not fall into one of the six above categories.

In some instances, an incident may involve more than one category of noncompliance.

(U) These categories are helpful for purposes of reporting and understanding the compliance incidents. Because the actual number of incidents remains classified, Figure 12A depicts the percentage of compliance incidents in each category that occurred during this reporting period, whereas Figure 12B provides that actual classified number of incidents.

---

\(^{41}\) (U) As described in the Section 707 Report, not all documentation errors are separately enumerated as compliance incidents.
Figure 12A: (U) Percentage Breakdown of Compliance Incidents Involving the NSA Targeting and Minimization Procedures

Figure 12B: (S//NF) Number of Compliance Incidents Involving the NSA Targeting and Minimization Procedures
(U) As Figures 12A and B demonstrate, the proportion of notification delays, which used to constitute the predominant share of incidents, has been substantially reduced. Tasking and detasking incidents often involve more substantive compliance incidents insofar as they can (but do not always) involve collection involving a facility used by a United States person or an individual located in the United States. Furthermore, incidents of noncompliance with minimization procedures are also a focus of the joint oversight team because these types of incidents may involve information concerning United States persons.

(S//NF) More specifically, the number of tasking incidents increased [redacted]; detasking incidents increased [redacted]; minimization incidents increased [redacted]; documentation incidents decreased [redacted]; and “other” category incidents decreased [redacted]. The number of notification delays decreased [redacted]. Additionally, as with the previous reporting period, there were no overcollection incidents in the current reporting period.

(U) The following chart, Figure 13, depicts the compliance incident rates, as compared to the average facilities on task, for tasking and detasking incidents over the previous reporting periods. While these tasking and detasking incidents are grouped in a single chart for a comparison, the tasking and detasking incidents are not relational to each other, i.e. an increase or decrease in the rate of tasking incidents does not result in an increase or decrease in the detasking incident rate.

---

42 (S//NF) The joint oversight team is examining whether it should revise the counting of documentation errors to address NSA’s revised targeting procedures. The targeting procedures approved by the FISC in November 2015 included a new documentation requirement that NSA provide a written explanation of the basis for the assessment, at the time of targeting, that the target possesses, is expected to receive, and/or is likely to communicate foreign intelligence information concerning the foreign power or foreign territory that is covered by the certification under which the accounts were tasked. The revised targeting procedures with this new documentation requirement was made pursuant to a PCLOB recommendation, as discussed above. An update will be provided in the subsequent joint assessment as appropriate.
(U) Over the time periods covered in the above chart, the tasking and detasking incident compliance rate has varied by fractions of a percentage point as compared to the average size of the collection. Tasking errors cover a variety of incidents, ranging from the tasking of an account that the Government should have known was used by a United States person or an individual located in the United States to typographical errors in the initial tasking of the account that affect no United States persons or persons located in the United States. On the other hand, detasking errors more often involve a facility used by a United States person or an individual located in the United States, who may or may not have been the targeted user. The percentage of compliance incidents involving such detasking incidents has remained consistently low.

(U) With respect to FBI’s targeting and minimization procedures, incidents of non-compliance with the FBI targeting procedures decreased from the rate of 0.01% in the prior reporting period to a rate below 0.01% in the current reporting period. The total number of
identified minimization errors also remains low. The joint oversight team assesses that FBI’s overall compliance with its targeting and minimization procedures is a result of FBI’s training and the processes it has designed to effectuate its procedures.

(U) Furthermore, there was one incident during this reporting period that involved CIA’s minimization procedures, which is the same amount of incidents that occurred during the previous reporting period for CIA. The joint oversight team assesses that CIA’s compliance is a result of its training, systems and processes that were implemented when the Section 702 program was developed to ensure compliance with its minimization procedures, and the work of its internal oversight team.

(S//NF) Finally, there were no incidents of non-compliance caused by errors made by a communications service provider in this reporting period, which represents a decrease from the incidents reported in the prior reporting period. The joint oversight team assesses that the low number of errors by the communications service providers is the result of continuous efforts by the Government and providers to ensure that lawful intercept systems effectively comply with the law while protecting the privacy of the providers’ customers.

(U) II. Review of Compliance Incidents – NSA Targeting and Minimization Procedures

(U) As with the prior Joint Assessment, this Joint Assessment takes a broad approach and discusses the trends, patterns, and underlying causes of the compliance incidents reported in the Section 707 Report. The joint oversight team believes that analyzing the trends of these incidents, especially in regard to their causes, helps the agencies focus resources, avoid future incidents, and improve overall compliance. The Joint Assessment primarily focuses on incidents involving NSA’s targeting and minimization procedures, the volume and nature of which are better-suited to detecting such patterns and trends. The following subsections examine incidents of non-compliance involving NSA’s targeting and minimization procedures. Most of these incidents did not involve United States persons, and instead involved matters such as typographical or other tasking errors, detasking delays with respect to facilities used by non-United States persons who may have entered the United States, or notification delays. Some incidents during this reporting period did, however, involve United States persons. United States persons were primarily impacted by: (1) tasking errors that led to the tasking of facilities used by United States persons; (2) delays in detasking facilities after NSA determined that the user of the facility was a United States person; and (3) non-compliance with the NSA’s minimization procedures involving the unintentional improper dissemination, retention, or querying of Section 702 information.
(U) In the subsections that follow, this Joint Assessment examines some of the underlying causes of non-compliance, focusing on incidents in this period that contributed to the increased compliance incident rate of 0.53%. In the previous reporting period, the compliance incident rate was 0.35%, which was consistent with the historical compliance incident rate. While the current incident rate still remains well under 1%, the joint oversight team found its increase significant and ultimately determined that the overall incident rate was significantly impacted by two types of tasking errors. This Joint Assessment first begins by examining these two subsets of tasking incidents that contributed to a majority of the tasking errors, even though the majority of these tasking errors did not impact United States persons. This Joint Assessment then focuses on examining and explaining incidents that have the greatest potential to impact United States persons’ privacy interests, even though those incidents represent a minority of the overall incidents.

(U) A. Errors That Resulted in the Increased Number of Tasking Incidents

(U) During this reporting period, the joint oversight team attributed the overall increase in incidents to an increase in two particular types of tasking incidents caused by agency personnel misapplying the requirements of NSA’s targeting procedures; these accounted for 72% of all tasking incidents. First, 49% of tasking incidents were caused by one particular target office misunderstanding the requirements of the targeting procedures. Second, 23% of tasking errors involved NSA failing to conduct a necessary foreignness check (i.e. checking that a targeted user is reasonably believed to be located outside the United States) prior to tasking a facility or NSA allowing too long of a delay between the necessary foreignness check and the actual tasking of the facility.

(U) 1. Incidents that Contributed to 49% of the Tasking Errors Due to a Misunderstanding by a Single NSA Targeting Office

(U) As noted above, 49% of the tasking errors identified during this reporting period were attributed to a misunderstanding by a single target office. The joint oversight team discovered this incident as part of its bi-monthly oversight review of newly tasked facilities, all of which are reviewed by NSD. NSD requested that NSA provide additional information about the connection between the targeted users of certain tasked facilities and the particular certification under which those facilities were tasked. After additional research, NSA advised that this particular target office

---

47 (U) While ODNI and DOJ strive to maintain consistency in the headings of these subsections, these headings may nonetheless change with each joint assessment depending on the incidents that occurred in each reporting period and their respective underlying causes.
had erroneously tasked those facilities under circumstances in which it did not have sufficient information to assess that the user would possess, receive, and/or communicate foreign intelligence information about the certification under which those facilities were targeted. While NSA analysts in this office believed that the targeted users were appropriately connected to the certification under which they were tasked, those analysts erroneously failed to utilize additional NSA resources to support their assessment and, therefore, could not reasonably determine, as required by the targeting procedures, whether or not targeting those facilities would likely produce the requisite foreign intelligence information. As a result of this incident, NSA required the target office to retake the NSA’s formal Section 702 online training course, and NSA issued guidance to all personnel involved in the Section 702 targeting process regarding the requirement in the targeting procedures that NSA must reasonably assess, based on the totality of the circumstances, that the target is expected to possess, receive, and/or likely communicate foreign intelligence information.

(U) 2. Incidents that Contributed to 23% of the Tasking Errors Due to Failing to Conduct the Required and Timely Foreignness Checks

(U) In 23% of the tasking incidents, NSA did not properly establish a sufficient basis to assess that the target was located outside the United States because NSA analysts either failed to conduct the required foreignness check or failed to conduct the required foreignness check in a timely manner. Even though these types of errors accounted for 23% of the tasking incidents during this reporting period, it was a decrease in these types of errors compared to the last reporting period (which was 56%). In all of these incidents during the current reporting period, NSA advised that there was no indication that the selectors were used by a United States person or by someone in the United States. NSA further advised that the relevant personnel were reminded of the Section 702 tasking requirements. Additionally, in an attempt to reduce these types of tasking errors in the future, NSA conducted refresher training, beginning in October/November 2015, for all NSA targeting adjudicators about the required pre-tasking checks. The joint oversight team continues to work with NSA to ensure that appropriate additional training efforts are utilized to further reduce these types of tasking incidents.
(U) C. Compliance Incidents Related to Incomplete Purges

(U) During this reporting period, there was an increase in the number of incidents involving the incomplete purge of information as required by NSA’s Section 702 minimization procedures, whereas in the previous reporting period no such incidents occurred.\(^57\) While this number of incidents is not entirely in line with historic reporting, as discussed further below, some of the incidents were the result of NSA proactively conducting purge verification assessments and are not further analyzed or discussed below (although the Section 707 report provides a detailed discussion of such).\(^58\) However, discussed below, are those purge incidents where NSA’s technical processes for identifying data subject to purge were not fully detecting all collection that needed to be purged or were not completely purging the required information.\(^59\) Furthermore, two additional incidents (discussed below) involved incomplete purges in specific systems – these two incidents had more substantial implications than other incidents and were the subject of multiple filings and compliance hearings before the FISC in connection with the 2015 Section 702 Certification renewal.\(^60\)

(U) The first step in any required purge is to identify what data must be purged. In some instances, NSA’s technical processes failed to properly identify the data required to be purged or failed to fully detect all of the data required to be purged (i.e. incomplete purges), which resulted in compliance incidents due to the incomplete removal of data subject to purge. To address these purge incidents affected by technical processes, NSA undertook activities to: (a) verify that data required to be purged has been removed from the applicable NSA systems\(^61\) (i.e. purge verification assessments) and (b) identify and resolve issues with its purge process when incomplete purges are identified. For example, NSA has continued to conduct purge verification assessments by comparing a sample of data that was added to NSA’s Master Purge List (MPL)\(^62\) between a certain

\(^{57}\) These applicable NSA systems are known as SIGINT Collection Source Systems of Record (SC-SSRs). Any system designated by NSA as an SC-SSR must employ a purge protocol to verify that information is purged when the system receives a request to destroy SIGINT information that NSA is not authorized to retain.

\(^{60}\) The Section 707 report provides further details as to the operation of the MPL.
date range with the data in an NSA system. The purpose is for NSA to identify whether the underlying data has in fact been purged from NSA’s systems as required. In addition, NSA performed a full comparison of the MPL with the data in NSA’s SC-SSRs. As a result of this MPL comparison process, NSA has identified incomplete purges in some of its SC-SSRs. NSA has been able to identify causes for these incomplete purges and has worked to develop solutions to address the root causes.

(U) Two incidents involving incomplete purges had more substantial implications than the other purge incidents. These two incidents were the subject of multiple filings and compliance hearings before the FISC in connection with the 2015 Section 702 Certification renewal and were addressed by the FISC in its November 6, 2015 Memorandum Opinion and Order.

(U) In the first incident, the Government explained that two particular NSA Mission Management Systems (MMS) had not historically conducted required purges of records from those systems. The first MMS had been marking and limiting access to Section 702-acquired data subject to purge. However, this MMS had not deleted or aged-off the data subject to purge; furthermore, domestic communications that had been marked for deletion in other systems and added to NSA’s MPL had not been historically purged from this MMS. NSA re-designed this MMS so that it would properly remove records subject to purge going forward. Additionally, NSA completed the removal in this MMS of historic Section 702-acquired data subject to purge and the historic domestic communications that had been marked for deletion and added to the MPL. However, NSA continues to work to develop a technical solution for this MMS to age-off applicable Section 702-acquired information.

(U) In the same incident, the Government explained that that a second MMS had been improperly purging information and that the incomplete purges potentially affected information collected pursuant to Section 702. NSA identified a system error in this second system as the cause for these incomplete purges. To remedy this error, NSA redesigned this second MMS to compare, on a daily basis, data in its system with all identifiers listed on the MPL. Thus, records associated with object identifiers listed on the MPL in purge state are now being appropriately deleted from this second MMS. This second MMS had also failed to properly age-off FISA-acquired information. This system now ages off data older than one year and no longer contains FISA-acquired information. The joint oversight team assesses that this incident highlights the importance for agency personnel to ensure that databases used to store Section 702 FISA-acquired information are configured appropriately to meet purge, deletion, and age-off requirements. This incident also demonstrates the need to have agency personnel work with the joint oversight team to
try to address potential issues in systems before those systems actually contain Section 702-acquired information.

(U) In the second more substantial incident,68 the Government reported that Section 702-acquired information subject to purge or age-off was being erroneously kept in two other NSA MMS (separate systems from those detailed above).69 Here, the first MMS is used in the pre-tasking process where NSA analysts most commonly use it as part of a determination of whether a facility can be properly tasked under Section 702. The second MMS is used in the post-tasking process where NSA analysts use it to perform checks to identify indications that a Section 702 target may be located in the United States. If these systems do not function properly, NSA analysts may not have the appropriate information at hand to fulfill the requirements of its targeting procedures to ensure that NSA reasonably believes the tasked facility is used by a non-United States person located outside the United States.

(U) Following a hearing during which the FISC addressed this particular incident, the FISC required the Government to justify the retention and use of data that was otherwise subject to purge in these two MMS databases.70 After receipt of the Government’s justification, the FISC addressed this matter in its November 6, 2015 Memorandum Opinion and Order. The FISC agreed that NSA’s Section 702 minimization procedures do not prohibit NSA from keeping data in these two MMS databases that is derived from domestic communications placed on the MPL (i.e. subject to purge) for the purpose of collection avoidance. However, the FISC voiced concern as to whether the retention of other categories of information subject to purge in those two MMS databases comply with NSA’s targeting and minimization procedures and, thus, ordered additional Government reporting on this topic. Subsequently, the Government reported that NSA would delete from these two MMS databases all data collected as a result of unauthorized electronic surveillance as well as all other categories of information subject to purge pursuant to its targeting and

---

68  
69  
70
minimization procedures. NSA detailed for the FISC a three-phase plan to effectuate required age-off, historic purge and prospective compliance with purge requirements.

(U) The joint oversight team believes that these compliance incidents and other historical CIA, FBI, and NSA purge-related incidents indicate that the Government must remain vigilant to ensure the appropriate and timely removal of data. As with prior Joint Assessments, the joint oversight team believes it is important for NSA to carefully consider the potential impacts on the purge process when NSA designs and updates its systems. Because the identification and destruction of relevant data can be complex, the joint oversight team also believes that NSA must continue to regularly monitor and re-evaluate the functioning of relevant systems. Finally, the joint oversight team continues to remain focused working with all three agencies to ensure the appropriate purging of data. For example, during this last reporting period, the joint oversight team continued to have conference calls and in-person meetings with NSA and FBI as it pertained to their purging of data.

(U) D. Effect of Other Technical Issues

(U) There were a small number of compliance incidents resulting from technical issues (other than the purge incidents discussed above) during this reporting period. Technical issues potentially have larger implications than other incidents because technical issues: often involve more than one facility; can remain undetected and uncorrected for a long period of time; and can proliferate dramatically in a short time period, including across numerous interconnected systems. As such, all agencies involved in the Section 702 program devote substantial resources towards the prevention, identification, and remedy of technical issues. Collection equipment and other related systems undergo substantial testing prior to deployment. The agencies also employ a variety of monitoring programs to detect anomalies in order to prevent or limit the effect of technical issues on acquisition. Members of the joint oversight team participate in technical briefings at the various agencies to better understand how technical system development and modifications affect the collection and processing of information. As a result of these efforts, potential issues have been identified, the resolution of which prevented compliance incidents from happening and ensured the continued flow of foreign intelligence information to the agencies. The joint oversight team believes that the historically limited number of overcollection incidents is the result of the efforts of all of the involved agencies. While technical issues can potentially have larger implications, this potential was largely avoided during this reporting period.

(U) Specifically, the technical issues that resulted in delayed detaskings were caused by data becoming corrupted, data not being properly processed due to a server backlog, and system errors. In these instances, the technology and systems failed to function as designed, and, thus, the systems failed. This resulted in delayed detasking incidents, whereby NSA was unable to timely detask facilities. NSA subsequently corrected these technical issues. Additionally, none of the users of the facilities at issue were believed to be United States persons.
In another incident, NSA discovered that, due to a technical issue, (1) one NSA system failed to generate the tasking record (i.e. tasking sheet) for NSD and ODNI to review to ensure NSA compliance with NSA targeting procedures, and (2) an NSA system failed to receive tasking information that enables NSA to conduct required post-tasking analysis. Once a facility has been appropriately tasked, NSA has the obligation to ensure, post-tasking, that the facility remains appropriately tasked - i.e. that NSA reasonably believes that the non-United States person user of the tasked facility continues to be located outside the United States and that the tasking will provide foreign intelligence information. NSA subsequently provided the tasking sheets to the joint oversight team who is reviewing them to determine that the facilities contained on those sheets were appropriately tasked. This technical issue was corrected in October 2015.

E. Effect of Human Errors

As reported in previous Joint Assessments, human errors caused some of the identified compliance incidents. Each of the agencies has established a variety of processes to both reduce human errors and to identify such errors when they occur. These processes have helped to limit such errors, but some categories of human errors are unlikely to be entirely eliminated. For example, despite multiple pre-tasking checks, instances of typographical errors or similar errors occurred in the targeting process that caused NSA to enter the wrong facility into the collection system. Such typographical errors accounted for approximately 4% of the tasking errors made in this reporting period, which is a decrease from the previous reporting period, in which typographical errors accounted for 8% of the tasking errors. Furthermore, no such incidents during this reporting period resulted in the tasking of a facility used by a United States person or person in the United States. Approximately 14% of the detasking delays from this reporting period were the result of inadvertent errors, such as an NSA analyst detasking some, but not all, of a target’s facilities that required detasking. As discussed below, approximately 21% of the
detasking delays were the result of faulty analysis or misunderstanding of procedures. As with other compliance incidents, any data acquired as a result of such tasking and detasking errors - regardless of whether or not the user proves to be a United States person or person in the United States - is required to be purged.

(U) NSA’s minimization procedures prescribe rules for using United States person identifiers to query Section 702-acquired data including that: (a) the queries be designed in a manner “reasonably likely to return foreign intelligence information;” (b) the queries are first approved in accordance with NSA’s internal procedures; and (c) the queries of Internet communications acquired through NSA’s upstream collection techniques are prohibited. During this reporting period, approximately 56% of the minimization procedures errors involved non-compliance with the minimization rules regarding queries (whereas it was approximately 78% in the previous reporting period). As with prior Joint Assessments, query incidents remain the cause of most compliance incidents involving NSA’s minimization procedures.

(U) Specifically, during this reporting period, just over half of the query incidents involved overly broad queries. These overly broad query errors are typically traceable to a typographical or comparable error in the construction for the query. For example, an overly broad query can be caused when an analyst mistakenly inserts an “or” instead of an “and” in constructing a Boolean query, and thereby potentially received overly broad results as a result of the query. As with previous reporting periods, there were no incidents of an analyst purposely running a query for non-foreign intelligence purposes against Section 702-acquired data identified during the reporting period.

(U) The remaining query incidents involved NSA analysts: (a) using United States person identifiers which had not been approved pursuant to NSA’s internal procedures to query Section 702-acquired data; (b) exceeding the scope of the authorization provided under NSA’s internal procedures; and/or (c) using approved United States person identifiers to query Internet communications acquired through NSA’s upstream collection techniques. For example, in one incident, a NSA analyst received the appropriate approval to use a United States person identifier to query Section 702-acquired data (excluding upstream). However, due to a misunderstanding, the analyst continued to use the United States person identifier as a query term past the approval’s expiration date. NSA discovered the error over three months later; the NSA target office discontinued the queries the same day the error was discovered. NSA advised that all results from the unauthorized use of the United States person identifier as a query term were deleted. NSA further advised that the relevant personnel were reminded of the Section 702 query requirements.
(U) The joint oversight team assesses that the overall rate of the types of errors described above is low. The joint oversight team believes that the low rate reflects the great care analysts use to enter information, the effectiveness of the NSA pre-tasking review process in catching potential errors, and the focus in NSA training and oversight in constructing reasonably designed queries.

(U) While the joint oversight team assesses that existing practices and systems adequately reduce the number of incidents discussed above, the joint oversight team assesses that other errors could potentially be reduced with new training, procedures or system modifications. The following subdivides such incidents into errors that could be potentially reduced through system or process changes, and those that could be addressed through training. Independent of the broader system, process, or training changes suggested below, in each of the individual incidents discussed below, data acquired as a result of the specific incidents has been purged and the personnel directly involved have been reinstructed regarding the applicable requirements.

(U) (1) Errors That Could Be Reduced Through System/Process Changes

(S//SI//NF) In prior Joint Assessments, the joint oversight team suggested that NSA consider making changes to its tasking tool and query tool. Specifically, the joint oversight team proposed two changes be made to NSA’s tasking tool. NSA subsequently implemented both proposed changes and modified its tasking tool. First, NSA’s tasking tool was configured in such a manner that could result in the unintentional retasking of a facility without the application of the NSA targeting procedures. Such incidents were identified during this reporting period. NSA modified its tasking tool so that requests from CIA and FBI, detasked facilities previously could have been erroneously retasked without application of the NSA targeting procedures unless NSA personnel verified that the facility was currently subject to Section 702 acquisition; one such error occurred during this reporting period. To resolve this issue, NSA modified its targeting tool to

80 (U) In a letter dated October 27, 2015, the U.S. House of Representatives Permanent Select Committee on Intelligence (HPSCI) requested that the Director of National Intelligence submit a report about specific questions contained in the letter pertaining to Section 702, including an update on the “status of the proposed changes [DOJ] suggested the [NSA] make to its tasking tool for Section 702 queries” and references the previous Joint Assessment (hereafter the HPSCI October 2015 letter). This HPSCI October 2015 letter also requested that the report evaluate “the possibility of including additional mechanisms for analyzing the foreignness of a target pre- and post-tasking.”

81 (U) On February 16, 2016, ODNI provided HPSCI with a report in response to the HPSCI October 2015 letter. The ODNI report, Assessment of Oversight and Compliance with Targeting Procedures (hereafter the ODNI February 2016 report), evaluated the process by which IC elements task foreign intelligence targets under Section 702, including providing an update on the status of proposed modifications DOJ and ODNI suggested in previous Joint Assessments that NSA make to its tools related to tasking and querying.
prevent those types of tasking requests to proceed; now the modification requires a NSA employee to specify that a tasking request is being requested pursuant to Section 702. This modification was completed in January 2016.83

(U) While modifying NSA’s tasking tool would have prevented these two methods of erroneously retasking facilities, these modifications would eliminate only 2% of the tasking errors that occurred in this reporting period. Such modifications would have eliminated 5% and 8% of tasking errors in the prior two reporting periods, respectively. Thus, these types of modifications could potentially reduce the already very small overall compliance incident rate.

(U) Additionally, as noted in prior Joint assessments, the joint oversight team believes NSA should assess modifications to systems used to query raw Section 702-acquired data to require analysts to identify when they believe they are using a United States person identifier as a query term. Such an improvement, even if it cannot be adopted universally in all NSA systems, could help prevent compliance instances with respect to the use of United States person query terms.84 In response to this recommended modification, NSA developed a potential solution and plans to test and implement it during calendar year 2016. Specifically, the solution being developed for NSA data repositories containing unevaluated and unminimized Section 702 information will require analysts to document whether the query being executed includes a known United States person identifier. Once the query is executed, the details concerning the query will be passed to NSA’s auditing system of record for post-query review and potential metrics compilation. As part of the testing, NSA will evaluate the accuracy of reporting this number in future Joint Assessments.85

(U) Additionally, the PCLOB, in its Section 702 report, recommended that NSA implement processes to annually count “the number of queries performed that employ U.S. person identifiers, specifically distinguishing the number of such queries that include names, titles or other identifiers potentially associated with individuals.” PCLOB’s Section 702 Report Recommendation 9(4). In the Section 707 Report, the Department of Justice reports (a) the number of metadata queries that use a United States person identifier and (b) the number of United States person identifiers approved for content queries. NSA subsequently declassified these numbers relating to calendar year 2015 metrics so as to report those numbers publicly as part of ODNI’s 2015 Transparency Report.

83 (U) As it pertains to recommended modifications to NSA’s tasking tool, the ODNI February 2016 report indicated that NSA was reviewing the recommendation and planned to engage in further discussions with DOJ and ODNI. The above information updates the information in the ODNI February 2016 report.

84

85 (U) As it pertain to recommended modifications to NSA’s query tool, the ODNI February 2016 report indicated that NSA planned to test and implement this recommendation during calendar year 2016 and also explained how the new modified compliance control mechanism would function.
(U) (2) Errors Caused by Misunderstandings of Processes or Procedures That Can Be Addressed Through Training

(U) Consistent with the general increase in the number of compliance incidents during this reporting period, the joint oversight team has identified a slight increase of incidents caused by analysts, officers, or agents misunderstanding or misapplying the requirements of NSA’s targeting or minimization procedures. A number of incidents identified during this reporting period (including the incident described above where one office misunderstood or misapplied the targeting procedures resulting in a significant number of tasking incidents from a single office)\(^8^6\) were attributable, to varying degrees, to a misunderstanding or misapplication of these rules. The overall number of such incidents compared to the number of targeting, detasking, and minimization decisions made by Government personnel remains very low, and the particular aspects of the procedures misunderstood or misapplied were diverse. The below-described incidents are examples of agency personnel misapplying the requirements of NSA’s targeting or minimization procedures, which resulted in either the inadvertent targeting of a U.S. person or the dissemination of information of or concerning a U.S. person that did not meet the requirements in the minimization procedures.

(U) For example, in two incidents, NSA personnel did not understand what efforts they were required to undertake to ascertain whether a targeted user was a United States person prior to tasking. These errors resulted in United States persons being erroneously tasked; however, upon discovering the tasking errors, NSA detasked the users’ facilities and ensured that all necessary purge requirements were completed. NSA further advised that the relevant personnel have been reminded of the Section 702 tasking requirements. In a third incident, an analyst did not understand the minimization requirements with regard to disseminating information concerning a United States person.
(U) The joint oversight team assesses that the low overall rate of such incidents and the fact that such incidents are not overly concentrated in any particular area generally reflects the strength of the agencies training programs.

(U) G. Intra- and Inter-Agency Communications

(U) Section 702 compliance requires good communication and coordination within and between agencies. In order to ensure targeting decisions are made based on the totality of the circumstances and after the exercise of due diligence, those involved in the targeting decision must communicate the relevant facts to each other. Analysts also must have access to the necessary records that inform such decisions. Good communication among analysts is also needed to ensure that facilities are promptly detasked when it is determined that the Government has lost its reasonable basis for assessing that the facility is used by a non-United States person reasonably believed to be located outside the United States for the purpose of acquiring foreign intelligence information. Furthermore, query rules regarding United States person identifiers and dissemination
decisions regarding United States person information require inter- and intra-agency communications regarding who the Government has determined to be a United States person.

(U) In general, the joint oversight team found that better communication and coordination between and among the agencies reduced certain types of errors from occurring during this reporting period. Still, in this reporting period, miscommunications resulted in errors and the joint oversight team assesses that there is room for continued improvement: approximately 6% (down from the prior reporting period’s 15%) of the detasking delays that occurred were attributable to miscommunications or delays in communicating relevant facts. Significantly, however, none of the inter- or intra-agency miscommunications resulted in the erroneous tasking, or the delay in the detasking, of a facility used by a United States person.

(U) The joint oversight team believes that agencies should continue their training efforts to ensure that appropriate protocols continue to be utilized. As part of its on-going oversight efforts, the joint oversight team will also continue to monitor NSA, CIA and FBI’s Section 702 activities and practices to ensure that the agencies maintain efficient and effective channels of communication.

(U) **III. Review of Compliance Incidents – CIA Minimization Procedures**

(S//NF) During this reporting period, there was only one incident involving noncompliance with the CIA minimization procedures, which is the same number that occurred during the previous reporting period.

(U) CIA’s sole compliance incident involved the untimely destruction of Section 702-acquired data as is required by its minimization procedures. CIA’s Section 702 Minimization Procedures require that CIA delete unminimized communications that may contain United States person information no later than five years from the expiration date of the Section 702 certification authorizing the collection. In this incident, the applicable data that was required to be deleted was not deleted due to a technical issue and that data remained in one of CIA’s systems for less than two weeks past the deletion deadline. CIA advised that it made no use of the information that was improperly retained for the short period of time.

(U) **IV. Review of Compliance Incidents – FBI Targeting and Minimization Procedures**

(U) There were a minimal number of incidents involving noncompliance with the FBI targeting and minimization procedures in this reporting period. As a percentage of FBI’s targeting actions during the reporting period, the FBI targeting compliance incident rate during this reporting
period decreased from 0.01% to almost zero. The one targeting incident in this reporting period was a process issue that was narrow in impact, and did not involve the targeting of a United States person or person located in the United States.\(^90\)

\(^{(S//NF)}\) The minimal number of incidents involving noncompliance with FBI’s minimization procedures resulted from misapplication or misunderstanding of the procedures by FBI employees and from technical issues.\(^91\) For example, one of the minimization incidents involved the improper querying of Section 702-acquired data which was caused by an FBI employee misunderstanding the rule.\(^92\) Specifically, FBI reminded the employee of the minimization procedures’ requirement concerning queries.
(U) The previous joint assessment discussed two minimization errors that involved the improper dissemination of United States person information. While no such errors of this type occurred during this current reporting period, the previous joint assessment explained that FBI had recalled five of the seven improper disseminations and further explained that, at that time, FBI was continuing to discuss the remaining two improper disseminations with NSD. This discussion between FBI and NSD continued through this and subsequent reporting periods.

(U) **V. Review of Compliance Incidents – Provider Errors**

(U) During this reporting period, there were no incidents (as opposed to minimal incidents during the last reporting period) of noncompliance by an electronic communication service provider with a Section 702(h) directive. Given that errors by the service providers can result in the acquisition of United States person information, the Government must actively monitor the acquisitions that the providers transmit to the Government. The joint oversight team believes that the historically low number of compliance incidents caused by service providers reflect, in part, the service providers’ commitment to comply with the law while protecting their customers’ interests. However, the low number of these incidents also reflects continued efforts by the Government and service providers to ensure that lawful intercept systems are effective and compliant with all applicable law and other requirements. The Government must continue to work with the service providers to prevent future incidents of non-compliance.

(U) **SECTION 5: CONCLUSION**

(U) During the reporting period, the joint oversight team found that the agencies have continued to implement the procedures and to follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702. As in previous reporting periods, the joint oversight team has identified no indications of any intentional or willful attempts to violate or circumvent the requirements of the Act in the compliance incidents assessed herein. Although the number of compliance incidents continued to remain small, particularly when compared with the total amount of collection activity, a continued focus is needed to address underlying causes of the incidents which did occur. The joint oversight team assesses that such focus should emphasize maintaining close monitoring of collection
activities and continued personnel training. Additionally, as part of its on-going oversight responsibilities, the joint oversight team, and the agencies’ internal oversight regimes, will continue to monitor the efficacy of measures to address the causes of compliance incidents during the next reporting period.
APPENDIX A
(U) IMPLEMENTATION OF SECTION 702 AUTHORITIES - OVERVIEW

(U) I. Overview - NSA

(U) The National Security Agency (NSA) seeks to acquire foreign intelligence information concerning specific targets under each Section 702 certification from or with the assistance of electronic communication service providers, as defined in Section 701(b)(4) of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA).1 As required by Section 702, those targets must be non-United States persons2 reasonably believed to be located outside the United States.

(S//NF) During this reporting period, NSA conducted foreign intelligence analysis to identify targets of foreign intelligence interest that fell within one of the following certifications:

1 (U) Specifically, Section 701(b)(4) provides:

   The term ‘electronic communication service provider’ means -- (A) a telecommunications carrier, as that term is defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153); (B) a provider of electronic communication service, as that term is defined in section 2510 of title 18, United States Code; (C) a provider of a remote computing service, as that term is defined in section 2711 of title 18, United States Code; (D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or (E) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).

2 (U) Section 101(i) of FISA defines “United States person” as follows:

   a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section101(a)(20) of the Immigration and Nationality Act [8 U.S.C. § 1101(a)(20)]), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3).
(U) As affirmed in affidavits filed with the Foreign Intelligence Surveillance Court (FISC), NSA believes that the non-United States persons reasonably believed to be outside the United States who are targeted under these certifications will either possess foreign intelligence information about the persons, groups, or entities covered by the certifications or are likely to receive or communicate foreign intelligence information concerning these persons, groups, or entities. This requirement is reinforced by the Attorney General’s Acquisition Guidelines, which provide that an individual may not be targeted unless a significant purpose of the targeting is to acquire foreign intelligence information that the person possesses, is reasonably expected to receive, and/or is likely to communicate.

(U) Under NSA’s FISC-approved targeting procedures, NSA targets a particular non-United States person reasonably believed to be located outside the United States by tasking facilities used by that person who possesses or who is likely to communicate or receive foreign intelligence information. A facility (also known as a “selector”) is a specific communications identifier tasked to acquire foreign intelligence information that is to, from, or about a target. A “facility” could be a telephone number or an identifier related to a form of electronic communication, such as an e-mail address. In order to acquire foreign intelligence information from or with the assistance of an electronic communications service provider, NSA first uses the identification of a facility to acquire the relevant communications. Then, after applying its targeting procedures (further discussed below) and other internal reviews and approvals, NSA “tasks” that facility in the relevant tasking system. The facilities are in turn provided to electronic communication service providers who have been served with the required directives under the certifications.

(U) Once information is collected from these tasked facilities, it is subject to FISC-approved minimization procedures. NSA’s minimization procedures set forth specific measures NSA must take when it acquires, retains, and/or disseminates non-publicly available information about United States persons. All collection of Section 702 information is routed to NSA. However, the NSA’s minimization procedures also permit the provision of unminimized communications to the Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI) relating to targets identified by these agencies that have been the subject of NSA acquisition under the certifications. The unminimized communications sent to CIA and FBI, in accordance with NSA’s targeting and minimization procedures, must in turn be processed by CIA and FBI in accordance with their respective FISC-approved Section 702 minimization procedures.6

(U) NSA’s targeting procedures address, among other subjects, the manner in which NSA will determine that a person targeted under Section 702 is a non-United States person reasonably
believed to be located outside the United States, the post-targeting analysis conducted on the facilities, and the documentation required.

(U) A. Pre-Tasking Location

(U) 1. Telephone Numbers

(S//SI//NF) For telephone numbers, NSA analysts may

(U) 2. Electronic Communications Identifiers

(S//SI//NF) For electronic communications identifiers, NSA analysts may

(U) Analysts also check this system as part of the “post-targeting” analysis described below.
(U) B. Pre-Tasking Determination of United States Person Status

(U) C. Post-Tasking Checks

(S//REL TO USA, FVEY) NSA also requires that tasking analysts review information collected from the facilities they have tasked. With respect to NSA’s review of

11 a notification e-mail is sent to the tasking team upon initial collection for the facility. NSA analysts are expected to review this collection within five business days to confirm that the user of the facility is the intended target, that the target remains appropriate to the certification cited, and that the target remains outside the United States. Analysts are then responsible to review traffic on an on-going basis to ensure that the facility remains appropriate under the authority. Should traffic not be viewed in at least once every 30 days, a notice is

11 (S//NF) NSA’s automated notification system to ensure analysts have reviewed collection is currently implemented only for , not . NSA is attempting to develop a similar system for
sent to the tasking team, as well as to their management, who then have the responsibility to follow up.

(U) **D. Documentation**

(S//NF) The procedures provide that analysts will document in the tasking database a citation to the information leading them to reasonably believe that a targeted person is located outside the United States. The citation is a reference that includes the source of the information, enabling oversight personnel to locate and review the information that led the analyst to his/her reasonable belief. Analysts must also identify the foreign power or foreign territory about which they expect the proposed targeting will obtain foreign intelligence information.

(S//NF) NSA has an existing database tool, for use by its analysts for Section 702 tasking and documentation purposes. The tool has been modified over time to accommodate the requirements of Section 702, to include, for example, certain fields and features for targeting, documentation, and oversight purposes. Accordingly, the tool allows analysts to document the required citation to NSA records on which NSA relied to form the reasonable belief that the target was located outside the United States. The tool has fields for the certification under which the target falls, and for the foreign power as to which the analyst expects to collect foreign intelligence information. Analysts fill out various fields for each facility, as appropriate, including the citation to the information on which the analyst relied in making the foreignness determination.

(U) NSA’s targeting procedures also require analysts to identify the foreign power or foreign territory about which they expect the proposed targeting will obtain foreign intelligence information and provide a written explanation of the basis for their assessment, at the time of targeting, that the target possesses, is expected to receive, and/or is likely to communicate foreign intelligence information concerning that foreign power or foreign territory.

(U) NSA also includes the targeting rationale (TAR) in the tasking record, which requires the targeting analyst to briefly state why targeting for a particular facility was requested. The intent of the TAR is to memorialize why the analyst is requesting targeting, and provides a linkage between the user of the facility and the foreign intelligence purpose covered by the certification under which it is being tasked. The joint oversight team assesses that the TAR has improved the oversight team’s ability to understand NSA’s foreign intelligence purpose in tasking facilities.

---

12 (U//FOUO) This paragraph was erroneously marked (U) in the previous joint assessment (i.e. the 14th Joint Assessment) but was appropriately marked (S//NF) in prior joint assessments.
Entries are reviewed before a tasking can be finalized. Records from this tool are maintained and compiled for oversight purposes. For each facility, a record can be compiled and printed showing certain relevant fields, such as: the facility, the certification, the citation to the record or records relied upon by the analyst, the analyst’s foreignness explanation, the targeting rationale. These records, referred to as “tasking sheets,” are reviewed by the Department of Justice’s National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) as part of the oversight process.

The source records cited on these tasking sheets are contained in a variety of NSA data repositories. These records are maintained by NSA and, when requested by the joint team, are produced to verify determinations recorded on the tasking sheets. Other source records may consist of “lead information” from other agencies, such as disseminated intelligence reports or lead information...

(U) F. Internal Procedures

(U) NSA has instituted internal training programs, access control procedures, standard operating procedures, compliance incident reporting measures, and similar processes to implement the requirements of the targeting procedures. Only analysts who have received certain types of training and authorizations are provided access to the Section 702 program data. These analysts must complete an NSA OGC and Signals Intelligence Directorate (SID) Oversight and Compliance training program; review the targeting and minimization procedures as well as other documents filed with the certifications; and must pass a competency test. The databases NSA analysts use are subject to audit and review by SID Oversight and Compliance. For guidance, analysts consult standard operating procedures, supervisors, SID Oversight and Compliance personnel, NSA OGC attorneys, and the NSA Office of the Director of Compliance.

(U) NSA’s targeting and minimization procedures require NSA to report to NSD and ODNI any incidents of non-compliance with the procedures by NSA personnel that result in the intentional targeting of a person reasonably believed to be located in the United States, the intentional targeting of a United States person, or the intentional acquisition of any communication in which the sender and all intended recipients are known at the time of acquisition to be located within the United
States, with a requirement to purge from NSA’s records any resulting collection. NSA must also report any incidents of non-compliance, including overcollection, by any electronic communication service provider issued a directive under Section 702. Additionally, if NSA learns, after targeting a person reasonably believed to be outside the United States, that the person is inside the United States, or if NSA learns that a person who NSA reasonably believed was a non-United States person is in fact a United States person, NSA must terminate the acquisition, and treat any acquired communications in accordance with its minimization procedures. In each of the above situations, NSA’s Section 702 procedures during this reporting period required NSA to report the incident to NSD and ODNI within the time specified in the applicable targeting procedures (five business days) of learning of the incident.

(U) The NSA targeting and minimization procedures require NSA to conduct oversight activities and make any necessary reports, including those relating to incidents of non-compliance, to the NSA Office of the Inspector General (NSA OIG) and NSA OGC. SID Oversight and Compliance conducts spot checks of targeting decisions and disseminations to ensure compliance with procedures. SID also maintains and updates an NSA internal website regarding the implementation of, and compliance with, the Section 702 authorities.

(U) NSA has established standard operating procedures for incident tracking and reporting to NSD and ODNI. The SID Oversight and Compliance office works with analysts at NSA, and with CIA and FBI points of contact as necessary, to compile incident reports which are forwarded to both the NSA OGC and NSA OIG. NSA OGC then forwards the incidents to NSD and ODNI.

(U) On a more programmatic level, under the guidance and direction of the Office of the Director of Compliance (ODOC), NSA has implemented and maintains a Comprehensive Mission Compliance Program (CMCP) designed to effect verifiable conformance with the laws and policies that afford privacy protection to United States persons during NSA missions. ODOC complements and reinforces the intelligence oversight program of NSA OIG and oversight responsibilities of NSA OGC.

(U) A key component of the CMCP is an effort to manage, organize, and maintain the authorities, policies, and compliance requirements that govern NSA mission activities. This effort, known as “Rules Management,” focuses on two key components: (1) the processes necessary to better govern, maintain, and understand the authorities granted to NSA and (2) technological solutions to support (and simplify) Rules Management activities. ODOC also coordinated NSA’s use of the Verification of Accuracy (VoA) process originally developed for other FISA programs to provide an increased level of confidence that factual representations to the FISC or other external decision makers are accurate and based on an ongoing, shared understanding among operational, technical, legal, policy and compliance officials within NSA. NSA has also developed a Verification of Interpretation (VoI) review to help ensure that NSA and its external overseers have a shared understanding of key terms in Court orders, minimization procedures, and other documents that govern NSA’s FISA activities. ODOC has also developed a risk assessment process to assess the potential risk of non-compliance with the rules designed to protect United States person privacy. The assessment is conducted and reported to the NSA Deputy Director and NSA Senior Leadership Team biannually.
(U) II. Overview - CIA

(U) A. CIA’s Role in Targeting

(S//NF) Although CIA does not target or acquire communications pursuant to Section 702, CIA has put in place a process, in consultation with NSA, FBI, NSD, and ODNI, to identify foreign intelligence targets to NSA (hereinafter referred to as the “CIA nomination process”). Based on its foreign intelligence analysis, CIA may “nominate” a facility to NSA for potential acquisition under one of the Section 702(g) certifications.

Nominations are reviewed and approved by a targeting officer’s first line manager, a component legal officer, a senior operational manager and the FISA Program Office prior to export to NSA for tasking.
The FISA Program Office was established in December 2010 and is charged with providing strategic direction for the management and oversight of CIA’s FISA collection programs, including the retention and dissemination of foreign intelligence information acquired pursuant to Section 702. This group is responsible for overall strategic direction and policy, programmatic external focus, and interaction with counterparts of NSD, ODNI, NSA and FBI. In addition, the office leads the day-to-day FISA compliance efforts. The primary responsibilities of the FISA Program Office are to provide strategic direction for data handling and management of FISA/702 data, as well as to ensure that all Section 702 collection is properly tasked and that CIA is complying with all compliance and purge requirements.

B. Oversight and Compliance

CIA’s FISA compliance program is managed by its FISA Program Office in coordination with CIA OGC. CIA provides small group training to personnel who nominate facilities to NSA and/or minimize Section 702-acquired communications. Access to unminimized Section 702-acquired communications is limited to trained personnel. CIA attorneys embedded with operational elements that have access to unminimized Section 702-acquired information also respond to inquiries regarding nomination and minimization questions. Identified incidents of noncompliance with the CIA minimization procedures are generally reported to NSD and ODNI by CIA OGC.

III. Overview - FBI

A. FBI’s Role in Targeting – Nomination for Acquiring In-Transit Communications

Like CIA, FBI has developed a formal nomination process to intelligence targets to NSA for the acquisition of in-transit communications. Including information underlying the basis for the foreignness determination and the foreign intelligence interest. FBI nominations are reviewed by FBI operational and legal personnel prior to export to NSA for tasking.

The FBI targeting procedures require that NSA first apply its own targeting procedures to determine that the user of the Designated Account is a person reasonably believed to be outside the United States and is not a
United States person. NSA is also responsible for determining that a significant purpose of the acquisition it requests is to obtain foreign intelligence information. After NSA designates accounts as being appropriate, FBI must then apply its own, additional procedures, which require FBI to review NSA’s conclusion of foreignness. More specifically, after FBI obtains the tasking sheet from NSA, it reviews the information provided by NSA regarding the location of the person and the non-United States person status of the person.
Unless FBI locates information indicating that the user is a United States person or is located inside the United States, FBI will...

If FBI identifies information indicating that NSA’s determination that the target is a non-United States person reasonably believed to be outside the United States may be incorrect, FBI provides this information to NSA and does not approve...

C. Documentation

The targeting procedures require that FBI retain the information in accordance with its records retention policies. FBI uses a multi-page checklist for each Designated Account to record the results of its targeting process, as laid out in its standard operating procedures, commencing with extending through, and culminating in approval or disapproval of the acquisition. In addition, the FBI standard operating procedures call for depending on the circumstances, which are maintained by FBI with the applicable checklist. FBI also retains with each checklist any relevant communications regarding its review of the information. Additional checklists have been created to capture information on requests withdrawn, or not approved by FBI.

D. Implementation, Oversight, and Compliance

FBI’s implementation and compliance activities are overseen by FBI OGC, particularly the National Security Law Branch (NSLB), as well as FBI’s Exploitation Threat Section (XTS), FBI’s Inspection Division (INSID), and FBI’s National Security Directorate (NSD). TS has the lead responsibility in FBI for requests. XTS personnel are trained on the FBI targeting procedures and FBI’s detailed set of standard operating procedures that govern its processing of requests. XTS also has the lead responsibility for facilitating FBI’s nominations to NSA communications. XTS, NSLB, NSD, and ODNI have all worked on training FBI personnel to
ensure that FBI nominations and post-tasking review comply with the NSA targeting procedures. Numerous such trainings were provided during the current reporting period. With respect to minimization, FBI has created a mandatory online training that all FBI agents and analysts must complete prior to gaining access to unminimized Section 702-acquired data in the FBI’s

In addition, NSD conducts training on the Section 702 minimization Procedures at multiple FBI field offices each year.

(S//NF) The FBI’s targeting procedures require periodic reviews by NSD and ODNI at least once every 60 days. FBI must also report incidents of non-compliance with the FBI targeting procedures to NSD and ODNI within five business days of learning of the incident. XTS and NSLB are the lead FBI elements in ensuring that NSD and ODNI received all appropriate information with regard to these two requirements.

(U) **IV. Overview - Minimization**

(U) Once a facility has been tasked for collection, non-publicly available information collected as a result of these taskings that concerns United States persons must be minimized. The FISC-approved minimization procedures require such minimization in the acquisition, retention, and dissemination of foreign intelligence information. As a general matter, minimization procedures under Section 702 are similar in most respects to minimization under other FISA orders. For example, the Section 702 minimization procedures, like those under certain other FISA court orders, allow for sharing of certain unminimized Section 702 information among NSA, FBI, and CIA. Similarly, the procedures for each agency require special handling of intercepted communications that are between attorneys and clients, as well as foreign intelligence information concerning United States persons that is disseminated to foreign governments.

(U) The minimization procedures do, however, impose additional obligations or restrictions as compared to minimization procedures associated with authorities granted under Titles I and III of FISA. For example, the Section 702 minimization procedures require, with limited exceptions, the purge of any communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be a non-United States person located outside the United States, but is in fact located inside the United States at the time the communication is acquired, or was in fact a United States person at the time of targeting.

(U) NSA, CIA, and FBI have created systems to track the purging of information from their systems. CIA and FBI receive incident notifications from NSA to document when NSA has identified Section 702 information that NSA is required to purge according to its procedures, so that CIA and FBI can meet their respective obligations.
United States Foreign Intelligence
Surveillance Court of Review

No. 08-01

IN RE: DIRECTIVES [redacted text]* PURSUANT TO
SECTION 105B OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT.

[redacted text]
Petitioner, Appellant.

ON PETITION FOR REVIEW OF A DECISION OF THE UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
[Hon. Reggie B. Walton, U.S. District Judge]

Before
Selya, Chief Judge,
Winter and Arnold, Senior Circuit Judges.

[redacted text]
Gregory G. Garre, Acting Solicitor General, with whom Michael B. Mukasey, Attorney General, Mark Filip, Deputy Attorney General,

*The text and footnotes that have been redacted from this opinion contain classified information.
J. Patrick Rowan, Acting Assistant Attorney General, John A. Eisenberg, Office of the Deputy Attorney General, John R. Phillips, Office of Legal Counsel, Sharon Swingle, Civil Division, and Matthew G. Olsen, John C. Demers, Jamil N. Jaffer, Andrew H. Tannenbaum, and Matthew A. Anzaldi, National Security Division, United States Department of Justice, were on brief, for respondent.

August 22, 2008
SELYA, Chief Judge. This petition for review stems from directives issued to the petitioner [redacted text] pursuant to a now-expired set of amendments to the Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. §§ 1801-1871 (2007). Among other things, those amendments, known as the Protect America Act of 2007 (PAA), Pub. L. No. 110-55, 121 Stat. 552, authorized the United States to direct communications service providers to assist it in acquiring foreign intelligence when those acquisitions targeted third persons (such as the service provider's customers) reasonably believed to be located outside the United States. Having received [redacted text] such directives, the petitioner challenged their legality before the Foreign Intelligence Surveillance Court (FISC). When that court found the directives lawful and compelled obedience to them, the petitioner brought this petition for review.

As framed, the petition presents matters of both first impression and constitutional significance. At its most elemental level, the petition requires us to weigh the nation's security interests against the Fourth Amendment privacy interests of United States persons.

After a careful calibration of this balance and consideration of the myriad of legal issues presented, we affirm
the lower court’s determinations that the directives at issue are lawful and that compliance with them is obligatory.

I. THE STATUTORY FRAMEWORK

On August 5, 2007, Congress enacted the PAA, codified in pertinent part at 50 U.S.C. §§ 1805a to 1805c, as a measured expansion of FISA’s scope. Subject to certain conditions, the PAA allowed the government to conduct warrantless foreign intelligence surveillance on targets (including United States persons) “reasonably believed” to be located outside the United States.1 50 U.S.C. § 1805b(a). This proviso is of critical importance here.

Under the new statute, the Director of National Intelligence (DNI) and the Attorney General (AG) were permitted to authorize, for periods of up to one year, “the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States” if they determined that the acquisition met five specified criteria. Id. These criteria included (i) that reasonable procedures were in place to ensure that the targeted person was reasonably believed to be located outside the United States; (ii) that the acquisitions did not

1We refer to the PAA in the past tense because its provisions expired on February 16, 2008.
constitute electronic surveillance;\(^2\) (iii) that the surveillance would involve the assistance of a communications service provider; (iv) that a significant purpose of the surveillance was to obtain foreign intelligence information; and (v) that minimization procedures in place met the requirements of 50 U.S.C. § 1801(h). Id. § 1805b(a)(1)-(5). Except in limited circumstances (not relevant here), this multi-part determination was required to be made in the form of a written certification “supported as appropriate by affidavit of appropriate officials in the national security field.” Id. § 1805b(a). Pursuant to this authorization, the DNI and the AG were allowed to issue directives to “person[s]” — a term that includes agents of communications service providers — delineating the assistance needed to acquire the information. Id. § 1805b(e); see id. § 1805b(a)(3).

The PAA was a stopgap measure. By its terms, it sunset on February 16, 2008. Following a lengthy interregnum, the lapsed provisions were repealed on July 10, 2008, through the instrumentality of the FISA Amendments Act of 2008, Pub. L. No. 110-261, § 403, 122 Stat. 2436, 2473 (2008). But because the certifications and directives involved in the instant case were

\(^2\)The PAA specifically stated, however, that “[n]othing in the definition of electronic surveillance . . . shall be construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States.” 50 U.S.C. § 1805a.
issued during the short shelf life of the PAA, they remained in effect. See FISA Amendments Act of 2008 § 404(a)(1). We therefore assess the validity of the actions at issue here through the prism of the PAA.

[redacted text]

II. BACKGROUND

Beginning in [redacted text] 2007, the government issued directives to the petitioner commanding it to assist in warrantless surveillance of certain customers [redacted text and footnote 3]. These directives were issued pursuant to certifications that purported to contain all the information required by the PAA.4

The certifications require certain protections above and beyond those specified by the PAA. For example, they require the AG and the National Security Agency (NSA) to follow the procedures set out under Executive Order 12333 § 2.5, 46 Fed. Reg. 59,941, 59,951 (Dec. 4, 1981),5 before any surveillance is undertaken. Moreover, affidavits supporting the certifications spell out

3[redacted text]

4The original certifications were amended, and we refer throughout to the amended certifications and the directives issued in pursuance thereof.

5Executive Order 12333 was amended in 2003, 2004, and 2008 through Executive Orders 13284, 13355, and 13470, respectively. Those amendments did not materially alter the provision relevant here.
additional safeguards to be employed in effecting the acquisitions. This last set of classified procedures has not been included in the information transmitted to the petitioner. In essence, as implemented, the certifications permit surveillances conducted to obtain foreign intelligence for national security purposes when those surveillances are directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States.

The government’s efforts did not impress the petitioner, which refused to comply with the directives. On [redacted text], the government moved to compel compliance. Following amplitudinous briefing, the FISC handed down a meticulous opinion validating the directives and granting the motion to compel.

The FISC’s decision was docketed on [redacted text]. Six business days later, the petitioner filed a petition for review. The next day, it moved for a stay pending appeal. The FISC refused to grant the stay. On [redacted text], the petitioner began compliance under threat of civil contempt. [redacted text]

On [redacted text], the petitioner moved in this court for a stay pending appeal. We reserved decision on the motion and compliance continued. We then heard oral argument on the merits and took the case under advisement. We have jurisdiction to review the FISC’s decision pursuant to 50 U.S.C. § 1805b(i) inasmuch as
that decision is the functional equivalent of a ruling on a petition brought pursuant 50 U.S.C. § 1805b(h). See In re Sealed Case, 310 F.3d 717, 721 (Foreign Int. Surv. Ct. Rev. 2002).

III. ANALYSIS

We briefly address a preliminary matter: standing. We then turn to the constitutional issues that lie at the heart of the petitioner's asseverational array.

A. Standing.

Federal appellate courts typically review standing determinations de novo, see, e.g., Muir v. Navy Fed. Credit Union, 529 F.3d. 1100, 1105 (D.C. Cir. 2008), and we apply that standard of review here.

The FISC determined that the petitioner had standing to mount a challenge to the legality of the directives based on the Fourth Amendment rights of third-party customers. At first blush, this has a counter-intuitive ring: it is common ground that litigants ordinarily cannot bring suit to vindicate the rights of third parties. See, e.g., Hinck v. United States, 127 S.Ct. 2011, 2017 n.3 (2007); Warth v. Seldin, 422 U.S. 490, 499 (1975). But that prudential limitation may in particular cases be relaxed by congressional action. Warth, 422 U.S. at 501; see Bennett v. Spear, 520 U.S. 154, 162 (1997) (recognizing that Congress can "modif[y] or abrogat[e]" prudential standing requirements). Thus,
if Congress, either expressly or by fair implication, cedes to a party a right to bring suit based on the legal rights or interests of others, that party has standing to sue; provided, however, that constitutional standing requirements are satisfied. See Warth, 422 U.S. at 500-01. Those constitutional requirements are familiar; the suitor must plausibly allege that it has suffered an injury, which was caused by the defendant, and the effects of which can be redressed by the suit. See id. at 498-99; N.H. Right to Life PAC v. Gardner, 99 F.3d 8, 13 (1st Cir. 1996).

Here, the petitioner easily exceeds the constitutional threshold for standing. It faces an injury in the nature of the burden that it must shoulder to facilitate the government’s surveillances of its customers; that injury is obviously and indisputably caused by the government through the directives; and this court is capable of redressing the injury.

That brings us to the question of whether Congress has provided that a party in the petitioner’s position may bring suit to enforce the rights of others. That question demands an affirmative answer.

The PAA expressly declares that a service provider that has received a directive “may challenge the legality of that directive,” 50 U.S.C. § 1805b(h)(1)(A), and “may file a petition with the Court of Review” for relief from an adverse FISC decision,
id. § 1805b(i). There are a variety of ways in which a directive could be unlawful, and the PAA does nothing to circumscribe the types of claims of illegality that can be brought. We think that the language is broad enough to permit a service provider to bring a constitutional challenge to the legality of a directive regardless of whether the provider or one of its customers suffers the infringement that makes the directive unlawful. The short of it is that the PAA grants an aggrieved service provider a right of action and extends that right to encompass claims brought by it on the basis of customers' rights.

For present purposes, that is game, set, and match. As said, the petitioner's response to the government's motion to compel is the functional equivalent of a petition under section 1805b(h)(1)(A). The petitioner's claim, as a challenge to the constitutionality of the directives, quite clearly constitutes a challenge to their legality. Thus, the petitioner's Fourth Amendment claim on behalf of its customers falls within the ambit of the statutory provision. It follows inexorably that the petitioner has standing to maintain this litigation.

B. The Fourth Amendment Challenge.

We turn now to the petitioner's Fourth Amendment arguments. In the Fourth Amendment context, federal appellate courts review findings of fact for clear error and legal
conclusions (including determinations about the ultimate constitutionality of government searches or seizures) de novo. See, e.g., United States v. Martins, 413 F.3d 139, 146 (1st Cir. 2005); United States v. Runyan, 290 F.3d 223, 234 (5th Cir. 2002). We therefore review de novo the FISC’s conclusion that the surveillances carried out pursuant to the directives are lawful.

The petitioner’s remonstrance has two main branches. First, it asserts that the government, in issuing the directives, had to abide by the requirements attendant to the Warrant Clause of the Fourth Amendment. Second, it argues that even if a foreign intelligence exception to the warrant requirements exists and excuses compliance with the Warrant Clause, the surveillances mandated by the directives are unreasonable and, therefore, violate the Fourth Amendment. The petitioner limits each of its claims to the harm that may be inflicted upon United States persons.

1. The Nature of the Challenge. As a threshold matter, the petitioner asserts that its Fourth Amendment arguments add up to a facial challenge to the PAA. The government contests this characterization, asserting that the petitioner presents only an as-applied challenge. We agree with the government.

A facial challenge asks a court to consider the constitutionality of a statute without factual development centered around a particular application. See, e.g., Wash. State Grange v.
Wash. State Repub. Party, 128 S.Ct. 1184, 1190 (2008). Here, however, there is a particularized record and the statute — the PAA — has been applied to the petitioner in a specific setting. The petitioner’s plaints take account of this setting. So viewed, they go past the question of whether the PAA is valid on its face — a question that would be answered by deciding whether any application of the statute passed constitutional muster, see, e.g., id. — and ask instead whether this specific application offends the Constitution. As such, the petitioner’s challenge falls outside the normal circumference of a facial challenge.

This makes perfect sense. Where, as here, a statute has been implemented in a defined context, an inquiring court may only consider the statute’s constitutionality in that context; the court may not speculate about the validity of the law as it might be applied in different ways or on different facts. See Nat’l Endow. for the Arts v. Finley, 524 U.S. 569, 584 (1998); see also Yazoo & Miss. Valley R.R. Co. v. Jackson Vinegar Co., 226 U.S. 217, 220 (1912) (explaining that how a court may apply a statute to other cases and how far parts of the statute may be sustained on other facts “are matters upon which [a reviewing court] need not speculate”).

We therefore deem the petitioner’s challenge an as-applied challenge and limit our analysis accordingly. This means
that, to succeed, the petitioner must prove more than a theoretical risk that the PAA could on certain facts yield unconstitutional applications. Instead, it must persuade us that the PAA is unconstitutional as implemented here.

2. The Foreign Intelligence Exception. The recurrent theme permeating the petitioner’s arguments is the notion that there is no foreign intelligence exception to the Fourth Amendment’s Warrant Clause. The FISC rejected this notion, positing that our decision in In re Sealed Case confirmed the existence of a foreign intelligence exception to the warrant requirement.

While the Sealed Case court avoided an express holding that a foreign intelligence exception exists by assuming arguendo that whether or not the warrant requirements were met, the statute could survive on reasonableness grounds, see 310 F.3d at 741-42, we believe that the FISC’s reading of that decision is plausible.

---

The Fourth Amendment reads:
The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV.
The petitioner argues correctly that the Supreme Court has not explicitly recognized such an exception; indeed, the Court reserved that question in United States v. United States District Court (Keith), 407 U.S. 297, 308-09 (1972). But the Court has recognized a comparable exception, outside the foreign intelligence context, in so-called "special needs" cases. In those cases, the Court excused compliance with the Warrant Clause when the purpose behind the governmental action went beyond routine law enforcement and insisting upon a warrant would materially interfere with the accomplishment of that purpose. See, e.g., Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995) (upholding drug testing of high­school athletes and explaining that the exception to the warrant requirement applied "when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement[s] impracticable" (quoting Griffin v. Wisconsin, 483 U.S. 868, 873 (1987))); Skinner v. Ry. Labor Execs. Ass’n, 489 U.S. 602, 620 (1989) (upholding regulations instituting drug and alcohol testing of railroad workers for safety reasons); cf. Terry v. Ohio, 392 U.S. 1, 23-24 (1968) (upholding pat-frisk for weapons to protect officer safety during investigatory stop).

The question, then, is whether the reasoning of the special needs cases applies by analogy to justify a foreign intelligence exception to the warrant requirement for surveillance.
undertaken for national security purposes and directed at a foreign power or an agent of a foreign power reasonably believed to be located outside the United States. Applying principles derived from the special needs cases, we conclude that this type of foreign intelligence surveillance possesses characteristics that qualify it for such an exception.

For one thing, the purpose behind the surveillances ordered pursuant to the directives goes well beyond any garden-variety law enforcement objective. It involves the acquisition from overseas foreign agents of foreign intelligence to help protect national security. Moreover, this is the sort of situation in which the government's interest is particularly intense.

The petitioner has a fallback position. Even if there is a narrow foreign intelligence exception, it asseverates, a definition of that exception should require the foreign intelligence purpose to be the primary purpose of the surveillance. For that proposition, it cites the Fourth Circuit's decision in United States v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980). That dog will not hunt.

This court previously has upheld as reasonable under the Fourth Amendment the Patriot Act's substitution of "a significant purpose" for the talismanic phrase "primary purpose." In re Sealed Case, 310 F.3d at 742-45. As we explained there, the Fourth
Circuit's "primary purpose" language — from which the pre-Patriot Act interpretation of "purpose" derived — drew an "unstable, unrealistic, and confusing" line between foreign intelligence purposes and criminal investigation purposes. Id. at 743. A surveillance with a foreign intelligence purpose often will have some ancillary criminal-law purpose. See id. The prevention or apprehension of terrorism suspects, for instance, is inextricably intertwined with the national security concerns that are at the core of foreign intelligence collection. See id. In our view the more appropriate consideration is the programmatic purpose of the surveillances and whether — as in the special needs cases — that programmatic purpose involves some legitimate objective beyond ordinary crime control. Id. at 745-46.

Under this analysis, the surveillances authorized by the directives easily pass muster. Their stated purpose centers on garnering foreign intelligence. There is no indication that the collections of information are primarily related to ordinary criminal-law enforcement purposes. Without something more than a purely speculative set of imaginings, we cannot infer that the purpose of the directives (and, thus, of the surveillances) is other than their stated purpose. See, e.g., United States v. Chem. Found., Inc., 272 U.S. 1, 14-15 (1926) ("The presumption of regularity supports the official acts of public officers, and, in
the absence of clear evidence to the contrary, courts presume that they have properly discharged their official duties.”).

We add, moreover, that there is a high degree of probability that requiring a warrant would hinder the government’s ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake. See, e.g., Truong Dinh Hung, 629 F.2d at 915 (explaining that when the object of a surveillance is a foreign power or its collaborators, “the government has the greatest need for speed, stealth, and secrecy”). Compulsory compliance with the warrant requirement would introduce an element of delay, thus frustrating the government’s ability to collect information in a timely manner.

For these reasons, we hold that a foreign intelligence exception to the Fourth Amendment’s warrant requirement exists when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States.

3. **Reasonableness.** This holding does not grant the government carte blanche: even though the foreign intelligence exception applies in a given case, governmental action intruding on individual privacy interests must comport with the Fourth
Amendment’s reasonableness requirement. See United States v. Place, 462 U.S. 696, 703 (1983). Thus, the question here reduces to whether the PAA, as applied through the directives, constitutes a sufficiently reasonable exercise of governmental power to satisfy the Fourth Amendment.

We begin with bedrock. The Fourth Amendment protects the right “to be secure . . . against unreasonable searches and seizures.” U.S. Const. amend. IV. To determine the reasonableness of a particular governmental action, an inquiring court must consider the totality of the circumstances. Samson v. California, 547 U.S. 843, 848 (2006); Tennessee v. Garner, 471 U.S. 1, 8-9 (1985). This mode of approach takes into account the nature of the government intrusion and how the intrusion is implemented. See Garner, 471 U.S. at 8; Place, 462 U.S. at 703. The more important the government’s interest, the greater the intrusion that may be constitutionally tolerated. See, e.g., Michigan v. Summers, 452 U.S. 692, 701-05 (1981).

The totality of the circumstances model requires the court to balance the interests at stake. See Samson, 547 U.S. at 848; United States v. Knights, 534 U.S. 112, 118-19 (2001). If the protections that are in place for individual privacy interests are sufficient in light of the governmental interest at stake, the constitutional scales will tilt in favor of upholding the
government’s actions. If, however, those protections are insufficient to alleviate the risks of government error and abuse, the scales will tip toward a finding of unconstitutionality.

Here, the relevant governmental interest — the interest in national security — is of the highest order of magnitude. See Haig v. Agee, 453 U.S. 280, 307 (1981); In re Sealed Case, 310 F.3d at 746. Consequently, we must determine whether the protections afforded to the privacy rights of targeted persons are reasonable in light of this important interest.

At the outset, we dispose of two straw men — arguments based on a misreading of our prior decision in Sealed Case. First, the petitioner notes that we found relevant six factors contributing to the protection of individual privacy in the face of a governmental intrusion for national security purposes. See In re Sealed Case, 310 F.3d at 737-41 (contemplating prior judicial review, presence or absence of probable cause, particularity, necessity, duration, and minimization). On that exiguous basis, it reasons that our decision there requires a more rigorous standard for gauging reasonableness.

This is a mistaken judgment. In Sealed Case, we did not formulate a rigid six-factor test for reasonableness. That would be at odds with the totality of the circumstances test that must guide an analysis in the precincts patrolled by the Fourth
Amendment. We merely indicated that the six enumerated factors were relevant under the circumstances of that case.

Second, the petitioner asserts that our Sealed Case decision stands for the proposition that, in order to gain constitutional approval, the PAA procedures must contain protections equivalent to the three principal warrant requirements: prior judicial review, probable cause, and particularity. That is incorrect. What we said there—and reiterate today—is that the more a set of procedures resembles those associated with the traditional warrant requirements, the more easily it can be determined that those procedures are within constitutional bounds. See id. at 737, 742. We therefore decline the petitioner’s invitation to reincorporate into the foreign intelligence exception the same warrant requirements that we already have held inapplicable.

Having placed Sealed Case into perspective, we turn to the petitioner’s contention that the totality of the circumstances demands a finding of unreasonableness here. That contention boils down to the idea that the protections afforded under the PAA are insufficiently analogous to the protections deemed adequate in Sealed Case because the PAA lacks (i) a particularity requirement, (ii) a prior judicial review requirement for determining probable cause that a target is a foreign power or an agent of a foreign...
power, and (iii) any plausible proxies for the omitted protections. For good measure, the petitioner suggests that the PAA’s lack of either a necessity requirement or a reasonable durational limit diminishes the overall reasonableness of surveillances conducted pursuant thereto.

The government rejoins that the PAA, as applied here, constitutes reasonable governmental action. It emphasizes both the protections spelled out in the PAA itself and those mandated under the certifications and directives. This matrix of safeguards comprises at least five components: targeting procedures, minimization procedures, a procedure to ensure that a significant purpose of a surveillance is to obtain foreign intelligence information, procedures incorporated through Executive Order 12333 § 2.5, and [redacted text] procedures [redacted text] outlined in an affidavit supporting the certifications.

The record supports the government. Notwithstanding the parade of horribles trotted out by the petitioner, it has presented no evidence of any actual harm, any egregious risk of error, or any broad potential for abuse in the circumstances of the instant case. Thus, assessing the intrusions at issue in light of the governmental interest at stake and the panoply of protections that are in place, we discern no principled basis for invalidating the
PAA as applied here. In the pages that follow, we explain our reasoning.

The petitioner's arguments about particularity and prior judicial review are defeated by the way in which the statute has been applied. When combined with the PAA's other protections, the procedures and the procedures incorporated through the Executive Order are constitutionally sufficient compensation for any encroachments.

The procedures are delineated in an ex parte appendix filed by the government. They also are described, albeit with greater generality, in the government's brief. Although the PAA itself does not mandate a showing of particularity, see 50 U.S.C. § 1805b(b), this pre-surveillance procedure strikes us as analogous to and in conformity with the particularity showing contemplated by Sealed Case. 310 F.3d at 740.

The procedures incorporated through section 2.5 of Executive Order 12333, made applicable to the surveillances through the certifications and directives, serve to allay the probable cause concern. That section states in relevant part:

The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against
a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power.

46 Fed. Reg. at 59,951 (emphasis supplied). Thus, in order for the government to act upon the certifications, the AG first had to make a determination that probable cause existed to believe that the targeted person is a foreign power or an agent of a foreign power. Moreover, this determination was not made in a vacuum. The AG's decision was informed by the contents of an application made pursuant to Department of Defense (DOD) regulations. See DOD, Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons, DOD 5240.1-R, Proc. 5, Pt. 2.C (Dec. 1982). Those regulations required that the application include a statement of facts demonstrating both probable cause and necessity. See id. They also required a statement of the period — not to exceed 90 days — during which the surveillance was thought to be required. See id.

7 At oral argument, the government augmented this description, stating that, under the DOD procedure, the NSA typically provides the AG with a two-to-three-page submission articulating the facts underlying the determination that the person in question is an agent of a foreign power; that the National Security Division of the Department of Justice writes its own memorandum to the AG; and
The petitioner's additional criticisms about the surveillances can be grouped into concerns about potential abuse of executive discretion and concerns about the risk of government error (including inadvertent or incidental collection of information from non-targeted United States persons). We address these groups of criticisms sequentially.

The petitioner suggests that, by placing discretion entirely in the hands of the Executive Branch without prior judicial involvement, the procedures cede to that Branch overly broad power that invites abuse. But this is little more than a lament about the risk that government officials will not operate in good faith. That sort of risk exists even when a warrant is required. In the absence of a showing of fraud or other misconduct by the affiant, the prosecutor, or the judge, a presumption of regularity traditionally attaches to the obtaining of a warrant. See, e.g., McSurely v. McClellan, 697 F.2d 309, 323-24 (D.C. Cir. 1982).

Here — where an exception affords relief from the warrant requirement — common sense suggests that we import the same

that an oral briefing of the AG ensues.

8[redacted text]
presumption. Once we have determined that protections sufficient to meet the Fourth Amendment’s reasonableness requirement are in place, there is no justification for assuming, in the absence of evidence to that effect, that those prophylactic procedures have been implemented in bad faith.

Similarly, the fact that there is some potential for error is not a sufficient reason to invalidate the surveillances. [redacted text]

Equally as important, some risk of error exists under the original FISA procedures – procedures that received our imprimatur in Sealed Case, 310 F.3d at 746. A prior judicial review process does not ensure that the types of errors complained of here [redacted text] would have been prevented.

It is also significant that effective minimization procedures are in place. These procedures serve as an additional backstop against identification errors as well as a means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons. The minimization procedures implemented here are almost identical to those used under FISA to ensure the curtailment of both mistaken and incidental acquisitions. These minimization procedures were upheld by the FISC in this case, and the petitioner stated at oral argument that it is not quarreling about minimization but, rather, about
particularity. Thus, we see no reason to question the adequacy of the minimization protocol.

The petitioner's concern with incidental collections is overblown. It is settled beyond peradventure that incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful. See, e.g., United States v. Kahn, 415 U.S. 143, 157-58 (1974); United States v. Schwartz, 535 F.2d 160, 164 (2d Cir. 1976). The government assures us that it does not maintain a database of incidentally collected information from non-targeted United States persons, and there is no evidence to the contrary. On these facts, incidentally collected communications of non-targeted United States persons do not violate the Fourth Amendment.

To the extent that the petitioner may be concerned about the adequacy of the targeting procedures, it is worth noting that those procedures include provisions designed to prevent errors. [redacted text] Furthermore, a PAA provision codified at 50 U.S.C. § 1805b(d) requires the AG and the DNI to assess compliance with those procedures and to report to Congress semi-annually.

9 The petitioner has not charged that the Executive Branch is surveilling overseas persons in order intentionally to surveil persons in the United States. Because the issue is not before us, we do not pass on the legitimacy vel non of such a practice.
**[4. A Parting Shot.** The petitioner fires a parting shot. It presented for the first time at oral argument a specific privacy concern that could possibly arise under the directives. This parting shot may have been waived by the failure to urge it either before the FISC or in the petitioner’s pre-argument filings in this court. We need not probe that point, however, because the petitioner is firing blanks: no issue falling within this description has arisen to date. Were such an issue to arise, there are safeguards in place that may meet the reasonableness standard. We do, however, direct the government promptly to notify the petitioner if this issue arises under the directives.\(^1\)

The foregoing paragraph is a summary of our holding on this issue. We discuss with greater specificity the petitioner’s argument, the government’s safeguards, and our order in the classified version of this opinion.]

**5. Recapitulation.** After assessing the prophylactic procedures applicable here, including the provisions of the PAA, the affidavits supporting the certifications, section 2.5 of Executive Order 12333, and the declaration mentioned above, we conclude that they are very much in tune with the considerations discussed in Sealed Case. Collectively, these procedures require

\(^{10}[^{redacted\space text}]\)
a showing of particularity, a meaningful probable cause determination, and a showing of necessity. They also require a durational limit not to exceed 90 days – an interval that we previously found reasonable. See *In re Sealed Case*, 310 F.3d at 740. Finally, the risks of error and abuse are within acceptable limits and effective minimization procedures are in place.

Balancing these findings against the vital nature of the government’s national security interest and the manner of the intrusion, we hold that the surveillances at issue satisfy the Fourth Amendment’s reasonableness requirement.

**IV. CONCLUSION**

Our government is tasked with protecting an interest of utmost significance to the nation – the safety and security of its people. But the Constitution is the cornerstone of our freedoms, and government cannot unilaterally sacrifice constitutional rights on the altar of national security. Thus, in carrying out its national security mission, the government must simultaneously fulfill its constitutional responsibility to provide reasonable protections for the privacy of United States persons. The judiciary’s duty is to hold that delicate balance steady and true.

---

"This time period was deemed acceptable because of the use of continuing minimization procedures. *In re Sealed Case*, 310 F.3d at 740. Those minimization procedures are nearly identical to the minimization procedures employed in this case. See text *supra.*"
We believe that our decision to uphold the PAA as applied in this case comports with that solemn obligation. In that regard, we caution that our decision does not constitute an endorsement of broad-based, indiscriminate executive power. Rather, our decision recognizes that where the government has instituted several layers of serviceable safeguards to protect individuals against unwarranted harms and to minimize incidental intrusions, its efforts to protect national security should not be frustrated by the courts. This is such a case.

We need go no further. The decision granting the government’s motion to compel is affirmed; the petition for review is denied and dismissed; and the motion for a stay is denied as moot.

So Ordered.
As members of the intelligence profession, we conduct ourselves in accordance with certain basic principles. These principles are stated below, and reflect the standard of ethical conduct expected of all Intelligence Community personnel, regardless of individual role or agency affiliation. Many of these principles are also reflected in other documents that we look to for guidance, such as statements of core values, and the *Code of Conduct: Principles of Ethical Conduct for Government Officers and Employees*; it is nonetheless important for the Intelligence Community to set forth in a single statement the fundamental ethical principles that unite us and distinguish us as intelligence professionals.

**MISSION**  We serve the American people, and understand that our mission requires selfless dedication to the security of our Nation.

**TRUTH**  We seek the truth; speak truth to power; and obtain, analyze, and provide intelligence objectively.

**LAWFULNESS**  We support and defend the Constitution, and comply with the laws of the United States, ensuring that we carry out our mission in a manner that respects privacy, civil liberties, and human rights obligations.

**INTEGRITY**  We demonstrate integrity in our conduct, mindful that all our actions, whether public or not, should reflect positively on the Intelligence Community at large.

**STEWARDSHIP**  We are responsible stewards of the public trust; we use intelligence authorities and resources prudently, protect intelligence sources and methods diligently, report wrongdoing through appropriate channels; and remain accountable to ourselves, our oversight institutions, and through those institutions, ultimately to the American people.

**EXCELLENCE**  We seek to improve our performance and our craft continuously, share information responsibly, collaborate with our colleagues, and demonstrate innovation and agility when meeting new challenges.

**DIVERSITY**  We embrace the diversity of our Nation, promote diversity and inclusion in our work force, and encourage diversity in our thinking.
ORDER APPOINTING AN AMICUS CURIAE

For the reasons set out below, the Court appoints Amy Jeffress to serve as amicus curiae in the above-captioned matter for the purpose of assisting the Court in considering the issues specified herein. This appointment is made pursuant to section 103(i)(2)(B) of the Foreign Intelligence Surveillance Act of 1978 (FISA), codified at 50 U.S.C. § 1803(i)(2)(B), as most recently amended by the USA FREEDOM Act, Pub. L. No. 114-23, 129 Stat. 268. This Order also addresses certain administrative matters relating to the participation of the amicus.

Background

On July 15, 2015, the government submitted certifications and accompanying targeting and minimization procedures ("the 2015 Certifications") pursuant to section 702 of FISA, codified at 50 U.S.C. § 1881a. The 2015 Certifications reauthorize certifications under
section 702 that the Court approved on August 26, 2014 (“the 2014 Certifications”). They also amend the 2014 Certifications, as well as predecessor certifications under section 702, to provide that information acquired pursuant to those certifications shall henceforward be governed by the minimization procedures that accompany the 2015 Certifications.

The government had submitted versions of the 2015 Certifications in draft form on June 15, 2015. After reviewing those drafts, the Court concluded “that this matter is likely to present one or more novel or significant interpretations of the law, which would require the Court to consider appointment of an amicus curiae” under section 103(i)(2). See [Redacted] Order issued on July 7, 2015 (“July 7 Order”), at 3. The Court further noted that the 30-day review period specified by section 702(i)(1)(B) would, as a practical matter, foreclose amicus participation. Id.

The Court may, however, extend that 30-day review period “as necessary for good cause in a manner consistent with national security.” § 702(j)(2). To help the Court decide “whether to extend the time it would have to act on the 2015 Certifications and revised procedures in order to allow for meaningful amicus assistance in reviewing them,” the Court ordered the government to “explain in writing whether – and if so, how long – an extension of the time for the Court to review the 2015 Certifications and revised procedures would be consistent with national security.” July 7 Order at 4.

On July 14, 2015, the government timely filed its Response to the July 7 Order, advising that “the government assesses that an extension of 60 to 90 days ... would be consistent with national security.” See [Redacted] Government’s Response to the Court’s Order of July 7, 2015, filed on July 14, 2015, at 7.
On July 23, 2015, the Court found that “the need for an extension to allow for [amicus] participation constitutes ‘good cause’” for an extension under section 702(j)(2). See and predecessor docketts, Order issued on July 23, 2015, at 3. Accordingly, it extended “the period for Court review under section 702(i)(1)(B) for 90 days, such that this review must be completed no later than November 12, 2015.” Id. The Court explained that it
does not expect or intend to use the entirety of this extended period. Rather, in order to avoid the burdens and costs that the government has ascribed to implementing multiple extensions, see Response at 8 n.8, the Court has decided in a single order to extend the period to the outermost date that is consistent with the government’s assessment of national security.

Id.

Appointment of Amicus Curiae

By the terms of section 103(i)(2)(A), the court “shall appoint” to serve as amicus curiae an individual who has been designated as eligible for such service under section 103(i)(1) “to assist . . . in the consideration of any application for an order or review that, in the opinion of the court, presents a novel or significant interpretation of the law, unless the court issues a finding that such appointment is not appropriate.” Under section 103(i)(1), the presiding judges of the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review have until November 29, 2015, to jointly designate individuals as eligible to serve as amicus under section 103(i)(1).1 To date, no such designations have been made. Under present circumstances, therefore, the appointment of such an individual “is not appropriate” under section 103(i)(2)(A), because, as of yet, there are no designated individuals who can serve.

---

1 Section 103(i)(1) requires such designations to be made “not later than 180 days after” the date of enactment of the USA FREEDOM Act, which was June 2, 2015.
Section 103(i)(2)(B) provides that the Court "may appoint an individual or organization to serve as amicus curiae . . . in any instance as such court deems appropriate." Persons appointed under this provision need not have been designated under section 103(i)(1). They shall, however, "be persons who are determined to be eligible for access to classified information, if such access is necessary to participate in the matters in which they may be appointed." § 103(i)(3)(B).

Here, the Court finds it appropriate to appoint Amy Jeffress as amicus curiae under section 103(i)(2)(B). Ms. Jeffress is well qualified to assist the Court in considering the issues specified herein. The Security and Emergency Planning Staff (SEPS) of the Department of Justice has advised that she is eligible for access to classified information.

Accordingly, it is HEREBY ORDERED as follows:

(1) Amy Jeffress is appointed as amicus curiae (hereinafter "amicus") in this matter pursuant to section 103(i)(2)(B).

(2) Pursuant to section 702(i)(2)(C) and (i)(3)(A)-(B), the Court must assess, among other things: (a) whether the minimization procedures that accompany the 2015 Certifications meet the definition of minimization procedures under 50 U.S.C. § 1801(b) or § 1821(4), as appropriate; and (b) whether those procedures are consistent with the fourth amendment to the Constitution of the United States. The amicus is directed to address whether these requirements are satisfied in view of the provisions of the procedures that apply to:

(i) queries of information obtained under section 702, particularly insofar as queries may be designed to return information concerning United States persons, see NSA Minimization Procedures at 7, FBI Minimization Procedures at 11-12, and CIA Minimization Procedures at 3-4; and

(ii) preservation for litigation purposes of information otherwise required to be destroyed under the minimization procedures, see NSA Minimization Procedures
at 8-9, FBI Minimization Procedures at 24-25, and CIA Minimization Procedures at 10-11.

The Court anticipates setting a briefing schedule at a later date.

(3) Pursuant to section 103(i)(6)(A)(i), the Court has determined that the materials identified in Exhibit A (attached hereto) are relevant to the duties of the amicus. By August 21, 2015, or after receiving confirmation from SEPS that the amicus has received the appropriate clearances and access approvals for such materials, whichever is later, the Clerk of the Court shall make the materials identified in Exhibit A available to the amicus.

(4) With the guidance and assistance of SEPS, the amicus shall handle classified information in accordance with the Security Procedures Established Pursuant to Public Law No. 95-511, 92 Stat. 1783, as Amended, By the Chief Justice of the United States for the Foreign Intelligence Surveillance Court And the Foreign Intelligence Surveillance Court of Review (Feb. 21, 2013) ("Security Procedures") (copy attached at Exhibit B). For purposes of the Security Procedures, the amicus shall be regarded as court personnel.

(5) Section 103(i)(6)(C) provides: "An amicus curiae designated or appointed by the court may have access to classified documents, information, and other materials or proceedings only if that individual is eligible for access to classified information and to the extent consistent with the national security of the United States." The Court believes that, in this matter, the amicus's access to classified information pursuant to paragraphs (3) and (4) above is consistent with the national security of the United States. If, however, the government believes otherwise, it shall provide written notice and explanation to the Court by August 18, 2015.
(6) The attorney for the government shall ensure that the Attorney General receives a copy of this Order pursuant to the notification requirement at section 103(i)(7).

ENTERED this 13th day of August 2015, in

THOMAS F. HOGAN
Judge, United States Foreign Intelligence Surveillance Court
SECRET/NOFORN

EXHIBIT A

Foreign Intelligence Surveillance Court of Review Materials

In re Directives, FISCR Docket No. 08-01, Opinion issued on Aug. 22, 2008

Foreign Intelligence Surveillance Court Materials

From [redacted]

Order issued on July 7, 2015

Government’s Response to the Court’s Order of July 7, 2015, filed on July 14, 2015

From [redacted] and predecessor docket:

Order Appointing Amicus Curiae (to which this Exhibit A is attached)

Order issued on July 23, 2015

The Government’s filing on July 15, 2015, of its Ex Parte Submission Of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications (including Certifications [redacted], accompanying targeting and minimization procedures, and supporting affidavits; unclassified discussion of the government’s oversight efforts regarding Section 702 implementation; 2015 Summary of Notable Section 702 Requirements; and redline-strikeout versions of selected documents)

From predecessor 702(i) Dockets:

All Opinions or Orders approving or disapproving certifications, targeting procedures, and minimization procedures pursuant to Section 702(i)(3), including written statements of the reasons for such approval or disapproval

From [redacted], et al.:

Opinion and Order issued on Aug. 11, 2014

SECRET/NOFORN
Exhibit B

Security Procedures Established Pursuant to Public Law No. 95-511, 92 Stat. 1783, as Amended, By the Chief Justice of the United States for the Foreign Intelligence Surveillance Court And the Foreign Intelligence Surveillance Court of Review

1. Purpose. The purpose of these procedures, as revised, is to meet the court security requirements of the Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783, as amended ("the Act"). These security procedures apply to both the Foreign Intelligence Surveillance Court established under § 103(a) of the Act and the Foreign Intelligence Surveillance Court of Review established under § 103(b), and to all supporting personnel of said courts. Except for the judges of the two courts, the same facilities, personnel, and security procedures shall be used by both courts, subject to such exceptions as may be authorized by the Chief Justice. These procedures have been adopted in consultation with the Attorney General and the Director of National Intelligence as required by the Act and supercede the security procedures issued on May 18, 1979. The term "court" as used herein refers to both Courts.

2. Quarters and Facilities. The quarters and facilities of the court, including a hearing room, work chambers, and storage facilities for court records, shall be constructed and maintained in accordance with applicable construction standards pertaining to sensitive compartmented information facilities adopted by the Director of National Intelligence. The location of court facilities may be changed by the court from time to time in consultation with the Chief Justice, the Attorney General, and the Director of National Intelligence.

3. Members of the Court. Judges to be designated as members of the court pursuant to § 103 of the Act shall be subject, before designation, to an updated background investigation to be conducted by the Federal Bureau of Investigation under applicable Executive Branch standards for investigations performed in support of determinations of eligibility for access to sensitive compartmented information or other classified national security information, insofar as they may be deemed applicable to the court. If a question of suitability to serve on the court is raised at any time after initial appointment, the matter is to be referred to the Chief Justice, who may elect to consult with the Attorney General and the Director of National Intelligence regarding the security significance of the matter before taking such action as the Chief Justice deems appropriate.

4. Appointment of Personnel. The court may have a Clerk of Court and such other legal, administrative or support personnel as it may require. The court may also arrange for the services of a court reporter, as it deems appropriate. Such personnel may have access to court

---

1 Section 103(c) of the Act reads in pertinent part: “The record of proceedings under this Act, including applications made and orders granted, shall be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of National Intelligence.” See also § 302(e) (physical search proceedings); § 501(f)(4) (proceedings regarding the production of records or other tangible things); § 702(k)(1) (proceedings regarding certain acquisitions of foreign intelligence information).
records and proceedings, including sensitive compartmented information or other classified
national security information contained therein, only as authorized by the court and only to the
extent necessary to the performance of an official function. Personnel appointed by or
designated for service to the court shall undergo appropriate background investigation by the
Federal Bureau of Investigation under applicable Executive Branch standards for investigations
performed in support of determinations of eligibility for access to sensitive compartmented
information or other classified national security information. All court personnel having access
to sensitive compartmented information or other classified national security information shall
sign appropriate security agreements. If a question concerning the security clearance of court
personnel is raised subsequent to appointment, the matter shall be referred to the court, which
may consult with the Attorney General and the Director of National Intelligence regarding its
security significance before taking such action as it deems appropriate.

5. Security Officer. The court shall designate as security officer the Director, Security
and Emergency Planning Staff, Department of Justice, or another individual who has
demonstrated competence in providing security for classified national security information and
sensitive compartmented information from among candidates submitted by the Attorney General
and the Director of National Intelligence. One or more alternate security officers may be
designated by the court as required. The security officer shall serve at the pleasure of the court
and will not be subject to removal by the Executive Branch without the concurrence of the court.
The security officer (and alternates) may be Executive Branch employees and may perform other
duties in the Executive Branch, so long as such duties do not conflict with their responsibilities to
the court. Additional personnel may be provided by the Department of Justice to perform
incidental security and administrative functions for the court provided appropriate security
clearances have been obtained.

The security officer shall be responsible to the court for document, physical, personnel,
and communications security. Under the supervision of the court, the security officer shall take
measures reasonably necessary to fulfill these responsibilities. The security officer shall arrange,
at a minimum, for an annual security review of court quarters and facilities and shall submit a
report to the court.

6. Security Functions of the Clerk of Court. The Clerk of Court, with the advice and
concurrence of the security officer, shall establish and maintain a control and accountability
system for all records of proceedings before the court that involve classified national security
information, and any other records or documents the court may designate. The Clerk, in
consultation with the security officer, shall further ensure that all court records are marked with
appropriate security classifications in accordance with Executive Order 13526 and its successors,
and procedures to be established by the court.

7. Court Proceedings. The court shall ensure that all court records (including notes,
draft opinions, and related materials) that contain classified national security information are
maintained according to applicable Executive Branch security standards for storing and handling
classified national security information. Records of the court shall not be removed from its premises except in accordance with the Act, applicable court rule, and these procedures. Insofar as the court may direct, the Clerk of the Court may, in coordination with the security officer, arrange for off-site storage of court records, provided that classified national security information contained therein is maintained according to the above-referenced security standards. Reports and exhibits submitted in support of applications to the court may be returned by the court to the applicant on a trust receipt basis.

Whenever a party other than the government makes a submission to the court that potentially contains classified national security information, the court shall promptly coordinate with the security officer to determine whether the submission contains classified national security information. The security officer shall, as directed by the court, consult with appropriate executive branch officials with regard to such a determination. The court may consider the submission while such a determination is pending, provided that the court safeguards the information in question as classified national security information in accordance with these procedures. The security officer shall, after consulting with the court, advise the parties of the results of the determination. If it is determined that the submission does contain classified national security information, the security officer shall ensure that it is marked with appropriate classification markings and the Clerk of Court shall ensure that it is handled in accordance with those markings under these procedures.

8. Security Procedures for Section 102(a) and Section 302(a). Certifications transmitted by the Attorney General to the Court under seal pursuant to Section 102(a) or Section 302(a) of the Act shall be numbered in sequence by the Clerk of Court, who shall maintain a record of all certifications received by the designated number and date of receipt.

Certifications received by the court for retention only shall be filed under seal in separate storage compartments. They shall only be accessed jointly by a representative designated by the court and a representative of the Executive Branch designated by the Attorney General. They may be unsealed only in accordance with the provisions of the Act.

9. Training. Members of the court and court personnel shall be briefed on security measures appropriate to the functions of the court by designees of the Attorney General and the Director of National Intelligence.

10. Term. These procedures shall remain in effect until modified in writing by the Chief Justice after consultation with the Attorney General and the Director of National Intelligence.
Issued this 21st day of FEBRUARY, 2013, after consultation with the Attorney General of the United States and the Director of National Intelligence as required by the Foreign Intelligence Surveillance Act.

John G. Roberts, Jr.
Chief Justice of the United States

The Attorney General concurs in the procedures for safeguarding certifications filed under Section 102(a) or Section 302(a) of the Act, as set forth in paragraph 8.²

Eric H. Holder, Jr.
Attorney General of the United States

² Section 103(c) provides that the Chief Justice shall establish security procedures for the court in consultation with the Attorney General and the Director of National Intelligence. Sections 102(a)(3) and 302(a)(3) provide that certifications of the Attorney General issued in accordance with Section 102(a)(1) or Section 302(a)(1)(A) of the Act shall be maintained under security measures established by the Chief Justice with the concurrence of the Attorney General, in consultation with the Director of National Intelligence.
BRIEF OF AMICUS CURIAE

On July 15, 2015, the government submitted to this Court certifications and accompanying targeting and minimization procedures (collectively, "the 2015 Certifications") seeking approval of the government's activities under Section 702 of the Foreign Intelligence Surveillance Act of 1978 (FISA), codified at 50 U.S.C. Section 1881a. The Court found that this matter raised "one or more novel or significant interpretations of the law" requiring the appointment of amicus curiae, and on August 13, 2015, the Court issued an Order ("Order") appointing me to serve as amicus curiae under section 103(j)(2)(B) of the FISA, 50 U.S.C.

The Order directed me to address whether the minimization procedures that accompany the 2015 Certifications (a) meet the definition of minimization procedures under 50 U.S.C. Section 1801(h) or Section 1821(4), as appropriate, and (b) are consistent with the Fourth Amendment, with respect to two specific provisions of those procedures. Specifically, the Order directed me to address the provisions that apply to (i) queries of information obtained under section 702 that may be designed to return information concerning U.S. persons; and (ii) preservation for litigation purposes of information otherwise required to be destroyed under the applicable minimization procedures. Order, at 4. I will address these issues separately in turn.

Before turning to the issues, some background information may be helpful for purposes of the record regarding my appointment and service as amicus. The Order designating my appointment was issued on August 13, 2015. On August 23, 2015, I was provided with a copy of that Order and received a briefing from Judge Hogan and the staff of the Foreign Intelligence Surveillance Court ("FISC") concerning the questions presented.

This material included the Court’s several Orders relating to the amicus appointment; the government’s explanatory memorandum or “Cover Note,” entitled “Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications” (“Cover Note”), along with the relevant DNI/AG certifications and targeting and minimization
SECRET//NOFORN

procedures (in both clean form and in redlined form reflecting changes from the 2014 procedures) and other exhibits that were submitted to the Court with the 2015 Certifications; and

prior FISC or FISA Court of Review decisions relating to the Section 702 program and the issues I was directed to address. I was also provided with the unclassified Privacy and Civil Liberties Oversight Board ("PCLOB") Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, issued on July 2, 2014 ("PCLOB Report").

I already possessed a security clearance issued by the Department of Justice ("DOJ") for other matters, and that clearance was verified by the DOJ's Security and Emergency Planning Staff ("SEPS") for purposes of this assignment. I do not have regular access to a facility where I can keep classified information, however, so I was not able to take possession of any of the classified materials. I was provided access to a secure conference room in the SEPS offices at 145 N Street, NE, where I could work and have access to the classified materials. SEPS personnel assisted with providing access to the conference room and the classified materials and secured the classified materials when I was not using them. While the space was not available after 5:00 pm in the evening or on weekends or during periods of unexpected government closures (such as during the Pope's September visit to Washington), I had access during regular work hours.¹

My understanding of my role as amicus was informed by the statute, 50 U.S.C. Section 1803(i), as well as the Court's Orders and my briefing from the Court. Section 1803(i)(4) sets

¹ In addition, the FISC staff provided access to secure space at the Courthouse on one federal holiday and one evening after hours.
forth the specific duties of amicus curiae. The duties relevant to this assignment include
providing “legal arguments that advance the protection of individual privacy and civil liberties”
or “legal arguments or information regarding any other area relevant to the issue presented to the
court” as appropriate. 50 U.S.C. Sections 1803(i)(4)(A) and (C). In order to understand and
present these arguments, I reviewed the PCLOB report and the written submissions and
testimony before the PCLOB for its hearings on Section 702 surveillance, as well as commentary
on Section 702 from academic experts and non-government advocacy groups. In addition, I met
with attorneys from the DOJ National Security Division (NSD) Office of Intelligence, who
answered specific questions about the operation of the Section 702 program and their oversight
of it. I also met with a member of the PCLOB, and again asked questions to ensure that I fully
understood the concerns that motivated the PCLOB’s recommendations. See 50 U.S. C. Section
1803(i)(6)(A)(ii). With that background, I should explain that I was not instructed to serve as an
advocate for any particular point of view, but as an amicus to the Court. This Brief contains my
opinion and recommendations on the issues presented based on the material that I have reviewed
and my analysis of those issues.²

² I have some familiarity with FISA and the government’s surveillance programs generally due to my previous
government service (in particular as Counselor to the Attorney General for national security and international
matters and as Chief of the National Security Section for the U.S. Attorney’s Office for the District of Columbia).
That background in intelligence collection and national security law satisfies the criteria of Section 1803(1)(3)(A). I
have never worked in the National Security Division or worked directly on the Section 702 program, however, so
the attorneys representing the government in this matter will have far greater familiarity with the program. That
said, I understand the Court’s need for an independent view of the issues I was directed to address and am honored
to serve the Court in this capacity.
Queries Designed to Return Information Concerning U.S. Persons

The use of queries to search the information collected under Section 702 for the communications of specific U.S. persons was one of the areas in which the PCLOB Report made specific recommendations for improvement. The PCLOB spent more than a year studying and debating the Section 702 program, including holding numerous public hearings and receiving written submissions from a wide variety of government officials, academic experts, interest groups, and any interested parties who chose to submit views. Given the PCLOB's bipartisan makeup, the record of its serious and diligent effort to understand the program, and the thoroughness and high quality of its Report, I give its recommendations great weight.

A. Background

The PCLOB Report contains a thorough explanation of the Section 702 surveillance program. That description is set forth on pages 16-79 of the Report. For purposes of my analysis, I have relied upon the PCLOB Report's explanation of how the Section 702 program operates as well as the Report's description of the principal safeguards in place (as of the date the Report was issued) to protect privacy and civil liberties interests.

Section 702 provides for the joint authorization by the Attorney General and Director of National Intelligence of "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. Section 1881a(a). The principal limitations to the Section 702 program are statutory. Specifically, the authorization of acquisitions under Section 702 must comply with Section 702(b), which provides:

An acquisition under subsection (a)--
SECRET//NOFORN

(1) may not intentionally target any person known at the time of acquisition to be located in the United States;

(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose is to target a particular, known person reasonably believed to be in the United States;

(3) may not intentionally target a United States person reasonably believed to be located outside the United States;

(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and

(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

50 U.S.C. Section 1881a(b). Acquisition under subsection (a) must also be conducted in accordance with targeting and minimization procedures that are adopted by the Attorney General, in consultation with the Director of National Intelligence, and subject to judicial review.

50 U.S.C. Section 1881a(e)(1)(A) and 50 U.S.C. Section 1881a(d) and (e).

Minimization procedures with respect to electronic surveillance are defined in 50 U.S.C. Section 1801(h):

“Minimization procedures”...means—

specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

3 "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.
50 U.S.C. Section 1801(h)(1).

As those limitations make clear, the program is directed at communications of non-U.S. persons located outside the United States. U.S. persons may not be targets of collection, so the collection of their communications is "incidental" to the program's purpose and requires strict procedures to ensure that the information is treated appropriately. The PCLOB Report thus rightly focused on the querying of the collection using U.S. person identifiers as warranting particular scrutiny to ensure that the privacy and civil liberties interests of U.S. persons are adequately protected.

B. PCLOB Recommendations

While the PCLOB Report concluded that "the core of the Section 702 program" was reasonable under the Fourth Amendment, it identified three aspects of the program as areas of concern and issued recommendations to improve upon existing policies and practices in order to further strengthen protections under the program in those areas. As stated in the PCLOB Report's Executive Summary:

On the whole, the text of Section 702 provides the public with transparency into the legal framework for collection, and it publicly outlines the basic structure of the program. The Board concludes that PRISM collection is clearly authorized by the statute . . . . The Board also concludes that the core of the Section 702 program - acquiring the communications of specifically targeted foreign persons who are located outside the United States, upon a belief that those persons are likely to communicate foreign intelligence, using specific communications identifiers, subject to FISA court-approved targeting rules and multiple layers of oversight - fits within the 'totality of the circumstances' standard for reasonableness under the Fourth Amendment, as that standard has been defined by the courts to date. Outside of this fundamental core, certain aspects of the Section 702 program push the program close to the line of constitutional reasonableness. Such aspects include the unknown and potentially large scope of incidental collection of U.S. persons' communications, the use of "about"
collection to acquire Internet communications that are neither to nor from the target of surveillance, and the use of queries to search for the communications of specific U.S. persons within the information that has been collected.

PCLOB Report at 8-9. The Court has directed me to address the third of those aspects – the use of queries to search for communications of specific U.S. persons.

The PCLOB Report made two specific recommendations to address its concerns with the use of U.S. person identifiers for querying Section 702-acquired information. The government has thoughtfully considered these recommendations and has made several changes to the Section 702 program in response.

PCLOB’s Recommendation 2 focused on the FBI’s use of U.S. person queries and made two specific suggestions:

The FBI’s minimization procedures should be updated to more clearly reflect the actual practice for conducting U.S. person queries, including the frequency with which Section 702 data may be searched when making routine queries as part of FBI assessments and investigations. Further, some additional limits should be placed on the FBI’s use and dissemination of Section 702 data in connection with non-foreign intelligence criminal matters.

PCLOB Report, at 11-12.

Recommendation 3 suggested changes to the NSA and CIA minimization procedures governing U.S. person queries:

The NSA and CIA minimization procedures should permit the agencies to query collected Section 702 data for foreign intelligence purposes using U.S. person identifiers only if the query is based upon a statement of facts showing that it is reasonably likely to return foreign intelligence information as defined in FISA. The NSA and CIA should develop written guidance for agents and analysts as to what information and documentation is needed to meet this standard, including specific examples.
SECRET//NOFORN

PCLOB Report, at 12. The use of U.S. person queries was also the subject of two separate statements, each signed by two PCLOB members, as described more fully below.

C. Scope of Collection of U.S. Person Communications

The use of U.S. person queries must be examined in the context of the scope of Section 702 collection. It is worth noting how the PCLOB's other concerns, relating to the scope of incidental and "about" collection, bear upon this analysis. The use of U.S. person identifiers in the querying process is of greater concern when considered in the context of the larger concerns with the scope of the information being queried. The Court has not directed me to examine the scope of "incidental" and "about" collection more broadly, but the PCLOB's concerns about the use of U.S. person identifiers to query the data are heightened due to the concerns that "incidental" and "about" collection result in a large and unknown quantity of U.S. person communications. (The incidental collection of U.S. person communications is the more relevant category given that the NSA does not query its "upstream" collection using U.S. person identifiers. 4)

The "incidental" collection of communications of U.S. persons under Section 702 is "incidental" only in that the communications are not targeted based on the U.S. person involved. Yet some of those communications are the most important communications obtained under Section 702, to the extent that they may reveal U.S.-based operatives communicating with foreign targets about terrorist plots, weapons of mass destruction, or other threats in the United States. In other words, while the U.S. person involved in an incidentally acquired

4 Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended (Exhibit B to the 2015 Certifications) ("NSA Minimization Procedures"); Section 3(b)(5).
communication would not (by definition) be the target of Section 702 collection, that person’s communication may be highly relevant to the purpose of the collection – as the ultimate purpose of the program is to collect foreign intelligence information (and in so doing to protect national security). This point is worth bearing in mind in the context of analyzing the querying process.

Yet the concerns with incidental collection are not with the would-be plotter and those in communication with him. Those communications are at the extreme end of the spectrum, where the justification for collecting and querying the communications is strongest. But not all Section 702 targets are international terrorists.
These scenarios suggest a potentially very large and broad scope of incidental collection of communications between lawful targets and U.S. persons that are not the type of communications Section 702 was designed to collect. This area of collection is where the privacy interests in the U.S. persons’ communications that are incidentally collected are strongest.

D. Analysis of Minimization Procedures

The scope of the incidental collection is broad. The potential for collecting a large quantity of U.S. person communications that have no foreign intelligence value raises significant Fourth Amendment concerns. I therefore agree with the PCLOB that the use of U.S. person information to query Section 702-acquired information must be governed by stringent procedures in order to meet the Fourth Amendment’s reasonableness requirement. The question is whether the minimization procedures that the agencies have adopted with respect to U.S. person queries meet that standard and protect the privacy interests of U.S. persons sufficiently to comply with the Fourth Amendment. In addition, the minimization procedures must comply with the purpose and statutory requirements of Section 702.

The agencies have different minimization procedures that are designed in light of their differing missions and roles in the acquisition and use of Section 702-acquired information. The use of U.S. person identifiers in querying is most difficult for FBI given its responsibilities for domestic law enforcement. The government has made changes to NSA’s and CIA’s

---

5 The American Civil Liberties Union highlighted similar concerns with the actual targets of surveillance in its submission to the PCLOB: “[T]he government’s surveillance targets may be political activists, victims of human rights abuses, journalists, or researchers. The government’s targets may even be entire populations or geographic regions.” Submission of Jameel Jaffer, Deputy Legal Director, ACLU Foundation (March 19, 2014) (available at PCLOB website, www.pclob.gov).
SECRET/NOFORN

minimization procedures to provide safeguards for U.S. person information, and their procedures now have specific requirements for U.S. person queries that protect against their misuse. The FBI’s procedures do not have such requirements. While I recognize that the FBI’s role makes it more difficult to adopt such procedures, the FBI’s existing minimization procedures do not in my view provide adequate safeguards for U.S. person queries of Section 702-acquired information and are not consistent with the purpose of Section 702. I therefore respectfully recommend that the Court find that the existing FBI minimization procedures must be changed to include additional protections in order to comply with the Fourth Amendment and the statutory requirements.

1. NSA and CIA Minimization Procedures

The NSA and CIA minimization procedures have both been amended in response to the PCLOB’s recommendation, which stated:

The NSA and CIA minimization procedures should permit the agencies to query collected Section 702 data for foreign intelligence purposes using U.S. person identifiers only if the query is based upon a statement of facts showing that the query is reasonably likely to return foreign intelligence information as defined in FISA. The NSA and CIA should develop written guidance for agents and analysts as to what information and documentation is needed to meet this standard, including specific examples.

PCLOB Report, at 139. The NSA and CIA minimization procedures that were submitted with the 2015 Certifications reflect this change, and both sets of procedures now require a written statement explanation of their justification of a U.S. person query.

The NSA procedures now provide (with newly added language emphasized in bold):

Any use of United States person identifiers as terms to identify and select communications must first be approved in accordance with NSA procedures,
which must require a statement of facts establishing that the use of any such identifier as a selection term is reasonably likely to return foreign intelligence information, as defined in FISA. NSA will maintain records of all United States person identifiers approved for use as selection terms. The Department of Justice’s National Security Division and the Office of the Director of National Intelligence will conduct oversight of NSA’s activities with respect to United States persons that are conducted pursuant to this paragraph.

Minimization Procedures Used by the National Security Agency in Connection with

Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended (Exhibit B to the 2015 Certifications) ("NSA Minimization Procedures"), Section 3(b)(5).

Similarly, the CIA procedures provide (with newly added language emphasized in bold):

CIA personnel may query CIA electronic and data storage systems containing unminimized communications acquired in accordance with section 702 of the Act. Such queries must be reasonably likely to return foreign intelligence information as defined in FISA. Any United States person identity used to query the content of communications must be accompanied by a statement of facts showing that the use of any such identity as a query term is reasonably likely to return foreign intelligence information as defined in FISA. CIA will maintain records of all such queries using United States person identities, and NSD and ODNI will review CIA’s queries of content using any such identity as a query term to ensure that they were reasonably likely to return foreign intelligence information as defined in FISA.

Minimization Procedures Used by the Central Intelligence Agency in Connection with

Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended (Exhibit E to the 2015 Certifications) ("CIA Minimization Procedures"), Section 4.

The requirement by both agencies of a written statement of facts is a significant enhancement to the safeguards of U.S. person communications acquired pursuant to Section 702.
Agency personnel conducting the queries must now set forth their reasons for each query based on a U.S. person identifier, and explain why the query is likely to return foreign intelligence information. That process ensures that every U.S. person query conducted by NSA and CIA is the subject of considered judgment reduced to writing. This requirement alone helps ensure that U.S. person queries are not overused or abused. In addition, the written statement of facts will be maintained and subject to supervisory review as well as oversight. The substantial oversight by DOJ and ODNI (described in NSD's unclassified summary of the oversight program, attached to the government’s Cover Note at tab 1) provides an additional important layer of protection to help ensure that the U.S. queries of Section 702 data are not used excessively or improperly. These procedures appear to be sufficient to ensure that the NSA and CIA are using U.S. person identifiers in a manner consistent with the Fourth Amendment and statutory requirements.

The government’s Cover Note states that these procedures are the subject of written guidance and training, comporting with the second part of the PCLOB Report’s Recommendation 3, namely: “The NSA and CIA should develop written guidance for agents and analysts as to what information and documentation is needed to meet this standard, including specific examples.” PCLOB Report, at 139; Cover Note, at 20-21.

The government has fully implemented the PCLOB’s recommendations with respect to the NSA and CIA’s use of U.S. person identifiers in querying Section 702-acquired information. I conclude that the NSA and CIA minimization procedures are sufficient to ensure that the use of U.S. person identifiers for that purpose complies with the statutory requirements of Section 702 and with the Fourth Amendment.
2. 

FBI Minimization Procedures

The PCLOB Report did not similarly recommend that the FBI minimization procedures require a written statement of facts to justify every use of a U.S. person identifier in querying the Section 702-acquired information. The difference in the majority’s recommendations for NSA and CIA on the one hand and FBI on the other is based on the differences between the missions of the agencies and the way that they conduct queries of the Section 702 collection. As the PCLOB Report explained: “The FBI’s rules relating to queries do not distinguish between U.S. persons and non-U.S. persons; as a domestic law enforcement agency, most of the FBI’s work concerns U.S. persons.” PCLOB Report, at 137.

The PCLOB Report therefore made a more modest recommendation with respect to the FBI:

The FBI’s minimization procedures should be updated to more clearly reflect actual practice for conducting U.S. person queries, including the frequency with which Section 702 data may be searched when making routine queries as part of FBI assessments and investigations. Further, some additional limits should be placed on the FBI’s use and dissemination of Section 702 data in connection with non-foreign intelligence criminal matters.

PCLOB Report, at 137.

The government has revised the FBI minimization procedures in response to the first part of this recommendation, and the procedures now explain in some greater detail the FBI’s practice for conducting these queries. The new language can be found in two footnotes in the FBI Minimization Procedures, specifically footnotes 3 and 4 at pages 11 and 12, respectively.

Footnote 3 provides:
It is a routine and encouraged practice for the FBI to query databases containing lawfully acquired information, including FISA-acquired information, in furtherance of the FBI’s authorized intelligence and law enforcement activities, such as assessments, investigations and intelligence collection. Section III.D. [of the minimization procedures] governs the conduct of such queries. Examples of such queries include, but are not limited to, queries reasonably designed to identify foreign intelligence information or evidence of a crime related to an ongoing authorized investigation or reasonably designed queries conducted by FBI personnel in making an initial decision to open an assessment concerning a threat to the national security, the prevention of or protection against a Federal crime, or the collection of foreign intelligence, as authorized by the Attorney General Guidelines [regarding opening assessments]. These examples are illustrative and neither expand nor restrict the scope of the queries authorized in the language above.

Minimization Procedures Used by the Federal Bureau of Investigation in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended (Exhibit D to the 2015 Certifications) (“FBI Minimization Procedures”), Section III.D.

Footnote 4 provides:

(b)(1); (b)(3); (b)(7)(E)
FBI Minimization Procedures, Section III.D.

These footnotes clarify the existing practice, but as noted in footnote 3, they do not restrict the use of U.S. person queries. In my view, restrictions like those adopted in the NSA and CIA procedures are necessary to comply with the Fourth Amendment.

Before turning to that analysis, it is worth noting the government has also made changes in response to the second point in PCLOB’s Recommendation 2. Specifically, the government has taken steps to impose additional limits on the FBI’s use of Section 702 data in connection with non-foreign intelligence criminal matters, though these limits are not reflected in the minimization procedures. The ODNI announced these reforms in its Signals Intelligence Reform 2015 Anniversary Report (available at http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#section-702, a website maintained by the ODNI). The specific reforms are described in the report as follows:

[C]onsistent with the recommendation of the Privacy and Civil Liberties Oversight Board, information acquired under Section 702 about a U.S. person will not be introduced as evidence against that person in any criminal proceeding except (1) with the approval of the Attorney General, and (2) in criminal cases with national security implications or certain other serious crimes. This change will ensure that, if the Department of Justice decides to use information acquired under Section 702 about a U.S. person in a criminal case, it will do so only for national security purposes or in prosecuting the most serious crimes.

lifts-as-prepared) on February 4, 2015. Specifically, he listed the “most serious crimes” for which the use of Section 702-acquired information would be permitted:

Under the new policy, in addition to any other limitations imposed by applicable law, including FISA, any communication to or from, or information about, a U.S. person acquired under Section 702 of FISA shall not be introduced as evidence against that U.S. person in any criminal proceeding except (1) with the prior approval of the Attorney General and (2) in (A) criminal proceedings related to national security (such as terrorism, proliferation, espionage, or cybersecurity) or (B) other prosecutions of crimes involving (i) death; (ii) kidnapping; (iii) substantial bodily harm; (iv) conduct that constitutes a criminal offense that is a specified offense against a minor as defined in 42 USC 16911; (v) incapacitation or destruction of critical infrastructure as defined in 42 USC 5195c(e); (vi) cybersecurity; (vii) transnational crimes; or (vii) [sic] human trafficking.

http://icontherecord.tumblr.com/post/110632851413/odni-general-counsel-robert-lifts-as-prepared. These limitations are responsive to the PCLOB’s recommendation and provide additional assurances that the government’s use of U.S. person identifiers will be cabined in a manner consistent with the Fourth Amendment. As policy statements made in reports and official remarks, they are not formally part of the complex structure of requirements that apply to Section 702 collection. I would recommend that these policies be specifically incorporated into the FBI’s minimization procedures, to ensure that they become binding and lasting reforms.

These changes respond to some of the PCLOB’s concerns and are improvements. Yet in my view they do not go far enough. I am not persuaded that the FBI should not be subject to similar requirements as NSA and CIA because of the difficulties in separating U.S. person queries from non-U.S. person queries or because of how the Section 702-acquired information is maintained in FBI’s databases. The civil liberties and privacy concerns with the Section 702 collection are not any less compelling in the context of FBI querying than they are with respect
to NSA and CIA – to the contrary, they are more so, precisely because the FBI’s mission includes domestic law enforcement. Furthermore, the FBI’s use of U.S. person queries strays well beyond the foreign intelligence purpose of the Section 702 program. In my view, the FBI should require a particularized statement of facts to support each query of Section 702-acquired information that justifies the need for the query. I conclude that the FBI’s minimization procedures without that requirement do not adequately comply with the Fourth Amendment and statutory requirements of Section 702.

The FBI’s querying procedures effectively treat Section 702-acquired data like any other database that can be queried for any legitimate law enforcement purpose. The minimization procedures do not place any restrictions on querying the data using U.S. person identifiers – in part because the FBI does not distinguish between U.S. and non-U.S. persons in querying its databases. As a result, FBI may query the data using U.S. person identifiers for purposes of any criminal investigation or even an assessment. There is no requirement that the matter be a serious one, nor that it have any relation to national security. For the reasons set forth below, these practices do not comply with Section 702 or the Fourth Amendment.

E.  Legal Analysis

The FBI’s minimization procedures fall short of what Section 702 and the Fourth Amendment require. They permit the FBI to go far beyond the purpose for which the Section 702-acquired information is collected in permitting queries that are unrelated to national security. They do not provide sufficient safeguards to protect the privacy and civil liberties interests at stake. For both reasons, the FBI’s minimization procedures should be revised to ensure that U.S.
person queries are conducted in a manner consistent with Section 702 and the Fourth Amendment.

1. The FBI’s Queries Are Inconsistent with the Purpose of Section 702

In one of the few decisions of the FISA Court of Review, the Court stated: “the FISA process cannot be used as a device to investigate wholly unrelated crimes.” In re Sealed Case, 310 F.3d 717, 736 (FISA Ct. Rev. Nov. 18, 2002) (holding that FISA did not require the government to demonstrate to the Court that its primary purpose in conducting surveillance was not criminal prosecution). Yet the FBI’s minimization procedures permit precisely such use of the Section 702-acquired information. Per the PCLOB Report:

With some frequency, FBI personnel will also query this data, including Section 702-acquired information [which is stored in the same repositories as traditional FISA data], in the course of criminal investigation and assessments that are unrelated to national security efforts. . . . [A]n assessment may be initiated “to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence information” (citing the Attorney General’s Guidelines for Domestic FBI Operations, § II.A.).

PCLOB Report, at 60. While the decision in In re Sealed Case predates the enactment of Section 702, Section 702 did not fundamentally change the purpose of FISA. The FBI’s virtually unrestricted querying of FISA and Section 702-acquired data is inconsistent with the purpose of Section 702 and should not be permitted.

Moreover, the FBI’s minimization procedures do not provide sufficient safeguards to ensure that U.S. person queries of Section 702-acquired information are justified and reasonable given the privacy interests those queries implicate. The FBI’s minimization procedures must
therefore be amended to provide similar safeguards to those that the changes to CIA’s and NSA’s procedures now provide.

2. Precedents Regarding Prior Certifications Are Not Binding on This Court

The Court has not previously found the agencies’ minimization procedures with respect to queries involving U.S.-person identifiers to be deficient. Even without the improvements that have been made through the changes described above, the Court found in reviewing Certifications for prior years that the minimization procedures governing the use of U.S. person identifiers under Section 702 met the statutory requirements of Section 702. When the government initially broadened the NSA’s minimization procedures to permit queries using U.S. person identifiers, Judge Bates considered the issues raised by this change and found that the minimization procedures (without the change described above in response to the PCLOB Report) were consistent with the statutory requirements and the Fourth Amendment.

This relaxation of the querying rules does not alter the Court’s prior conclusion that NSA minimization procedures meet the statutory definition of minimization procedures. The Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under the Foreign Intelligence Surveillance Act ("FBI SMPs") contain an analogous provision allowing queries of unminimized FISA-acquired information using identifiers – including United States-person identifiers – when such queries are designed to yield foreign intelligence information. See FBI SMPs § III.D. In granting hundreds of applications for electronic surveillance or physical search since 2008, including applications targeting United States persons and persons in the United States, the Court has found that the FBI SMPs meet the definitions of minimization procedures at 50 USC 1801(h) and 1821(4). It follows that the substantially-similar querying provision found at Section 3(b)(5) of the amended NSA minimization procedures should not be problematic in a collection that is focused on non-United States persons located outside the United States and that, in the aggregate, is less likely to result in the acquisition of nonpublic information regarding non-consenting United States persons.
In re DNI/AG Certifications (Oct. 3, 2011), at 23-24. The purpose of queries in the current version of the FBI Minimization Procedures, § III.D., is broader, however, than what the Court described, in permitting queries that identify information that "reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime"\(^6\) (emphasis added). In addition, while I agree with the Court's analysis that the Section 702 collection may be less likely than traditional FISA-acquired information to contain U.S. person information, traditional FISA acquisition occurs pursuant to individualized judicial determinations, so the scope and scale of the incidental collection in those cases does not raise the same concerns as the incidental collection under Section 702, as explained in Section I.C. above and in the PCLOB Report.

The Court's prior decisions should not, in my view, preclude the Court from reaching a different conclusion with respect to the 2015 Certifications. Prior FISC decisions should not be viewed (and have not been so understood by the Court) as binding precedent to the same extent as in the traditional Article III context. While the Court's decision and rationale in approving the 2011 Certifications and other prior decisions are instructive, the fact that the Court has previously approved similar or identical procedures should not be binding on this Court in evaluating the sufficiency of the procedures submitted with the Section 2015 Certifications. Due to the unusual nature of proceedings before the FISC, its consideration of substantially similar certifications from one year to the next may change due to developments in the Court's understanding of the relevant programs over time, in addition to changes in the law. The Court's

\(^6\) I do not have the 2011 Procedures and do not know whether the language was the same as the current version.
consideration of the issues before it is also constrained by the ex parte nature of FISC proceedings. In my view, there is both new information available to the Court as well as an intervening legal development that the Court can and should take into account in reaching a different conclusion in evaluating the 2015 Certifications.

The PCLOB Report and its observations and recommendations with respect to incidental collection and U.S. person queries constitute significant new information available to the Court.\(^7\) It would not be unprecedented for this Court to reach a different conclusion than the Court has reached in the past based on new information. Developments in the understanding of how the Section 702 program operates have provided a sufficient basis in prior years for the Court to reject certifications that had previously been approved in identical or substantially similar form.

For example, in ruling on the 2011 Certifications, Judge Bates took into account new information regarding NSA’s “upstream” collection, and based on concerns with that collection, ruled that minimization procedures that had previously been approved for prior years were not constitutional. In re DNI/AG 702(g) Certification, \[REDACTED\], at 80 (Oct. 3, 2011). The Court explained that the new information about the government’s collection fundamentally altered its understanding of the scope of collection pursuant to Section 702 and required a reexamination of its prior approvals of the program. Id. at 15.

\(^7\) While the PCLOB Report was issued in July, 2014, which was prior to the Court’s approval of the 2014 Certifications, the time frame for submission and consideration of the 2014 Certifications did not permit consideration of its observations and recommendations. The 2014 Certifications were filed with the Court on July 28, 2014. In re DNI/AG 702(g) Certification, \[REDACTED\], (Aug. 26, 2014), at 1. The Court issued its decision on August 26, 2014 (Id. at 43), and the decision makes no mention of the PCLOB Report.
In addition, Congress enacted the USA FREEDOM Act in June, 2015, authorizing the appointment of amicus curiae, in recognition that there may be matters presented to the Court that present a “novel or significant” interpretation of the law. 50 U.S.C. Section 1803(i)(2)(A). Congress envisioned that there would be matters for which information and argument from amicus curiae would help the Court evaluate the arguments and information presented by the government. The Court has found that the 2015 Certifications present such issues, in recognition of its ongoing obligation to evaluate the Certifications presented each year in light of all available information concerning the operation of the Section 702 program. That information now includes the PCLOB Report’s substantial and weighty analysis of the Fourth Amendment issues surrounding the use of U.S. person identifiers to query Section 702-acquired information.

3. The Fourth Amendment Applies to Querying

The government may argue\(^8\) that the Fourth Amendment should not apply at all to the querying of Section 702-acquired information, because the Court has already found that the collection itself – which is the actual “search” – satisfies the Fourth Amendment’s reasonableness requirement. The argument would be that the collection itself is the search, and once that collection is authorized, querying the collection is simply a use of the information like any other, and not subject to the Fourth Amendment. That argument should be rejected in the context of electronic evidence. The issues relating to electronic evidence have changed the law.

---

\(^8\) Due to the statutory deadlines and costs associated with extending the deadlines for authorizing the program (see Government’s Response to the Court’s Order of July 7, 2015 (July 14, 2015), at 8, n. 8), the Court ordered that the amicus brief and the government’s brief in this matter be submitted at the same time, on October 16, 2015, so we are not in a position to respond directly to one another’s arguments until oral argument, which the Court scheduled for October 20, 2015, if the Court determines that oral arguments would be beneficial—Briefing Order (Sept.-16-2015), at 4.
regarding what constitutes a search. A separate warrant is required to search the contents of a

cell phone or computer hard drive when those items are lawfully seized in connection with an

individual’s arrest or a lawfully authorized search that does not specifically authorize such

searches. See Riley v. California, 573 U.S. ___, 134 S.Ct. 2473, 2493 (2014) (holding that

police must obtain warrant to authorize search of digital contents of cell phone lawfully seized

incident to arrest).

The government may seek to rely on case law from other contexts that suggests that if

information is lawfully collected in a manner consistent with the Fourth Amendment, the

querying of that information does not implicate the Fourth Amendment. See Boroian v. Mueller,

616 F.3d 60, 67-68 (1st Cir. 2010) (running search of an individual’s DNA profile against other

profiles in a DNA database “does not violate an expectation of privacy that society is prepared to

recognize as reasonable, and thus does not constitute a separate search under the Fourth

Amendment”); Johnson v. Quander, 440 F.3d 489, 498-99 (D.C. Cir. 2006) (accessing records

stored in a DNA database is not a “search” for Fourth Amendment purposes). The scope and

manner of Section 702 collection is so unusual and so different from the manner of collection of

DNA that these cases should not control. DNA is generally collected within the traditional

structures of the criminal justice system in compliance with constitutional guarantees. It is

collected from persons who are subject to arrest based on probable cause. It may also be

collected pursuant to court order. The government is not incidentally collecting large quantities

of DNA using methods unrelated to specific law enforcement objectives and depositing it in its

---

9 The government may also occasionally collect “abandoned” DNA, such as from the discarded coffee cup of a

known suspect, but this practice is significantly infrequent that it does not substantially increase the contents of

DNA databases.
databases. The incidental collection of Section 702 information is far removed from the stringent requirements of criminal procedure and warrants different treatment.

4. Amended Minimization Procedures Would Provide Sufficient Protection

PCLOB Chairman Medine and Board Member Wald, in their separate statement, made a recommendation that would go further than the PCLOB majority recommendation, and further than mine as well. They recommended:

Each U.S. person identifier should be submitted to the FISA court for approval before the identifier may be used to query data collected under Section 702 for a foreign intelligence purpose, other than in exigent circumstances or where otherwise required by law. The court should determine, based on documentation submitted by the government, whether the use of the U.S. person identifier for Section 702 queries meets the standard that the identifier is reasonably likely to return foreign intelligence information as defined under FISA.

PCLOB Report, Annex A, at 151-152 (footnotes omitted). This recommendation has the appeal of restoring the traditional case by case assessment that the FISA court conducts in reviewing individual applications for electronic surveillance and physical searches. While such court approval for every U.S. person query would be ideal, in my view the requirement that each U.S. person query be supported by a written statement explaining why the query is likely to return foreign intelligence information or is otherwise justified, subject to oversight and review, is sufficient to meet the statutory and constitutional requirements.

My recommendation goes beyond the suggestion in the separate statement by PCLOB Board Members Rachel Brand and Elisebeth Collins Cook. Their statement explained that the issue of queries using U.S. person identifiers divided the Board. Specifically with respect to the FBI, they noted:
In the case of the FBI, this issue is intertwined with questions about querying Section 702 information for non-foreign intelligence purposes, the potential use of Section 702 information in criminal proceedings, and longstanding efforts to ensure information sharing within the agency.

PCLOB Report, Annex B, at 161. They did not recommend limiting FBI’s ability to query using U.S. person identifiers. Instead, they endorsed the majority report’s more limited recommendations. They also raise numerous objections to the other separate statement’s proposed requirement of specific FISC approval for queries using U.S. person identifiers.

The PCLOB majority recommendation does not in my opinion go far enough. In my view, specific changes to the FBI minimization procedures are required in order to ensure that U.S. person queries are conducted in a manner consistent with Section 702 and the Fourth Amendment. The procedures should require a written justification for each U.S. person query of the database that explains why the query is relevant to foreign intelligence information or is otherwise justified. If that means in practice that every FBI query of the Section 702-acquired information requires a written justification, that practice may be what is needed. Imposing such a requirement would not substantially restrict the FBI’s ability to query Section 702-acquired information when there is a legitimate reason to do so. Rather, it would impose an internal check on the querying process, and a fairly minimal one. If an FBI agent is querying Section 702-acquired information to return information regarding a U.S. person, there should be a sufficient basis to justify that query. This requirement may therefore limit querying the Section 702-acquired information when there is no value to the query. That restriction does not seem unreasonable.
SECRET/NOFORN

There are several ways in which the FBI may be able to amend its minimization procedures to ensure that querying is conducted in a manner consistent with the requirements of Section 702. The requirement that NSA and CIA have adopted in their minimization procedures is one option, but there may be other language that better accommodates the different manner in which FBI maintains and queries the information. The Court should reject the minimization requirements as drafted on the ground that they do not provide sufficient protection for this information and require amended procedures that do.

II. Litigation-Related Preservation of Material Otherwise Required to be Destroyed

The second issue that I have been directed to address is “the preservation for litigation purposes of information otherwise required to be destroyed under the minimization procedures.” Order, at 4.

A. Relevant Minimization Procedures

The NSA, FBI, and CIA minimization procedures all contain provisions that permit the agencies to retain information that would otherwise be subject to destruction requirements based on a determination that such retention is necessary given competing obligations to maintain information for litigation purposes.

Specifically, NSA’s minimization procedures provide:

Notwithstanding the destruction requirements set forth in these minimization procedures, NSA may retain specific section 702-acquired information if the Department of Justice advises NSA in writing that such information is subject to a preservation obligation in pending or anticipated administrative, civil, or criminal litigation. . . . The Department of Justice shall notify NSA in writing once the section 702-acquired information is no longer required to be preserved for such
litigation matters, and then NSA shall promptly destroy the section 702-acquired information as otherwise required by these procedures.

NSA Minimization Procedures, Section 3(c)(4)a. NSA must provide NSD a summary of all such matters each year. NSA’s procedures also include a requirement that the retention of this information be reported to the FISC and coordinated with the Department of Justice so that NSA is promptly notified when the preservation obligation is no longer in force and can take steps to destroy the material upon such notification:

The Department of Justice’s National Security Division will promptly notify and subsequently seek authorization from the FISC to retain the material as appropriate and consistent with law. NSA will restrict access to and retain such information in the manner described in subparagraph 4(a), at the direction of the Department of Justice until either the FISC denies a government request for authorization to retain the information or the Department of Justice notifies NSA in writing that the information is no longer required to be preserved for such litigation matters. After receiving such notice, NSA shall promptly destroy the section 702-acquired information as otherwise required by these procedures.

NSA Minimization Procedures, Section 3(c)(4)b.

CIA’s minimization procedures include similar requirements:

Notwithstanding the destruction requirements set forth in these minimization

CIA Minimization Procedures, Section 11.a. CIA must similarly report to NSD a summary of all material retained under this provision. Id.

FBI’s minimization procedures are substantially similar to those of NSA and CIA with respect to this issue. They provide:
The FBI may temporarily retain specific FISA-acquired information that would otherwise have to be destroyed under these procedures, \((b)(1); (b)(3); (b)(7)\). FBI Minimization Procedures, Section III.G.4.

B. Legal Analysis

This issue has been the subject of several prior FISC opinions. Specifically, Judge Collyer addressed this issue in ruling on the lawfulness of a change to the FBI's minimization procedures (applicable to FISA electronic surveillance and physical searches, not Section 702 collection) relating to the retention of litigation-related information. She noted: “The Government requests this relief [the changes to the minimization procedures] to eliminate the tension between the destruction requirements contained in the [Special Minimization Procedures] and the obligations to preserve information for litigation in other courts.” In re Standard Minimization Procedures for FBI Electronic Surveillance and Physical search Conducted Under the Foreign Intelligence Surveillance Act, Docket Nos.: Multiple, including \((0)(1); (0)(3); (0)(7)\) at 3. In ruling, the Court found that “the restrictions on access that the Government proposes, along with the reporting requirements . . . strike an appropriate balance between the
competing concerns of not retaining the data longer than necessary and having the Government comply with its litigation obligations.” Id.

Judge Hogan agreed with these conclusions in ruling on the same issues in the context of the 2014 DNI/AG Certifications for the Section 702 program. The Court reasoned:

As with the corresponding provision of the FBI Minimization Procedures, the Court is satisfied that this approach – preservation of particular information as long as there is a litigation need for that information, subject to strict controls on access – strikes a proper balance between the protection of United States person information, on the one hand, and the litigation obligations of the government and fairness to other parties to that litigation, on the other.


The Court's Order approving the 2014 Certifications required the government to submit a written report, on or before December 31 of each calendar year, detailing the information being retained pursuant to these litigation-retention provisions. I requested and have reviewed two reports that the government submitted in 2014 to meet this requirement. The names and other identifying information that would reveal the specific cases at issue were redacted, but the information presented in unredacted form is sufficient for me to confirm that the reports meet the requirements of the Order, and that the reports demonstrate that the amount of information retained for this purpose relates to a relatively small number of matters. In addition, the reports demonstrate that the cases at issue are being monitored so that the destruction requirements can be met once the cases have been resolved so that preserving the relevant information is no longer required.
Both reports were submitted by the National Security Division’s Office of Intelligence.
The first report, dated December 15, 2014, informed the Court that [blacked out].
The second report, dated December 30, 2014, informed the Court that the FBI did not retain any unminimized Section 702-acquired information otherwise subject to destruction.

As noted above, NSA’s minimization procedures were amended to require NSA to provide the information necessary for this report. NSA Minimization Procedures, Section 3(c)(4)a.1. CIA’s minimization procedures were similarly amended. CIA Minimization Procedures, Section 11. The FBI’s minimization procedures were not amended to reflect this obligation, though my understanding is that the FBI is complying with the Court’s Order and the report that I reviewed shows that the FBI did comply. For completeness and in order to ensure compliance, the FBI’s minimization procedures should be amended to incorporate this requirement.

The government has also taken steps to respond to the Court’s suggestion in its 2014 Memorandum and Opinion regarding section 702-acquired information that is subject to destruction requirements other than the “age-off” requirement but may need to be preserved to satisfy litigation preservation obligations. The government’s explanation of those steps is set forth in its Cover Note, at page 22. These changes adequately respond to the Court’s concerns.
and ensure that the Court is duly informed of the circumstances where the government finds that Section 702-acquired information must be preserved for litigation purposes that otherwise conflict with the minimization procedures.

The Court's 2014 Order and the government's submissions pursuant to the Order reflect a reasonable and diligent accommodation of the two competing directives that the government must follow. The government's usual destruction policies for the Section 702-acquired information are in direct conflict with the need to preserve information that is necessary to or potentially discoverable in a relatively small number of criminal, civil, and administrative litigation matters. In the [redacted] for which information is preserved by NSA and CIA, according to the December 15, 2014, report submitted by NSD, [redacted] requires that the information be preserved. The privacy interests that lie behind the destruction requirements are in direct conflict [redacted]. Those privacy interests, while compelling, are general in nature. The litigation preservation requirement, on the other hand, is specific to [redacted]. Moreover, [redacted] (and others that may arise in the future that would similarly require preservation) will eventually be resolved in court, at which point the information being preserved will be subject to destruction pursuant to the normal policies.

In ruling on the 2014 Certifications, the Court recognized the competing interests at stake and therefore issued its August 26, 2014, Order directing the government to file annual reports that set forth what information is being preserved for litigation purposes. Those reports enable
the Court to conduct effective oversight of this requirement and to ensure that the competing interests are properly balanced.

III. Conclusion

With respect to the issue of U.S. person queries of Section 702-acquired information, I conclude that the 2015 Certifications meet the statutory requirements of Section 702, with one exception: the Court should require that the FBI minimization procedures be revised to include safeguards for querying Section 702-acquired information using U.S. person identifiers to ensure that querying is conducted in a manner consistent with the purpose of Section 702 and its statutory requirements.

With respect to the issue of preservation of information for litigation purposes, I conclude that the Court’s Order and the government’s reports reflect a proper balance of the competing requirements to destroy information pursuant to the applicable minimization procedures and to preserve information necessary for litigation purposes. I recommend that the Court’s Order in response to the 2015 Certificates contain the same annual reporting requirement that was included in the 2014 Order and do not recommend any further steps to address this issue.

Respectfully submitted,

Amy Jeffress
ARNOLD & PORTER LLP
601 Massachusetts Avenue NW
Washington, DC 20001
D.C. Bar No. 449258
(U) GOVERNMENT'S RESPONSE TO THE COURT'S BRIEFING ORDER OF SEPTEMBER 16, 2015

(S//OC/NI)- The United States respectfully submits this response to the Briefing Order of the Foreign Intelligence Surveillance Court ("FISC" or "Court") issued on September 16, 2015, in the above-captioned docket numbers. Specifically, this response addresses whether the following two aspects of the minimization procedures submitted with DNI/AG 702(g) Certifications [REDACTED] (hereinafter the "2015 Reauthorization Certifications") meet the definitions of minimization procedures in sections 101(h) and 301(4) of the Foreign Intelligence Surveillance Act ("FISA" or "the

Classified by: Chief, Operations Section, OJ, NSD, DOJ
Reason: Multiple Sources
Declassify on: 20401016

ACLU 16-CV-8936 (RMB) 00083
Act”), 50 U.S.C. §§ 1801(h) and 1821(4), and are consistent with the Fourth Amendment to the Constitution: (1) "queries of information obtained under section 702, particularly insofar as queries may be designed to return information concerning United States persons," and (2) "preservation for litigation purposes of information otherwise required to be destroyed under the minimization procedures." See In Re DNI/AG 702(g) Briefing Order at 3 (FISA Ct. Sept. 16, 2015). For the reasons discussed in detail below, the government respectfully submits that both of these aspects of the minimization procedures meet the definition of minimization procedures under 50 U.S.C. §§ 1801(h) and 1821(4) and are consistent with the Fourth Amendment to the Constitution of the United States.

I. (U//FOUO) The Provisions of the Proposed Minimization Procedures Regarding Queries Designed to Return Information, Including Concerning United States Persons, Obtained Under Section 702 Are Consistent With the Act and the Fourth Amendment

(U//OC//NF) Communications acquired pursuant to section 702 of the Act, 50 U.S.C. § 1881a, are subject to both targeting procedures and minimization procedures intended to ensure that agencies target non-United States persons reasonably believed to be located outside the United States who are assessed to communicate or possess foreign intelligence information. Once these communications are acquired, authorized
intelligence professionals at the National Security Agency ("NSA"), Federal Bureau of Investigation ("FBI"), and Central Intelligence Agency ("CIA") are permitted to review them in order to assess whether they may be retained or disseminated.\(^1\) This review can be accomplished either on a communication-by-communication basis or by tailored querying of the acquired communications. Such queries promote both efficiency and privacy. By using queries, personnel can more quickly identify communications of interest – i.e., those that contain foreign intelligence information – while filtering out communications that may contain private information that are unlikely to contain the desired foreign intelligence information. Stated differently, tailored queries of section 702-acquired communications reasonably designed to return foreign intelligence information or, in the case of the FBI, evidence of a crime, regardless of whether such queries are designed to return United States person information, are simply a way for

\(^1\) See, e.g., DNI/AG 702(g) Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended, Ex. B at 3-4, § 3(b)(1) (filed July 28, 2014) ("2014 NSA Minimization Procedures") (recognizing that analysts may review communications, including those containing United States person information, that are "clearly not relevant to the authorized purpose of the acquisition"). As the Court is aware, NSA’s upstream Internet collection pursuant to section 702 can acquire multi-communication transactions (MCTs), which can include discrete communications that are not to, from, or about a tasked selector. For this reason, NSA’s minimization procedures provide additional access and handling restrictions for certain MCTs. Notably, however, United States person queries are not permitted to be conducted in NSA’s upstream Internet collection, see 2015 Reauthorization Certifications, Ex. B at 7, meaning that any United States person information in such MCTs will not be returned based on a query of NSA’s upstream Internet collection using United States person identifiers.
intelligence professionals to more efficiently focus on particular communications from a larger set of lawfully acquired communications that they are already authorized to review under Court-approved minimization procedures. Tailored queries using United States person identifiers as selection terms further assist in ensuring that communications that contain United States person information are not unnecessarily or indiscriminately reviewed.

The current NSA and CIA minimization procedures applicable to information collected pursuant to section 702 permit tailored queries of such information using United States person identifiers as selection terms where there is a reasonable basis to expect the query to return foreign intelligence information. See, e.g., 2014 NSA Minimization Procedures at 6-7; DNI/AG 702(g) Minimization Procedures Used by the Central Intelligence Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended, Ex. E at 3 (filed July 28, 2014) (“2014 CIA Minimization Procedures”). The current FBI minimization procedures applicable to section 702 information permit tailored queries using United States person identifiers where there is a reasonable basis to expect the query to return foreign intelligence information or evidence of a crime. See, e.g., DNI/AG 702(g) Minimization Procedures Used by the Federal Bureau of Investigation in Connection With Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, Ex. E at 3 (filed July 28, 2014).

(S//OC/NF) In the proposed minimization procedures submitted to the Court with the 2015 Reauthorization Certifications, the government has made several changes to provisions of the NSA, FBI, and CIA minimization procedures regarding United States person queries. None of the changes to the 2015 procedures expand the agencies’ authorities; each of these changes incorporates existing practices or policy restrictions, or clarifies or enhances existing practices designed to ensure queries are limited to authorized and appropriate purposes. These changes were made in response to policy recommendations of the Privacy and Civil Liberties Oversight Board ("PCLOB") concerning the government’s use of United States person identifiers to conduct tailored queries of section 702-acquired communications. The PCLOB did not find the government’s query practices inconsistent with the Act or the Fourth Amendment, but made several policy recommendations to ensure the proper balance of privacy and national security. See, e.g., PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act at 9, 137-139 (July 2, 2014).
("PCLOB 702 Report").\(^2\) As explained in the 2015 Reauthorization Certifications Cover Filing (which is incorporated herein by reference), and as discussed below, these changes clarify obligations that the current minimization procedures already impose, incorporate existing practices or policy restrictions into the procedures, or enhance protections. As such, the government believes that these enhancements to the query

\(^1\)\(^{(S//NF)}\) After conducting an in-depth review of the section 702 program, including evaluating whether the program complies with the statutory and constitutional requirements, the Board "recognize[d] the considerable value that the section 702 program provides in the government's efforts to combat terrorism and gather foreign intelligence." \(\text{Id. at 134.}\) The PCLOB concluded that, "at its core, the program is sound," PCLOB 702 Report at 134, and did not find that the use of United States person queries was inconsistent with the requirements of the Act or the Fourth Amendment. In doing so, however, the Board acknowledged that "certain aspects of the Section 702 program push the program close to the line of constitutional reasonableness," including "the use of queries to search for the communications of specific U.S. persons within the information that has been collected" \(\text{Id. at 9.}\) The PCLOB report accordingly included a number of policy recommendations related to United States person queries, and the government has addressed those recommendations in the proposed NSA, FBI, and CIA minimization procedures currently pending with the Court. \(\text{See 2015 Reauthorization Certifications, Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications at 7-9, 20 (filed July 15, 2015)}\) ("2015 Reauthorization Certifications Cover Filing").

(U) Chairman Medine and Board Member Ward issued a separate statement regarding United States person queries, recommending that the section 702 minimization procedures require that (1) "Americans' communications . . . be purged of information that does not meet the statutory definition of foreign intelligence information relating to Americans" at the time that the results of a United States person query are generated; and (2) the Court approve each United States person identifier to be used to query data collected pursuant to section 702 prior to a query being conducted. PCLOB 702 Report at 151-152 (annex A). As discussed in a separate statement issued by Board Members Brand and Collins Cook, the Board as a whole rejected those suggestions as unworkable and potentially exacerbating civil liberty concerns. \(\text{Id. at 161-165 (annex B).}\)
provisions further contribute to the reasonableness of those provisions and of the minimization procedures overall.

A. (U) The Proposed Query Provisions Are Consistent With the Act

1. (U) Background

(S//NF) The government’s querying, including with the use of United States person identifiers, of lawfully acquired section 702 collection to identify foreign intelligence information or, in the case of the FBI, evidence of a crime is entirely consistent with the requirements of the Act. Nothing in the Act or its legislative history prohibits the government from performing queries of FISA-acquired information using United States person identifiers; to the contrary, as explained below, the legislative history suggests that appropriate controls on retrieving data were a form of minimization contemplated by Congress. Minimization procedures, including those with similar query provisions to those in the procedures submitted with the 2015 Reauthorization Certification, have been previously approved by this Court. The modifications the government has now proposed, as described in more detail below, continue to place limitations on how and when queries using United States person identifiers can be performed, limitations that satisfy the statutory definition of minimization procedures.

(S//NF) As an initial matter, section 702 acquisition is a focused collection that targets non-United States persons located outside the United States for the purpose of...
collecting foreign intelligence information. United States persons may not be targeted under this program, and, as the Court has previously acknowledged, "[i]t is reasonable to presume that most persons in communication with a non-U.S. person target located overseas are themselves likely to be non-U.S. persons located overseas." *In re DNI/AG Certification* Mem. Op. at 38 n.44 (FISA Ct. Sept. 4, 2008) ("2008-A Mem. Op."). Moreover, the techniques used for section 702 collection do not constitute bulk collection. See 2014 Mem. Op. at 26 ("acquisitions are not conducted in a bulk or indiscriminate manner"); *ibid* Mem. Op. at 8; see also PCLOB 702 Report at 103 (noting that the section 702 program "consists entirely of targeting individual persons and acquiring communications associated with those persons," and "does not operate by collecting communications in bulk"). Instead, section 702 acquisition is "effected through thousands of discrete targeting decisions for individual facilities." 2014 Mem. Op. at 26. These facilities are tasked to acquire communications from telephony providers, by or with the assistance of the FBI from, or through NSA’s upstream Internet collection.³ See, e.g., *In re DNI/AG 702 Certification*.

³ "NSA’s acquisition of Internet communications through its upstream collection under Section 702 is accomplished by acquiring Internet ‘transactions,’ which may contain a single, discrete communication, or multiple discrete communications, including communications that are neither to, from, nor about targeted facilities." *In Re DNI/AG 702 Certifications*.

(U) Although the purpose of section 702 acquisition is not to acquire United States person communications, there has always been a recognition that the incidental collection of such communications was an expected result of the acquisition. As Senator Chambliss specifically noted in supporting section 702’s reauthorization, when Congress first passed section 702, “Congress also understood that this incidental collection would likely provide the crucial lead information necessary to thwart terrorists like the 9/11 hijackers who trained and launched their attacks from within the United States.” 158 Cong. Rec. S8413 (daily ed. Dec. 27, 2012) (statement of Sen. Chambliss). The PCLOB reached a similar conclusion, noting that “[t]he incidental collection of communications between a U.S. person and a non-U.S. person located outside the United States, as well as communications of non-U.S. persons outside the United States that may contain information about U.S. persons, was clearly contemplated by Congress at the time of drafting” section 702. PCLOB 702 Report at 82–83. Moreover, the PCLOB noted that “one of the purposes of the program is to

discover communications between a target overseas and a person in the United States,"
which can be particularly important in identifying and disrupting terrorist plots against
the homeland. *Id.* at 114–115.

2. (U) **Legal Analysis**

*(S//OE/NF)* Section 702 requires the adoption of minimization procedures that
comply with the definitions of such procedures in Titles I and III of the Act. *See* 50
U.S.C. § 1881a(e)(1) (requiring the Attorney General to adopt minimization procedures
that meet the definition of minimization procedures under 50 U.S.C. §§ 1801(h) or
1821(4), as appropriate). This Court has found that the 2014 NSA, FBI, and CIA
Minimization Procedures “comport with the definition of minimization procedures at
Section 1801(h).” *See* 2014 Mem. Op. at 26. The portions of subsections 1801(h) and
1821(4) applicable to queries using United States person identifiers are as follows:^4

(1) specific procedures, which shall be adopted by the Attorney General
that are reasonably designed in light of the purpose and technique of the
particular surveillance [or physical search], to minimize the acquisition

---

^4 (U) Subsections 1801(h)(4) and 1821(4)(D), which address surveillances or searches conducted
pursuant to other parts of the Act, respectively, are not at issue with respect to United States
person queries of section 702-acquired information. While perhaps not directly at issue,
subsections 1801(h)(2) and 1821(4)(B), which require that each agency’s minimization
procedures restrict the dissemination of certain United States person information, would
preclude the dissemination of United States person query results which did not constitute
foreign intelligence information as defined by subsection 1801(e)(1) unless it was first
determined that such information was necessary to understand foreign intelligence information
or assess its importance, thus providing an additional layer of protection with respect to United
States person information obtained from such queries.
and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

*   *   *

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes[.]

50 U.S.C. § 1801(h)(1) & (3) (bracketed text from 1821(4)(A)). The United States person query provisions in the current and proposed NSA, FBI, and CIA section 702 minimization procedures meet the definition of minimization procedures, as specified in both of the above subsections.

(S//NF) In particular, the United States person query provisions “are reasonably designed in light of the purpose and technique” of section 702 acquisition “to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.”

50 U.S.C. §§ 1801(h)(1), 1821(4)(A). As described above, both the purpose (targeting non-United States persons located outside the United States to acquire foreign intelligence information) and the technique (tasking specific, individual selectors at telephony and Internet providers to acquire communications to, from, or about those tasked selectors) are designed to limit the acquisition of non-publicly available
information concerning United States persons that would not be foreign intelligence information. See Mem. Op. at 23 ("The targeting of communications pursuant to Section 702 is designed in a manner that diminishes the likelihood that U.S. person information will be obtained").

(U) In light of this purpose and technique of the section 702 acquisition, the government respectfully submits that the restrictions placed on the retrieval of incidentally acquired United States person information by the NSA, FBI, and CIA, and the oversight requirements imposed on those restrictions, are reasonably designed to properly ensure the minimization of "nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. §§ 1801(h)(1), 1821(4)(A). In particular, FISA's legislative history suggests that Congress recognized that "provisions with respect to . . . what [information] may be retrieved and on what basis" can be one of the "means and techniques which the minimization procedures may require to achieve the purpose set out in the definition." H.R. Rep. No. 95-1283, pt. 1, at 56 (1978). The provisions at issue here restrict queries using United States person identifiers, permitting such queries only if there is a reasonable basis to expect the query is likely to return foreign intelligence information or, in case of the FBI, evidence of a crime. Queries for purposes other than identifying foreign intelligence
information or evidence of a crime -- for example for political, personal, or financial
interests -- are prohibited.

(U) A tailored query conducted under a reasonable expectation that it would be
likely to return foreign intelligence information plainly would be “consistent with the
need of the United States to obtain, produce, and disseminate foreign intelligence
information.” 50 U.S.C. §§ 1801(h)(1), 1821(4)(A). Specifically, the ability to use specific
query terms to more efficiently and effectively identify foreign intelligence information
contained in section 702-acquired information – including, for instance, to learn about
the activities of a United States person terrorist suspect, to help identify a United States
person in contact with a foreign intelligence officer, or to search for communications
concerning a United States person who is the planned victim of an assassination or
kidnapping plot – is a critical tool to ensure that the United States can timely “obtain,
produce, and disseminate foreign intelligence information.” Id. The requirement that
query selection terms be reasonably likely to return foreign intelligence information
minimizes the likelihood that information unrelated to those foreign intelligence needs
would be returned.
Likewise, a query by the FBI that is reasonably expected to return evidence of a crime\(^5\) is also consistent with a statutory scheme that expressly contemplates the retention and dissemination of non-foreign intelligence information that is evidence of a crime. See 50 U.S.C. § 1801(h)(3); see generally In re Sealed Case, 310 F.3d 717, 731 (FISA Ct. Rev. 2002) (noting that Title I minimization procedures allow “the retention and dissemination of non-foreign intelligence information which is evidence of ordinary crimes for preventive or prosecutorial purposes”); H.R. Rep. No. 95-1283, pt. 1, at 62 (noting that section 101(h)(3) “applies to evidence of crimes which otherwise would have to be minimized because it was not needed to obtain, produce, or disseminate foreign intelligence information”). Given that the FBI is a law enforcement agency as well as a member of the Intelligence Community, the ability to query for evidence of a crime using United States person identifiers can help the FBI pursue important leads regarding criminal activity. Such queries may be important not only to aid foreign intelligence-related criminal investigations (including regarding espionage, state-sponsored cyber attacks, and material support for terrorism), but also in other criminal cases, such as to help locate a kidnapper, monitor human trafficking, or identify distributors of child pornography. See, e.g., 2015 Reauthorization Certifications, 2015 Reauthorization Certifications, Ex. D at 11.

---

\(^5\) As noted above, only the FBI’s section 702 minimization procedures allow for using United States person query terms to identify information that is evidence of a crime. See, e.g., 2015 Reauthorization Certifications, Ex. D at 11.
Ex. D at 31-32 (allowing the FBI to disseminate child exploitation material, including child pornography, to the National Center for Missing and Exploited Children).

-(S) Regarding each of these types of queries, the PCLOB found that “rules and oversight mechanisms are in place to prevent U.S. person queries from being abused for reasons other than searching for foreign intelligence or, in the FBI’s case, for evidence of a crime.” PCLOB 702 Report at 131. And since the PCLOB’s 2014 report, additional restrictions regarding the querying and use of information for non-foreign intelligence purposes have been imposed or are included in the FBI’s 2015 minimization procedures. The proposed FBI minimization procedures include a new requirement

See 2015 Reauthorization Certifications, Ex. D at 12 n.4.

-(S//O|C|//N|F) The oversight mechanisms referenced by the PCLOB report include the requirement in the NSA, FBI, and CIA minimization procedures that the Department of Justice’s National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) conduct oversight of each agencies’ United States
person queries. This required oversight helps to ensure that each agency is conducting queries designed to “achieve the purpose set out in the [minimization procedures] definition.” H.R. Rep. No. 95-1283, pt. 1, at 56.

(U) Finally, Congress was aware of, and approved, the government’s use of United States person identifiers as selection terms for content queries. In reauthorizing section 702 in 2012, Congress was aware of the ongoing incidental collection of communications of or concerning United States persons under section 702 authority and expressed not only its acceptance of such incidental acquisitions, but also of the use of tailored queries using identifiers of United States persons as selection terms to specifically select those communications. For example, the Senate Select Committee on Intelligence, and then the Senate as a whole, rejected two amendments intended to prohibit the government from querying the contents of communications acquired under section 702 to find communications of particular United States persons. See Sen. Rep. No. 112-229 at 10 & 15 (2012); cf. Grayson v. Wickes Corp., 607 F. 2d 1194, 1196 (7th Cir. 1979) (considering the fact that the Senate had “considered and rejected an amendment

---

(U//FOUO) Each set of minimization procedures requires the NSD and ODNI to conduct oversight of each agencies’ queries using United States person identifiers, although the nature of the documentation related to such queries varies in conjunction with the different missions and system capabilities of each agency. Compare 2015 Reauthorization Certifications, Ex. B at 7 and Ex. E at 3, with id., Ex. D at 11-12. To facilitate this oversight all agencies are required to keep records of the query terms used to conduct United States person queries of content.
that would have permitted the parties to a Title VII [of the Civil Rights Act] action to demand a trial by jury” as further evidence that jury trials are not required in such actions). More recently, in passing the USA FREEDOM Act, Congress amended the Act to require the government to publicly report metrics related to its United States person queries, see USA FREEDOM Act, Pub. L. 114-23, § 603(b)(2), 129 Stat. 268, 292 (2015), making clear that Congress understands that the government queries section 702-acquired data using United States person identifiers, while also not amending the statute to prohibit such a practice.

Likewise, this Court has previously approved section 702 minimization procedures that permit the government to query section 702-acquired information using United States person identifiers, including as recently as the section 702 certifications submitted and approved last year. See 2014 Mem. Op. at 41; 2014 NSA Minimization Procedures at 6-7; 2014 FBI Minimization Procedures at 11; and 2014 CIA Minimization Procedures at 3. In prior docket, this Court has specifically relied on the longstanding authority under FBI’s standard minimization procedures to query Titles I and III FISA information using United States person identifiers in approving the comparable authority with respect to section 702-acquired information. See In Re DNI/AG 702 Certifications, Mem. Op. at 23-24 (FISA Ct. Oct. 3,
2011) ("2011 Mem. Op."). Specifically, in an opinion concerning the section 702
Certifications submitted to the FISC in 2011, Judge Bates explained that:

[In granting] of applications for electronic surveillance or physical search since 2008, including applications targeting U.S. persons and persons in the United States, the Court has found that the meet the definitions of minimization procedures. . . . It follows that the substantially-similar querying provision found at Section 3(b)(5) of the amended NSA minimization procedures [for section 702 information] should not be problematic in a collection that is focused on non-United States persons located outside the United States and that, in the aggregate, is less likely to result in the acquisition of nonpublic information regarding non-consenting United States persons.

_Id; see also_ Mem. Op. at 23 (noting that although the "targeting of communications pursuant to section 702 is designed in a manner that diminishes the likelihood that U.S. person information will be obtained," the "protection to U.S. persons afforded by the proposed minimization procedures nearly replicates the protection afforded such persons in cases involving search or surveillance intentionally targeting U.S. persons").

--(S) Accordingly, for the reasons explained above, the government submits that the United States person query provisions in the minimization procedures submitted with the 2015 Reauthorization Certifications meet the definitions of minimization procedures in sections 101(h) and 301(4) of the Act.
B. (U) The Proposed Query Provisions Are Consistent With the Fourth Amendment

(S//ORCON/NOFORN) This Court has found that the NSA’s, CIA’s, and FBI’s current section 702 minimization procedures are consistent with the requirements of the Fourth Amendment. See 2014 Mem. Op. at 40. The above-described enhancements to the query provisions proposed by the government provide protections in addition to those that were already found to satisfy the Fourth Amendment. The fact that information is collected under section 702 without a warrant or a finding of probable cause does not undercut the Court’s conclusion as to the reasonableness of the program or the permissibility of subsequent United States person queries conducted pursuant to the Court-approved procedures.

(S//NF) No warrant or probable cause is required for collection under section 702 because it targets non-United States persons reasonably believed to be located outside the United States, who generally do not have Fourth Amendment rights, for foreign intelligence purposes. See, e.g., United States v. Verdugo-Urquidez, 494 U.S. 259, 265 (1990); 2014 Mem. Op. at 39. For any rights that United States persons may have in communications in the possession of targets of section 702 acquisitions, any

---

7(S) The Court has also previously concluded that to the extent that the Warrant Clause of the Fourth Amendment might otherwise apply, section 702 acquisitions would fall within the foreign intelligence exception to the warrant requirement. See 2014 Mem. Op. at 38 (citing Mem. Op. at 34-36).
governmental action implicating those rights must comport with the Fourth Amendment's reasonableness requirement. The Fourth Amendment does not require a "one-size-fits-all" approach to protecting the rights of United States persons before the government can look at or use lawfully acquired information. Instead, the Fourth Amendment requires that the government's actions be viewed in their totality. See In re Directives Pursuant to Section 105B of the Foreign Intel. Surv. Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008) (citation omitted) (hereinafter "In re Directives"). "This mode of approach takes into account the nature of the government intrusion and how the intrusion is implemented. The more important the government interest, the greater the intrusion that may be constitutionally tolerated." Id. (internal citations omitted); see also Maryland v. King, 133 S. Ct. 1958, 1970 (2013) (describing reasonableness balancing test in which courts "weigh the promotion of legitimate governmental interests against the degree to which the search intrudes upon an individual's privacy" (internal quotation marks and brackets omitted)).

(U) Nothing in the Fourth Amendment or governing precedent imposes an additional requirement or limitation beyond the reasonableness inquiry. In particular, nothing in the Fourth Amendment requires that queries of lawfully collected information using United States person identifiers must be subject to separate, independent judicial process involving, for example, a warrant or showing of probable cause. In the only district court case to consider Section 702 queries using United States
person identifiers, the District of Oregon concluded that "subsequent querying of a
[section] 702 collection, even if U.S. person identifiers are used, is not a separate search
and does not make [section] 702 surveillance unreasonable under the Fourth
Amendment." United States v. Mohamud, 2014 WL 2866749, at *24 (D. Or. June 24,
2014). For example, courts have held in the context of DNA databases that the
government’s querying of information that has already lawfully been obtained does not
implicate any reasonable expectation of privacy beyond that implicated in the initial
collection. See, e.g., Boroian v. Mueller, 616 F.3d 60, 67-68 (1st Cir. 2010) ("[T]he
government’s retention and matching of [an individual’s] profile against other profiles
in [a DNA database] does not violate an expectation of privacy that society is prepared
to recognize as reasonable, and thus does not constitute a separate search under the
Fourth Amendment."); see also Johnson v. Quander, 440 F.3d 489, 498-99 (D.C. Cir. 2006)
("[A]ccessing the records stored in [a DNA] database is not a ‘search’ for Fourth
Amendment purposes. . . . [I]f a snapshot is taken in conformance with the Fourth
Amendment, the government’s storage and use of it does not give rise to an
independent Fourth Amendment claim."). That is true even where the queries or uses
are not those for which the collection was initially authorized. See, e.g., King, 133 S. Ct.

8 (U) The District Court did acknowledge that querying using a United States person identifier
was "a very close question," but ultimately held that such queries did not entail "any significant
additional intrusion past what must be done to apply minimization procedures." Id.
at 1980 (upholding warrantless collection of DNA for identification of persons arrested for serious offenses and subsequent use of DNA in investigation and prosecution of unrelated, unsolved crimes); *Jabara v. Webster*, 691 F.2d 272, 279 (6th Cir. 1982) (upholding dissemination by NSA of intelligence collected without a warrant for intelligence purposes to FBI for purposes of criminal investigation).

—(S//NF)—Turning to the reasonableness inquiry, as this Court has recognized, "[t]he government's national security interest in conducting [section 702] acquisitions 'is of the highest order of magnitude.'" [37] Mem. Op. at 37 (quoting *In re Directives*, 551 F.3d at 1012); see also 2014 Mem. Op. at 39; cf. *Haig v. Agee*, 453 U.S. 280, 307 (1981) ("It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation." (internal quotation marks omitted)). This vital interest in obtaining timely foreign intelligence information must be balanced against any legitimate privacy interests of United States persons whose communications may be incidentally collected and subsequently queried because they are in contact with non-United States person targets abroad.

(U) In some contexts, the rules the government adopts with respect to review of United States person communications can be relevant to the reasonableness of the collection program under the Fourth Amendment. For example, the Foreign Intelligence Surveillance Court of Review analyzed such rules in concluding that the Protect America Act (PAA), the predecessor to section 702, was constitutionally
reasonable. See In re Directives, 551 F.3d at 1015 (finding it “significant,” in upholding the PAA, that “effective minimization procedures are in place” to “serve as an additional backstop against identification errors as well as a means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons”).

(U) The government respectfully asserts that the privacy interests implicated by queries using United States person identifiers are properly accounted for by the minimization procedures. As discussed above, consistent with applicable FISC-approved minimization procedures, the government is permitted to review the information it lawfully collects under section 702 – which includes information concerning United States persons – to assess whether the information should be retained or disseminated. Accordingly, United States person information is, by necessity, already subject to review (and use) under the Court-approved minimization procedures. The government respectfully submits that it would be an incongruous result to authorize the communication-by-communication review of lawfully collected information but then to restrict the more focused review of the same information in response to tailored queries designed to return foreign intelligence information or, in the case of the FBI only, evidence of a crime.

(S//OC/NF) Moreover, section 702 requires the government to use both targeting and minimization procedures, approved in advance by this Court, to protect the privacy interests of United States persons. As a result of these procedures, United

---
States person queries are authorized only for section 702 data that is collected through the use of specific selectors, chosen in conformity with the targeting procedures, and that is acquired through NSA’s telephony collection or Internet communications acquired by or with the assistance of the FBI from [b](1); [b](3); [b](7)(E). The NSA and FBI targeting procedures are reasonably designed to ensure that only non-United States persons reasonably believed to be located overseas are targeted, and only when there are reasonable grounds to believe that those persons possess or are likely to possess, receive or communicate foreign intelligence within the scope of the approved certifications. 50 U.S.C. § 1881a(b), (d)(1) & (f)(1)(A). See also Mem. Op. at 39 n.47 ("It is fairly obvious why communications to and from targets identified under these [targeting] procedures would be expected to contain foreign intelligence information."). Such targeting procedures “direct the government’s acquisitions toward communications that are likely to yield the foreign intelligence information sought, and thereby afford a degree of particularity that is reasonable under the Fourth Amendment.” Id. at 39-40.

In addition to the targeting procedures, the ability to query using United States person identifiers for foreign intelligence information or evidence of a

\[\text{(S//NFO\textregistered)}\]  As stated above, United States person identifiers may not be used as query terms for communications collected under NSA’s upstream Internet collection techniques. See 2015 Reauthorization Certifications, Ex. B at 7.
crime must be viewed in the context of the many other protections found within the minimization procedures. These restrictions limit both who has the ability to query any data and what may be done with the results of any queries. For example, the proposed CIA minimization procedures require that CIA personnel “specifically agree to: comply with these [section 702] minimization procedures; comply with all CIA direction on the handling of information acquired under section 702; and not make any use of, share, or otherwise disseminate any information acquired pursuant to section 702 without specific CIA approval.” See 2015 Reauthorization Certifications, Ex. E at 1. Likewise, the proposed NSA and FBI section 702 minimization procedures contain similar restrictions on the personnel who may access section 702-acquired information. See, e.g., 2015 Reauthorization Certifications, Ex. B at 1, 4 & Ex. D at 6-8. Moreover, the proposed NSA, FBI, and CIA procedures permit dissemination of non-publicly available and personally identifying information concerning United States persons only under prescribed circumstances, to include when the information constitutes foreign intelligence information or is necessary to understand foreign intelligence information. Id. Ex. B at 14-15; Ex. D at 30-31; Ex. E at 4. In other words, the proposed procedures by design aim to ensure that any intrusion on any privacy interests of United States persons is reasonably balanced against the government’s foreign intelligence needs.

(S/NC) In light of the limitations imposed by the section 702 targeting and minimization procedures, the government’s authority to query section 702-acquired
information using United States person identifiers raises no additional Fourth Amendment issue. Indeed, this Court has repeatedly found that the section 702 targeting and minimization procedures satisfy any Fourth Amendment concerns resulting from the incidental collection of United States person communications. See, e.g., 2014 Mem. Op. at 39-40. This programmatic judicial review, in the context of targeting non-United States persons overseas for foreign intelligence purposes, is itself an important factor in assessing the reasonableness of the statutory scheme and its implementation for Fourth Amendment purposes, including the use of United States person queries. See In re Directives, 551 F.3d at 1012-13 (noting that prior judicial approval, though not indispensable, is among the factors relevant to assessing Fourth Amendment reasonableness). Although the proposed procedures submitted with the 2015 Reauthorization Certifications amend those provisions of the NSA, FBI, and CIA minimization procedures regarding United States person queries of section 702 information, they do not expand the agencies’ ability to conduct such queries, but instead incorporate existing practices into the proposed procedures. See 2015 Reauthorization Certifications Cover Filing at 7-10, 20-21. By incorporating these practices into the procedures, the procedures are more, not less, protective of privacy.
II. (U//FOUO) The Provisions of the Proposed Minimization Procedures Regarding the Preservation of Information For Litigation Purposes Otherwise Subject to Destruction Requirements Are Consistent With the Act and the Fourth Amendment

(S(/OC/NF) The current FBI, NSA, and CIA section 702 minimization procedures permit the retention of information for litigation-related reasons when that information would otherwise be subject to destruction under other provisions of the applicable minimization procedures. Specifically, the current FBI minimization procedures permit the FBI to retain information otherwise subject to destruction under its retention schedule if “the FBI and NSD determine that such information is reasonably believed to be necessary for, or potentially discoverable in, administrative, civil, or criminal litigation.” 2014 FBI Minimization Procedures at 21-22. The current NSA and CIA minimization procedures also contain provisions that allow those agencies to retain information for litigation purposes if advised by the Department of Justice, notwithstanding certain destruction requirements that might otherwise apply. See 2014 NSA Minimization Procedures at 8; 2014 CIA Minimization Procedures at 9.

A. (U) Summary of Procedural Changes

(S(/OC/NF) In its 2014 Memorandum Opinion, this Court approved the litigation-related provisions in the 2014 NSA, FBI, and CIA minimization procedures. See 2014 Mem. Op. at 41. Additionally, the Court suggested that these provisions in the NSA and CIA minimization procedures be further expanded to account for
circumstances where section 702-acquired information is subject to a destruction
requirement other than age-off and may need to be preserved to satisfy the
government’s preservation obligations without requiring the government to seek relief
from the minimization procedures from this Court. See 2014 Mem. Op. at 23-24.
Specifically, the Court found that “preservation of particular information as long as
there is a litigation need for that information, subject to strict controls on access – strikes
a proper balance between the protection of United States person information, on the one
hand, and the litigation obligations of the government and fairness to other parties to
that litigation, on the other.” Id. at 23. Moreover, the Court encouraged the
government, in the interests of “efficiency and consistency . . . to consider further
revision of these procedures to address such situations with generally applicable rules,
rather than on a piecemeal basis.” Id. at 24.10

In the proposed NSA and CIA minimization procedures submitted
to the Court with the 2015 Reauthorization Certifications, the government has made
changes to provisions of those procedures consistent with the Court’s interest in more
“generally applicable rules.” The government has modified the language in the
proposed NSA and CIA minimization procedures to permit the retention of specific

10 The Court expressed a similar sentiment during oral arguments regarding the
2014 section 702 reauthorization certifications. See In Re DNI/AG 702 Certifications,
section 702-acquired information otherwise subject to age-off or certain other
destruction requirements if the Department of Justice advises the relevant agency in
writing that such information is subject to a preservation obligation in pending or
anticipated administrative, civil, or criminal litigation. See 2015 Reauthorization
Certifications, Ex. B at 8-9, Ex. E at 10-11. Importantly, information retained for such
litigation-related purposes may not be used for analytical purposes:

2015 Reauthorization Certifications, Ex. B

at 8; see also 2015 Reauthorization Certifications, Ex. D at 24-25, Ex. E at 10-11.

Moreover, by only allowing the NSA, FBI, and CIA to preserve specific information
otherwise subject to destruction under the minimization procedures upon a written
finding by the Department of Justice that the information needs to be preserved, the
government ensures that these materials are only being preserved when “there is a
litigation need for that information.” 2014 Mem. Op. at 23.

(S//NF) Although the proposed procedures allow the NSA and CIA at the
direction of the Department of Justice to retain information subject to a broader range of
destruction requirements to satisfy the government’s preservation obligations, those
agencies’ procedures do not allow the NSA and CIA to retain, without the Court’s
permission, information that may be subject to destruction requirements that are not
specified in the minimization procedures (for instance, as applicable to unauthorized
collection, such as the unintentional tasking of a selector to section 702 acquisition
causd by a typographical error in the targeting process). See 2015 Reauthorization
Certifications, Ex. B at 8-9, Ex. E at 10-11. When information is subject to a destruction
requirement other than those contained in the minimization procedures the relevant
provisions in the NSA's and CIA's proposed minimization procedures specify when
and how the Department of Justice will notify and request authorization from this
Court to continue to retain section 702-acquired information as appropriate and
consistent with law. Id. NSA, FBI, and CIA must promptly destroy the information, as
required, after the Department of Justice notifies the agencies in writing that retention is
no longer necessary for litigation-related purposes. See 2015 Reauthorization
Certifications, Ex. B at 8-9; Ex. D at 25; Ex. E at 10-11.

11(6) Although not all communications that might be acquired from such targeting are
explicitly addressed in NSA's or CIA's minimization procedures, NSA's targeting procedures
require that any information collected from the intentional targeting of a United States person
or person not reasonably believed to be located outside the United States at the time of targeting
must be purged from NSA databases. See 2015 Reauthorization Certifications, Ex. A at 9.
Moreover, the government purges any collection from such targeting from government analytic
databases in order to prevent the use of such information in non-conformance with 50 U.S.C.
§ 1809.
In its 2014 Memorandum Opinion, the Court also ordered the government to submit an annual report identifying matters in which the agencies were retaining information otherwise subject to the age-off requirement specified in the NSA, FBI, and CIA minimization procedures. 2014 Mem. Op. at 42. Under the proposed minimization procedures currently subject to review by the Court, NSA and CIA are obligated to annually provide NSD a summary of all litigation matters requiring preservation of section 702-acquired information that would otherwise be subject to destruction, a description of the section 702-acquired information being preserved for each such litigation matter, and if possible, the status of each such litigation matter. See 2015 Reauthorization Certifications, Ex. B at 8-9, Ex. E at 10-11.¹²

B. (U) Legal Analysis

The current and proposed provisions allowing for the retention of section 702-acquired information for litigation purposes are intended to prevent prejudice to civil litigants and to protect the rights of criminal defendants while continuing to satisfy the government’s obligations under the Fourth Amendment as well as limiting the retention of and access to non-publicly available United States person data as required by FISA.

¹² (U) The FBI also provides similar information to NSD.
(U) The duty to preserve information in non-criminal litigation generally arises from the common-law duty to take reasonable steps to avoid spoliation of relevant evidence for use at trial; the inherent powers of the courts; and court rules governing the imposition of sanctions. See, e.g., Silvestri v. Gen. Motors, 271 F.3d 583, 590-91 (4th Cir. 2001); Convolve, Inc. v. Compaq Computer Corp., 223 F.R.D. 162, 176-77 (S.D.N.Y 2004). Depending on the facts of each case, once the duty to preserve takes effect, the preserving party may be required to suspend existing policies related to deleting or destroying files and preserve relevant documents related to the litigation. The government recognizes that the common law obligation to preserve information for non-criminal matters in most cases cannot take precedence over the government’s obligations to comply with the Fourth Amendment or FISA statutory requirements.\(^\text{13}\)\(^\text{(S)}\)

\(^{13}\text{(S)}\) As this Court has recognized in a different context, the need to balance the requirements of FISA minimization procedures with the needs of civil litigants is very fact specific. For example, such requirements applicable to information entitled to minimal privacy protections can be outweighed by the needs of a litigant challenging the lawfulness of that collection. On March 7, 2014, the Court issued an order denying, without prejudice, a government motion to amend the Primary Order issued in docket number BR14-01 which sought to authorize the preservation and/or storage of bulk call detail records or “telephony metadata” beyond five years after its initial collection in order to satisfy the government’s common law obligations to preserve potentially relevant evidence for civil litigation-related purposes. In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, Docket No. BR14-01 (FISA Ct. Mar. 7, 2014). Among other things, the Court found that in the absence of any documented interest on the part of the civil plaintiffs to preserve information, or a court order compelling it, the government’s general common law obligation to preserve potentially relevant evidence did not in that matter supersede its obligation to destroy the voluminous non-targeted set of records at issue under the applicable provisions of FISC orders. Id. Following
See In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, Docket No. BR14-01, Mem. Op. at 3-4 (FISA Ct. Mar. 7, 2014) (concluding that because the obligation to preserve relevant records in civil litigation "is a matter of federal common law . . . it may be displaced by statute whenever Congress speaks directly to the issue," referencing retention restrictions statutorily derived from 50 U.S.C. § 1861(c), (g)); 50 U.S.C. § 1881a(b), (e)). The proposed minimization procedures reflect the need for a fact-specific balancing of these constitutional and FISA statutory requirements on one side with a party’s common law and rule-based interests on the other by only allowing the agencies to preserve data at the direction of the Department of Justice upon a finding that there is a preservation obligation.

(U) Unlike in civil matters, certain preservation and discovery obligations in criminal matters are constitutional requirements that in some cases may require the government to balance the Fifth Amendment due process rights of one defendant

the issuance of a preservation order, the Court subsequently issued an order granting the government’s motion for temporary relief from the Primary Order’s destruction requirement. See In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, Docket No. BR14-01 (FISA Ct. Mar. 12, 2014). As noted above, these decisions were made in a different context, and the government submits that these opinions in docket number BR14-01 are distinguishable from the issue currently before the Court, which involves the preservation of specific targeted acquisitions under section 702, as opposed to the voluminous, non-targeted production of call detail records at issue in the NSA Section 215 bulk telephony metadata program.
against the possible Fourth Amendment privacy rights of another individual. For example, the government is obligated by constitutional and statutory requirements to ensure that criminal defendants are provided with a fair trial and that exculpatory material and impeachment evidence are disclosed, where required.\textsuperscript{14} See \textit{Brady v. Maryland}, 373 U.S. 83, 87 (1963) ("[T]he suppression by the prosecution of evidence favorable to an accused upon request violates due process where the evidence is material to either guilt or punishment, irrespective of the good faith or bad faith of the prosecution."); see also \textit{Giglio v. United States}, 405 U.S. 150 (1972) (extending \textit{Brady} principles to evidence affecting the credibility of government witnesses); 18 U.S.C. § 3500 (Jencks Act) (requiring the government to produce statements of government witnesses to the defense after a witness has testified at trial). The preservation provisions of the proposed FBI, NSA, and CIA section 702 minimization procedures, which reflect each agencies’ unique mission, would allow the government to strike the appropriate balance of what may be competing constitutional rights and statutory

\textsuperscript{14}(S//NF) As noted above, the NSA and CIA practices for helping prosecutors satisfy these constitutional and statutory obligations in criminal matters are different than the FBI’s, in part because NSA and CIA are not law enforcement agencies.
requirements by only allowing the agencies to preserve data at the specific instruction of the Department of Justice.\textsuperscript{15}

\textit{S/NF} In contexts concerning the FBI's retention of non-section 702 FISA-acquired information, this Court has previously recognized the government's need to retain such information for litigation purposes. In an order dated [BLACKED OUT], the Court

\textsuperscript{15} (U//FOUO) This is not to suggest that the United States Intelligence Community (USIC), whose mission includes the performance of intelligence activities necessary for the conduct of foreign relations and the protection of national security, is subject to the same criminal discovery obligations as a law enforcement agency; rather, it recognizes that the Department of Justice may determine that in certain, limited circumstances, information in the USIC's possession may trigger the government's obligations to preserve information related to a criminal prosecution.

(S//NF) Any retention of information to satisfy preservation obligations for litigation purposes must also, however, comply with and be balanced by the statutory requirements regarding nonpublicly available United States person information. As discussed above, 50 U.S.C. § 1881a(g)(2)(A)(ii) requires that a section 702 certification contain minimization procedures that meet the definition of minimization procedures under Title I or Title III of the Act (i.e., 50 U.S.C. §§ 1801(h) and 1821(4)). The proposed NSA, FBI, and CIA section 702 minimization procedures have been carefully crafted to balance the competing concerns of not retaining data longer than permitted by the minimization procedures and allow each agency to comply with any preservation obligations it may have. Specifically, these minimization procedures require
consultation between the relevant agency and the Department of Justice regarding the
initiation (and subsequent removal) of any litigation hold. The proposed changes to the
NSA and CIA minimization procedures also require ongoing consulting with and
reporting to the Department of Justice regarding all administrative, civil, or criminal
litigation matters necessitating preservation of section 702-acquired information
otherwise subject to destruction, a description of the information retained for each such
litigation matter, and, if possible, the current status of the matter. See 2015
Reauthorization Certifications, Ex. B at 8-9, Ex. E at 10-11.

(S//NF) Moreover, the FBI, NSA, and CIA minimization procedures
strictly limit access to information retained for litigation-related purposes to
personnel working on the particular litigation matter, except on a case-by-case
basis after consultation with the Department of Justice. Id.; 2015 Reauthorization
Certifications, Ex. D at 24-25. Although the information has not been destroyed,
there is nothing in the Act that requires destruction as the sole means to
minimize retention of data. Indeed, Congress recognized that placing
restrictions on access to data -- rather than destroying it -- may be sufficient to
meet the minimization procedures definition. H.R. Rep. No. 95-1283, pt. 1, at 56
(1978) (noting that minimizing retention of data should be done by "destruction
where feasible," but that it could also entail "other measures designed to limit
retention," including "provisions with respect to ... what may be retrieved and

TOP SECRET//SI//ORCON//NOFORN
on what basis”) (emphasis added); see also 2011 Mem. Op. at 78-79 (suggesting that the adoption of “more stringent post-acquisition safeguards” may satisfy the reasonableness requirement of the Fourth Amendment). The above-described access restrictions are consistent with Congress’ original understanding of how the government may need to minimize retention of data in circumstances where the destruction of that data is not feasible.

(U) Conclusion

(S//OC/NF) For the foregoing reasons, the government respectfully requests that the Court approve the submitted 2015 Reauthorization Certifications, including the accompanying targeting and minimization procedures, in their entireties. Specifically, the government submits that the two aspects of the FBI, NSA, and CIA proposed section 702 minimization procedures discussed herein -- queries designed to return information concerning United States persons and the preservation for litigation purposes of information otherwise required to be destroyed -- are consistent with both the Act and the Fourth Amendment. Accordingly, the government respectfully requests that this Court enter orders pursuant to subsection 702(i)(3)(A) of the Act approving: DNI/AG 702(g) Certifications [REDACTED] the use of the targeting and minimization procedures attached thereto as Exhibits A, B, C, D, E, and G in connection with acquisitions of foreign intelligence information in accordance with those certifications; and the use of the minimization procedures attached as Exhibits B,
D, and E to DNI/AG Certifications in connection with foreign intelligence information acquired in accordance with DNI/AG 702(g)

Respectfully submitted,

John P. Carlin
Assistant Attorney General

Stuart J. Evans
Deputy Assistant Attorney General

By:

(b)(6); (b)(7)(C)
Deputy Chief, Operations Section

(b)(6); (b)(7)(C)
Unit Chief, Operations Section

(b)(6); (b)(7)(C)
Deputy Unit Chief, Operations Section

(b)(6); (b)(7)(C)
Attorney

Office of Intelligence
National Security Division
U.S. Department of Justice
TOP SECRET//SI//ORCON//NOFORN

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT

IN RE: Washington, D.C.
October 20, 2015
2:01 p.m.

TRANSCRIPT OF PROCEEDINGS
HELD BEFORE THE HONORABLE THOMAS F. HOGAN
FOREIGN INTELLIGENCE SURVEILLANCE COURT

APPEARANCES:

FOR THE DEPARTMENT OF JUSTICE: (b)(6); (b)(7)(C)
STUART J. EVANS, ESQ.

FOR THE AMICUS CURiae:
AMY JEFFRESS, ESQ.

COURT STAFF: (b)(6); (b)(7)(C)

Court Reporter: (b)(6)

Proceedings recorded by mechanical stenography; transcript produced by computer-aided transcription
PROCEDINGS

THE COURT: All right. Good afternoon. We're here on the matter that we had appointed Amicus counsel to look into under the new statute. I want to introduce you to Judge James Parker Jones from the Western District of Virginia, one of our newer FISA judges, who is just attending this ceremony with me and who will probably be kicking me under the table telling me how to behave here.

This matter before the Court is, as I've said on the report, materials received entitled "The Briefs of Amicus Curiae" from the Amicus we appointed here, Ms. Amy Jeffress, whom the Court acknowledges for her excellent work in a very tight time frame in this matter and appreciates the work that she's given to the Court, and to all of us, for this report.

What I want to start with is a couple of things. One is, I'd like to have introduced the parties who are going to be arguing for the Court for the record. And Ms. Jeffress is one, and we've got about 18 others so I'll assume we'll reduce that to one or two on the government's side, and we won't hear from everybody. But also, after that, anyone who may be intending to be a fact witness, if there's questions I want to ask and develop, if they would introduce themselves, if there's any officials here from the relevant agencies. I think the Court -- counsel for the
Court have at least advised the Court -- the government that my interest, and I believe to -- first of all, my interest really is to the issues she's raised as to the inquiry into the 702 materials by the FBI on evidence of crimes.

The second inquiry that she had -- the first was as to the aspects that we found were appropriate under the new law, I'd call it, The Freedom Act, and some minimization procedures adopted by the CIA, NSA, and then the FBI; and it's the FBI we're concerned mostly about. And the second issue was the retention of materials for litigation purposes, which I think the Amicus has covered as well.

And if the government wants to be heard on any of those others, they can be, but my interest really is in the FBI's minimization procedures and the use of inquiries by the FBI into potential criminal activity in the 702 collections.

So, with that, if we can have the parties who are going to argue introduce themselves first; and then, if there are any identified fact witnesses, we can have them introduced as well.

(b)(6); (b)(7)(C) from the Department of Justice.

MR. EVANS: Stuart Evans, also from the Department of Justice, Your Honor.

THE COURT: All right. And Ms. Jeffress.
MS. JEFFRESS: Your Honor, Amy Jeffress,
FISC Amicus.

THE COURT: All right. Thank you.

Any potential fact witnesses you may have here if
I have questions to ask, potentially, the FBI?

MR. EVANS: Your Honor, at this time we do have
several representatives from the FBI in the room with us.
We had not been anticipating, necessarily, presenting a fact
witness, but depending on whether the Court had relevant
questions, that's something that we can --

THE COURT: If I develop questions that you don't
answer and you want to turn to someone else to answer them,
then we'll have them sworn at that time. We'll hold off
until then.

All right. Well, I think that we will begin with
the Amicus and her report, and Ms. Jeffress, you'll want to
cover the other areas as well, but I'm obviously interested
in what you have developed as an issue in this FBI
minimization procedures and their appropriateness or not as
it affects the collection and dissemination of matters
related to crime and your position in that matter. So if
you can take the podium, please.

MS. JEFFRESS: Yes, good afternooon.

THE COURT: Thank you for your work on this
matter.
MS. JEFFRESS: Thank you, Your Honor. And thank you for appointing me to serve in this role.

Before I begin, I wanted to add one point to what I set forth in my brief about my understanding of my role as Amicus. One interpretation of the Amicus provision of the statute would be that my job is to present all legal arguments that advance the protection of individual privacy and civil liberties interests.

Many advocacy groups and academic experts presented these arguments to the Privacy and Civil Liberties Oversight Board in much greater detail than I have set forth in my brief. I did not think that the time allowed for my participation permitted me to serve that role, as a privacy and civil liberties advocate, broadly speaking. Rather, my understanding of the role that I was asked to and was able to fill, given the time constraints and my own abilities as advisor to the Court, was really to evaluate the program and to determine whether there were any aspects of the certifications and the procedures submitted to the Court that did not comply with the statutory and constitutional requirements, as I viewed it, with respect to the two specific issues that the Court noted in the order.

So I reviewed the program with that goal in mind and found that I thought that the FBI's minimization procedures are not consistent with the purpose of Section
702 or the Fourth Amendment because specifically they do not
provide sufficient safeguards of the U.S. person information
that is incidentally collected in the 702 -- Section 702
program.

To start with, Your Honor, I would first address
the issue of whether querying warrants a separate Fourth
Amendment analysis at all.

THE COURT: Yes, exactly.

MS. JEFFRESS: You could argue that a query is not
a search under the Fourth Amendment; that it is --

THE COURT: Well, if the original materials are
appropriately collected, which they are, I assume, if they
permitted them, how is looking at the materials a new
search?

MS. JEFFRESS: Right. It's not a new search so
much as it is a separate action that I think does warrant
Fourth Amendment scrutiny and needs to be treated as a
separate action subject to the Fourth Amendment
reasonableness test, and I think that that is appropriate,
and I'd also note that the Private and Civil Liberties
Oversight Board thought so as well. If you look at their
report on Pages 95 and 96, they talk about how -- and I'll
just quote -- concerns about post-collection practices such
as the use of queries to search for the communications of
specific U.S. persons cannot be dismissed on the basis that
the communications were, quote, lawfully collected, unquote.
That's the end of that quote.

The report, though, goes on to say that the Court must consider whether the procedures that govern the acquisition, use, dissemination and retention of U.S. persons -- and then I'll quote again -- quote, appropriately balance the government's valid interests with the privacy of U.S. persons, end quote. And I think that that querying process, too, is subject to a totality of the circumstances test to determine whether it's reasonable under the Fourth Amendment.

THE COURT: Well, if your bottom line conclusion is that if the minimization procedures are sufficient and consistent with the reasonableness requirement of the Fourth Amendment, that wouldn't solve your problem.

MS. JEFFRESS: That's correct. That's correct.

And with respect to the NSA's procedures and the CIA's procedures, I thought that they did. I thought that the requirements that may have been followed before the recent changes to the minimization procedures, but that it is now very clear, requiring that each U.S. person query be supported by a statement of facts that explains why the information is being sought and why it's relevant to foreign intelligence, or why it's expected to produce foreign intelligence information, I thought, justified the query in
a way that the FBI's procedures don't because they allow for
really virtually unrestricted querying of the Section 702
data in a way that NSA and CIA have restrained it through
their procedures.

I would just also note that the PCLOB report, on
Page 96, notes that given the low standards for collection
of information under Section 702, quote, The standards for
querying the collected data to find the communications of
specific U.S. persons may need to be more rigorous than
where higher standards are required at the collection stage,
unquote. And that's what distinguishes, in my view, Section
702 from the information collected pursuant to traditional
FISA applications or in other databases that are collected
under more traditional criminal procedure methods.

And then, Your Honor, the government may have
arguments on that point that I would want to respond to, but
I thought, for the interest of just introducing my position,
I would move to the second step in my analysis, which is
that the current procedures do not meet the Fourth Amendment
reasonableness test, and, as I've already said, I think that
the NSA and CIA do have sufficient protections in requiring
a written statement that reflects that each specific query
is designed to produce foreign intelligence information, and
that really justifies the intrusion on U.S. person
information that the queries implicate.
The FBI minimization procedures, though, do not. They allow the information to be queried for any legitimate law enforcement purpose, and I find two problems with that. One is that there need be no connection to foreign intelligence or national security, and that is the purpose of the collection, of course, and so they're overstepping, really, the purpose for which the information is collected.

THE COURT: Well, if you look at the -- it is somewhat anomalous, but it is in the statute. I mean, 702, the authorization, the original authorization, it talks about targeting persons reasonably believed to be located outside the United States to acquire foreign intelligence information. That's the purpose of it. But then you go back to the minimization procedures. It's under (h) and, I guess, in 1801(h), "Minimization procedures', with respect to electronic surveillance, means," and then it talks about (1), specific procedures, which I'm sure you're familiar with, having been at Justice and all, and the Attorney General's adopted these; (2), the procedures that require and what to do about it; and then (3) says, "notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been or is being or is about to be committed and that is to be retained or disseminated for law enforcement purposes."
So the statute recognizes another purpose, does it
not, of this collection of the foreign intelligence
information as a subsidiary of that or subset that there may
be evidence of a crime that's collected as well, which is
approved to be distributed under the statute?

MS. JEFFRESS: That's correct, Your Honor, and I
would note that you're correct that it also specifies any
crime. So it doesn't just restrict that to --

THE COURT: Right, as long as it's a serious crime
or a kidnapping or some type that people talk about.

MS. JEFFRESS: No, no, and I think that that is an
important point to note. And it explains why the government
is permitted to retain and disseminate evidence of a crime,
and that's that, you know, when the government collects it
pursuant to these lawful authorities, if there is evidence
of a crime, it would be somewhat counterintuitive for the
government not to be able to use that and to act on it.

But I think that the use -- the querying process
is different because there is no finding that this
incidental collection is such evidence, and that takes me to
the second point that I wanted to make about the FBI's
minimization procedures, which is that there are -- there is
no limitation on what type of matter can be the subject of a
query. So an assessment can be the subject of a query, and
assessments can be initiated for virtually any reason. I'm
sure there are limits on improper reasons, you know, racial
discrimination and things like that, and that's out of
bounds, of course, but really there is no threshold that
needs to be met.

And for an assessment, I would note that there are
restrictions even on the use of grand jury subpoenas for
assessments. So grand jury subpoenas can only be issued to
request subscriber information for telephone numbers or
email addresses, and so they're really viewed as considered
the very lowest of the purpose for which you would need a
query.

And I think that that opens up the Section 702
database to a really very wide-ranging, really virtually
unrestricted use by the FBI that I think should be cabined
in order to meet the Fourth Amendment reasonableness test.

I found that that unrestricted querying just is
inconsistent with the language and the analysis in the FISA
Court of Reviews case In Re: Sealed Case, which stated
plainly that the FISA process cannot be used as a device to
investigate wholly unrelated crimes, and I think that that's
what this querying process allows the FBI to do without any
restriction of the querying process.

THE COURT: That's Judge Silberman, 736 of his
opinion, you're talking about. He says, for example, a
group of international terrorists engaged in bank
robberies -- which is something I'm going to raise in a minute -- in order to finance or manufacture a bomb, the evidence of bank robbery should be treated just as evidence of a terrorist act itself, but the FISA process cannot be used as a device to investigate wholly unrelated ordinary crimes.

MS. JEFFRESS: That's what I thought was the language that made me -- gave me pause about what the FBI is doing with the Section 702 database here because that's exactly what it seems these minimization procedures permit.

THE COURT: That case, in essence, approved the practice of retaining and disseminating information about possible crimes --

MS. JEFFRESS: It does.

THE COURT: -- under proper controls.

MS. JEFFRESS: Right. And there's a very careful balancing in the opinion of the purpose -- the national -- the foreign intelligence purpose of the statute and the need to preserve and use evidence in a crime, but I thought it was a very careful analysis.

And on Page 735, there's also some language that I thought was instructive where the Court wrote, "The addition of the word 'significant' to [the section at issue] imposed a requirement that the government have a measurable foreign intelligence purpose other than just criminal
prosecution of even foreign intelligence crimes." So the
Court was grappling with what purpose the statute required,
and I think came to a conclusion that's instructive in this
context.

The last point that I would make, Your Honor, and
then I'm happy to answer specific questions from the Court,
but I thought that the government actually appeared to
recognize the need for limits in one regard with respect to
the changes that have been made to the NSA and CIA
minimization procedures, but also even in the government's
brief on Page 14, the government says, "Given that FBI is a
law enforcement agency as well as a member of the
intelligence community, the ability to query for evidence of
a crime using U.S. person identifiers can help the FBI
pursue important leads regarding criminal activity."

And I think that's good language, "important
leads." They clearly want to be able to use it for examples
that they cited: espionage, cyber crimes, terrorism, and,
you know, they said perhaps to help locate a kidnapper. And
I think that that -- that may be justifiable, but there's no
restriction in the minimization procedures that restrict it
even to important leads or important crimes. They can use
it for any purpose, and I just found that to be beyond --

THE COURT: Is it your impression, from what
you've been able to read in the PCLOB report, that an agent
or analyst who is conducting the assessment of a nonsecurity
crime would get generally responsive results against the
queries in the 702-acquired data, and I'm referring, not to
mislead you, that the PCLOB reports says, and notably, the
FBI says they don't get that.

MS. JEFFRESS: I saw that, and I don't know what
to make of it because it's anecdotal, and they didn't have
much support for it, but I take it that that is true, and
maybe you can find out more. But I don't know that that
is -- that that answers the question because going forward
it may be that it does draw responsive data or it may prove
the point, Your Honor, that maybe they don't need to be
querying the Section 702 database in cases that are not
national-security related.

THE COURT: All right. If the relevant
minimization procedures were modified, as you suggested to
us in the beginning, assuming incorporating executive branch
policies that limit this to national security, provided
these inquiries are serious crimes and that -- and to be
used as evidence in serious criminal cases, I mean, would
the modification be sufficient to satisfy, you think, the
concerns you have about violating the Fourth Amendment?

MS. JEFFRESS: Your Honor, I didn't make a
specific recommendation for what -- how the FBI should meet
this.
THE COURT: Did you talk about maybe they should record or have a written inquiry each time they want to do this? Every officer in the FBI would have to sit and write a justification up when he wants to send an inquiry in.

MS. JEFFRESS: That is one option, Your Honor, and the option that you just mentioned a moment ago in terms of limiting the types of matters that can be the subject of a query would be another; or perhaps you'd have both, given the sensitivity of the incidentally collected information.

But I would note that the FBI's general counsel, James Baker, testified three times that I'm aware of, possibly more than that, before the Privacy and Civil Liberties Oversight Board. He's one of the most authoritative experts on the program, and I think that he would certainly be highly capable of designing minimization procedures that would provide appropriate restrictions but also allow the FBI to use the information for purposes that are really justified and necessary to protect national security.

But I would note both of those options are ones that I think probably would satisfy the Fourth Amendment reasonableness test but are not present in the current procedures.

THE COURT: One of the things that was pointed out in PCLOB, and some of the government's materials as well, is
that this set of data is commingled with other data the FBI
has normally in their files and that it's essentially a
practical impossibility to distinguish between the two.
Would your requirement sort of be putting more emphasis on
the minimization procedures or making them more restrictive
and require them somehow to separate those out?
The government can answer in a minute as to that.
But would that be necessary, you think, to have a separate
data bank?

MS. JEFFRESSION: That, again, is why I didn't delve
into the specifics of what I think would be required. I
think separating it, if that's not possible, then perhaps
they need a justification and a set of requirements
surrounding the use of the querying in the entire database,
and that may be more practical.

THE COURT: I'll ask the government. I think it's
flagged somehow that it's NSA material anyway within the
same data bank. It is flagged because they do have some
procedures about that.
All right. Let me just switch with you for a
minute. On the retention -- the second prong of your
assignment that you've accepted from us was a retention for
litigation purposes beyond the normal purging time frames.
Even though there's an exception to the minimization
procedures that we've adapted and that are normally
required, you had felt that that was a justifiable
exception?

MS. JEFFRESS: I did, Your Honor. I just couldn't
see how the government would handle those competing
directives other than they have. It seems to me that the
government's made a real effort to comply with the
destruction requirements, but in the face of court orders,
where information is specifically designated as being
necessary for specific cases, I think that those specific
cases are good cause to maintain the information despite the
otherwise applicable destruction requirements.

So especially after having read the reports that
the government files annually with the Court, which your
order from 2014 required them to file, I thought that the
material that was being preserved was limited in nature. It
was specifically preserved for purposes of, you know, a
relatively small number of cases, and I just don't know how
else the government would accommodate the needs in those
cases, which seemed to me to be wholly legitimate and
specific. Where, of course, the destruction policies in the
minimization requirements are important, and they're
important in the Court's analysis of the program overall,
they're also general in nature in that they're, you know,
age-off requirements that apply to the entire body of data
and not to specific elements of it apart from that material
that is required to be destroyed because it's inadvertently collected and really shouldn't have been collected, but collected basically because of errors.

So I thought that the government had handled that appropriately, Your Honor, and, with the Court's oversight, I don't have any concerns about that aspect of the procedures.

THE COURT: All right. Anything else you want to address the Court about on these issues at this time?

MS. JEFFRESS: No. Do I come back or...?

THE COURT: You'll get a chance to come back.

MS. JEFFRESS: Thank you, Your Honor.

THE COURT: Thank you, Ms. Jeffress.

I'll hear from you at this time on behalf of the government. And you can focus, I think, your argument principally on the issues we've discussed with Ms. Jeffress and explain why this querying of the U.S. person information should be subject to Fourth Amendment search review or what is reasonable looking at this that can be done with proper minimization procedures to make sure that this is being appropriately done under the law.

Thank you, Your Honor. And the government appreciates your careful consideration of these issues. We appreciate the views of Amicus and the ability to address them in this hearing.
To begin with, to start with the Fourth Amendment issue that you addressed, we would agree with your earlier comments that the querying of this information after it's been lawfully acquired is not a separate Fourth Amendment event. It is not a separate search, and Amicus did not cite case law that suggests that it would be. It's certainly the case that the program as a whole must comply with the Fourth Amendment and must be reasonable under the Fourth Amendment.

THE COURT: Well, let me ask you about that. Suppose a local agent in the field office runs across somebody's name and, without any basis to think that he did anything wrong, he starts making an inquiry into the database of the FBI and gets a hit that there are some 702 evidence or materials that he can't see so he asks someone who has a FISA clearance to go ahead and make the inquiry, and they bring back something like a credit card fraud or something, and that has nothing to do, that he can tell, with any foreign intelligence issues. I mean, aren't there some protections that should apply there?

So I want to be very clear on that point. The FBI can only conduct a query for an authorized purpose. Now, that authorized purpose for FBI is different than NSA and CIA, but it must be an authorized purpose. They cannot go in and query because they come across someone who, as you point out, hasn't done anything wrong. That is
already prohibited by the minimization procedures.

The authorized purpose that the FBI had is either
for queries that are reasonably designed to return foreign
intelligence information or reasonably designed to return
evidence of a crime. Those two purposes, as Your Honor
points out, come directly from the definition of
minimization procedures in the statute.

They are also the joint purposes of the FBI
itself. It is a dual law enforcement and intelligence
agency, and certainly one of the things that we've learned
in the last 15 years is that we can't make artificial
distinctions between these two roles of law enforcement and
intelligence, and so perhaps hypothetical examples do help.

You can have instances, for example, where the FBI
is investigating a crime. Let's take a minor crime as
opposed to the more major ones. Let's take a minor crime
like something like cigarette smuggling, a federal offense,
or money laundering. The FBI queries in these federated
systems. They query not just the 702 information but other
information that they obtain from intelligence and law
enforcement, from their foreign partners. Query across.

When they conduct that query, they're not looking
at that time for foreign intelligence information. They're
looking for evidence of that crime, but to the degree
something then pings in the 702 and connects a dot that they
didn't know was there -- so they find, yes, my cigarette-smuggler actually is speaking with individuals -- that investigation has now taken a very different turn. Now we have a national security element to that investigation.

But when that query was conducted, the government didn't know that. We can only connect the dots by looking at the information. When we ran that query, we were doing so because we were looking for evidence of a crime across all of our systems.

Those federated queries are something that come from a number of experiences the government's had and a number of the commission reports. So going back to the 9/11 Commission, that Commission was quite critical of the government saying that one of the weaknesses that enabled the 9/11 attacks to occur was the government's failure to make use of information already in its repositories. There were three hijackers, the Commission found, that we couldn't identify and didn't because we didn't look at all the information that we already had.

To use an example more recent and even more on point, the Webster Commission's report on the Fort Hood attack criticized the government's queries of information in its possession. The people doing the assessment of Nidal Hasan did not identify several messages between Anwar Aulaqi
and Nidal Hasan, and the commission deemed it essential that
the FBI possess the ability to search all of its
repositories and to do so without balkanizing those data
sources.

And so these systems that do these federated
queries that allow us to, yes, to query the 702 information,
but all of these sources are in direct response to those
findings, and they're in direct response to our efforts over
the last 15 years to bring down this artificial wall between
the law enforcement mission of the FBI and its national
security intelligence mission.

THE COURT: As I asked the Amicus, the PCLOB said
that anecdotally the FBI has advised the board that it is
ever likely an agent or analyst who is conducting an
assessment of a non-national security crime will get a
response or result from the query against 702-acquired data,
and I know Rachel Brand and her counterparts say it never
happens, according to her.

Do you know anything about that?

{[b](6); [b](7);[c] So we would say at the very least it
would be extremely rare, and we believe that's one of the
many reasons why the privacy impact of these queries would
be quite low.

It's not surprising that it would be quite rare.

We are talking about a targeted program. Targets for 702
collection have to be non-U.S. persons outside the United States who the government reasonably believes possess or can communicate foreign intelligence information. It's a big program, but as the Court recognizes, it's a targeted program. This is not bulk surveillance.

I know in the Amicus brief there's a footnote about the government conducting surveillance of entire geographic regions. That is not this program. This program is targeted on people outside of the United States, and the likelihood that in any given query information about a U.S. person is going to be returned is quite low. However, if it happens, when it happens, it can be quite significant. It can connect that dot that we were not aware of before.

THE COURT: Is there any requirement in the minimization procedures that's been suggested by the government now that the FBI personnel be required to record the purpose of the query? Is there a written statement made or anything?

So that is something that the government has taken a look at in the past. We believe that the procedures, as they are, are sufficient, both as a statutory and constitutional matter. We don't believe that a difference in documentation -- and let's be clear, what we're talking about is a difference in documentation. FBI does have to document some aspects of their query, as do NSA...
and CIA. The particulars of that documentation vary, but there is a documentation of parts of it throughout, and I can explain that in more detail.

THE COURT: What's the rationale for the difference in the CIA/NSA minimization procedures and the FBI minimization procedures?

[(D)(6); (D)(7)(C)] So it goes fundamentally to the different missions of those organizations. The NSA and the CIA have a -- are foreign-focused intelligence organizations. They have little need usually to query U.S. persons. It happens much more rarely, and they don't have that law enforcement mission that the FBI has.

FBI has all of those things. FBI had also -- as I mentioned in the commission report, has a duty to do these federated queries across these systems, so they're conducting queries on a much more regular basis. But the fact that there isn't a documentation requirement with respect to the justification doesn't mean that the queries don't have to be documented.

So what is required of the FBI is that every query is recorded. Those query terms are recorded; what the agent -- which agent did the query is recorded; whether the information has been exported to another system is recorded.

And what the National Security does with those records for the FBI is we go out to about 30 field offices a
year, and we sit down with the agents and analysts, and we make them justify the queries; take a sample, and make them justify those queries. And what we've found is that they can. The agents and the analysts, they understand the rules because they have to have a justification. They can't, to use your first example, query someone just because they come across them, and they've done nothing wrong. They know they have to have a justification, and they've given them to us.

We've done some effective oversight of that.

We've found no systemic problems. We've found FBI agents and analysts understand the rules. We've found a few isolated incidents, but those incidents have been things like an individual querying their own name for work flow purposes.

THE COURT: In your example you gave, for instance, of cigarette-smuggling which turns out to be potentially related to national security matters, is the experience such now you think the FBI queries of 702 data can be limited to national-security-related crimes? I mean, do you have a database where you can recognize crimes generally associated with national security?

I think limiting the queries to national security crimes is going to cause us to miss connecting some of the dots or something we do not realize is a national security event before we conduct the query
and, in fact, has national security implications.

So to take another example, for example, for cyber security. FBI could be investigating a spear phishing attempt, a criminal attempt to access a computer. They have no indication that there's any sort of foreign connection. They run a query like this in those federated systems, and they find out -- they did not know before, but they find out that, you know, we have ________ cyber hackers who have been using this account. They just didn't know that.

So if we limit what those queries can have, we're going to miss those instances where we're going to make that connection. As I said, those connections are going to be rare, but very important when we find them.

THE COURT: Again, on the numbers, is there any FBI information available as to the actual numbers of queries that come up with hits that 702 evidence is available about a crime? And maybe it happens a hundred times a month, or is it once a year? I don't know.

So we don't have -- we, unfortunately, do not have specific information about when evidence of a crime is returned from one of those queries. What I can say, Your Honor, is that in no instance to date has the government used, in a criminal trial or in a non-national security matter, 702-obtained information.
THE COURT: So I understand the program -- I want to make sure I understand it. The 702 data that is mixed in with the other information you have is still segregated in a sense that when a query is made it hits a 702 data. That comes back that way. I mean --

Certainly, Your Honor. It's identified as FISA information, and this can occur in one of two different ways in this federated system.

If the agent has a subject matter reason to have access to FISA information and has the full training in the FISA minimization procedures, when they run a query like this, they will return the results, and it will be clear to them that this is FISA information and, in fact, as they look at it, 702 information.

If the agent does not -- is a criminal agent working mostly those cigarette cases, they would not have access to FISA information in the course of their normal duties. They would not have the FISA training. When they run that same query, they would -- the content would not be returned to them. Metadata would not be returned to them. The only thing that would be returned to them was an indication that there is some information available in this database that contains FISA.

And what the procedures before you do is they require that individual to go to someone who does have the
training and the minimization procedures. They have access
to the data to rerun the query. And there is a new
requirement, a new restriction, that has not been in the
procedures before that also requires supervisory approval
both from the criminal agent's supervisor and the national
security agent's supervisor before that second query is run
to ensure that it's appropriate, to ensure -- to use your
first example again -- they are not running queries for
someone for whom they have no reason to.

THE COURT: Again about whether you can ask
questions whether they be related to national- or foreign-
intelligence-related crimes was Judge Silberman's expression
that the Amicus pointed out where he talks about
international terrorists engaged in bank robbery that's
obviously to finance or manufacture a bomb. The evidence of
bank robbery is treated just like a terrorist act itself.
I'm not going to get into that.

So he concludes, then, but the FISA process cannot
be used as a device to investigate wholly unrelated ordinary
crime.

(b)(6), (b)(7)(C): So I think unfortunately the quote
the Amicus identified really turns the actual holding of In
Re: Sealed Case on it's head. So In Re: Sealed Case was a
case about the initial targeting of an individual, getting
that authorization from the FISA court in order to -- and it
was saying that we could not get a FISA for purely criminal reasons. But the holding of that case was that not even constitutionally a primary purpose of the government, but only a significant purpose of the government needed to be to obtain foreign intelligence information.

And Amicus's brief repeatedly refers to the purpose, the purpose. The purpose is an even stronger standard than a primary purpose, which has been rejected by In Re: Sealed Case and has been rejected by Congress in the Patriot Act. It must be that it's a significant purpose, and in 702 we have that purpose because when we're acquiring the information, we are acquiring information only because we've assessed that the target of that collection, in addition to being a non-U.S. person who we believe to be outside the United States, either possesses or is communicating foreign intelligence information.

THE COURT: PCLOB says at one point -- and really I'd like the opportunity to question what the PCLOB has said. But the PCLOB said at one point, at Page 161 there's a statement -- I made a note -- that it received -- the FBI receives only, quote, a small portion of the 702 collection. Do you know what that is, or --

Yes, I do, Your Honor. Thank you.

That's actually a point I was hoping to return to.
Not surprisingly, the individuals that the FBI is identifying are related to the things that FBI investigates. They are the CT cases. They are the cyber cases, weapons of mass destruction. Those are cases that they have already opened.

THE COURT: But when an FBI analyst has supposedly been tasked to email accounts, and he's reviewing all the emails, and he has a task because you were talking about weapons of mass destruction or something, but in there he finds ordinary credit card fraud, would that change the analysis of whether he could then use that and proceed with an investigation? It wasn't what he was looking for. Do you know anything about that?

 Andrea Reed	02:43:07PM 25

(b)(5); (b)(7)(C) It was not originally what they were
looking for, but FISA -- and this is not just the 702 --
FISA from the beginning, from 1978, has recognized that the
FBI might come across evidence of a crime in the course of
doing their investigation.

Now, I would say, as I said earlier, the
government has not used 702-obtained information in a non-
national security crime to date. This is an instance where,
and sort of interestingly, the interest of defendants and
the interest of the intelligence community happen to align,
right?

The intelligence community -- this is -- puts a
great deal of importance on this program. They're not going
to risk their sources and methods for this important program
on an ordinary crime, and that's where the use policy that
the government announced earlier this year stems from, is
the fact that the information is not going to be used in an
ordinary crime because we're not just going to risk our
sources and methods in those instances.

THE COURT: Is there any reason why the
minimization procedures could not incorporate some
restrictions to limit the searches to, as I said, certain
crimes related to national security?

I'm not sure where -- the Amicus has argued in her
brief, and she can raise this again, but that it's -- there
are certainly possibilities, if not probabilities, that
there will be incidental collection. I mean, we're talking of bits of information, collection of American conversations or whatever with others abroad, et cetera, or emails, et cetera, that are totally innocent, and it seems to me that the minimization procedures in effect now would allow the FBI to make inquiries that would then go into this information to see what might be there that would return anything about a crime because they had some -- you're saying some investigation open about somebody. But I don't know how you limit that appropriately to satisfy the requirements in the statute. There has to be reasonableness under the Constitution for this search or this inquiry, at least, to be made of this information. I'm struggling with that a little bit.

(b)(6); (b)(7)(C): I think, from a statutory perspective, as you mentioned earlier, the statute doesn't distinguish between crimes. It just says evidence of a crime.

With respect to reasonableness, the government would really assert that when the Court looks at these procedures, they need to look at the sum of these procedures as opposed to isolating aspects of them. It starts with a targeting and a limited collection aperture of the targeting in the first place and for those purposes. That doesn't mean we will not receive some incidental U.S. person
information. That's probably only where it starts.

You also have the access controls that are limiting this information to individuals who are working on these national security issues. You have the controls on retention, you know, the controls on dissemination. You have the controls of attorney-client communications. You have the controls on querying that can only be done for an authorized purpose.

All of these privacy controls are an integrated approach to protect Americans' civil liberties and privacy, and that whole of all of those protections, we have found, does a very good job of ensuring that no one is rifling through these communications.

THE COURT: Do we have numbers or ballpark figures as to the number of inquiries made by the FBI? Not just for crime, but just the numbers made to the 702 collection of materials on a yearly basis?

[b](6):[b](7)(C) So we don't have specific numbers. It's a substantial number of queries, particularly because of these federated systems. They don't break down by U.S. person or non-U.S. person. A query is a query. But it is a routine and encouraged practice for the FBI to conduct queries at the beginning of an assessment.

This is the way that the FBI, looking at its lawfully acquired information, makes its initial
determinations about whether further investigation, which
often involves further more privacy invasive steps, is
warranted or not. They conduct these queries, and then,
based on the results, either have confidence, no, there's
nothing here, and stop, or there is some additional
information that we need to investigate.

THE COURT: What problems would arise if the
Amicus's suggestion of modifying the minimization procedures
to be more precise and tightly controlled, although it may
be a written authorization, et cetera, would arise to the
FBI by having to do that?

So maybe to start with that written
justification requirement. Because these systems are
queried on such a routine basis, these federated systems in
some ways are FBI's Google of its lawfully acquired
information. They are quite routine. They must have that
justification before they query, but they're quite routine
queries.

And so the implications here -- there are
technical issues we would have to work out. But far more
concerning to us than the technical issues are the practical
ones. If we require our agents to write a full
justification every time -- think about if you wrote a full
justification every time you used Google. Among other
things, you would use Google a lot less. Well, one of the
things that we learned from these commission reports is
that's not what we want. We want the FBI to look and
connect the dots in its lawfully acquired information.

So there's a practical limitation that's going to
just cause the FBI to use these tools that we've spent a
good deal of time and learned some very hard lessons in
order to have to build; and in addition to that -- I'm
sorry, I'm losing my place here for a moment. In addition
to that, once you have that requirement, that bureaucratic
requirement, the FBI really has two choices. Either you're
going to have agents use the system less, or
alternatively -- and the FBI, when it was examining this
very kind of requirement said, well, one of the things we
might have to do is then pull the 702 information out. Pull
it out of the federated system. Balkanize the data again.

THE COURT: That was my next question.

Unlearn that lesson and have it in a
separate repository. And if we have it in that separate
repository, again, we're going to miss our dots because we
now have to query multiple systems. It's that querying of
multiple systems that has gotten us, as the government,
again and again and again. We finally, I think, have
learned our lesson. We don't want to unlearn it.

THE COURT: All right. Do you have any other
issues you wanted to address in this matter?
Your Honor, if you have no further questions.

THE COURT: Anything else?

All right. Thank you, I appreciate it.

(b)(6); (b)(7)(C) Thank you, Your Honor.

THE COURT: We'll get Ms. Jeffress up and get a chance for her last word here.

MS. JEFFRESS: Thank you, Your Honor. I'd like to first go back to the question that the Court asked.

(b)(6); (b)(7)(C)

THE COURT: Can you lower the mic a second. I can't see. That's why.

(b)(6); (b)(7)(C)

MS. JEFFRESS: There you go. Better?

THE COURT: Thank you.

(b)(6); (b)(7)(C)

MS. JEFFRESS: I wanted to go back to the question the Court asked with respect to the rationale for the difference between FBI's procedures and NSA's and CIA's, and that's, in fact, the subject that was just talking about, that it would be more difficult to adopt those -- to adopt similar procedures because the FBI's queries are so frequent. I don't think that that is necessarily an answer that justifies not complying with the Fourth Amendment. It doesn't seem to me to be too unreasonable to require.
As explained, the queries are already recorded, and when the Department of Justice goes to field offices to do oversight, they require the agents to explain them, and they have, in fact, found, which is good to know, that the agents can explain them. I don't think it's a real imposition to have the agents have to put that explanation in writing before they conduct the query, and I think it is a step that perhaps may mean that they don't always do it in the cases where now they do always do it, but perhaps that means because now they are doing it in cases where there really isn't a real obvious need to be doing it, assessments that aren't sufficiently important, and other circumstances.

So I don't think it's an unreasonable requirement, and I don't think that it would rebuild the wall or render the government unable to connect the dots. If the matter is important enough where the dots are important and could be connected, I think that the FBI will do it.

I also wanted to explain the point that I made about the scope of the incidental collection. I did not mean, in my Footnote 7, to endorse what the ACLU statement said about the program, and I actually don't think that statement is accurate. What I was really trying to do is to say, "Here's the extreme end of this criticism."

But I do stand by the text that I wrote with respect to how often Americans' communications could be
intercepted incidentally because the targets are so wide, and [redacted] actually did explain that to some extent; that the FBI only receives a certain portion of the Section 702 information, which is helpful. But the entire body of it really does likely intercept lots of information of, you know, Americans who are communicating with friends overseas who, as I pointed out, [redacted]

So I thought that the scope was really very -- potentially very broad, although I didn't take the same view that the ACLU took of that.

And, Your Honor, you mentioned that your concern is with, you know, obtaining information about credit card fraud and the like, and I think that they're -- that's one issue, but there is a potentially greater issue with just the intrusiveness of having the innocent communications reviewed. And there are lots of private communications that take place over email that people who are -- whose communications are incidentally collected would not want to be reviewed for any purpose, and so I think there should be stricter limitations for that reason.

I wanted to also respond to the comment about my turning the logic of In Re: Sealed Case on its head. And I understand [redacted] point, but I don't think that I did that because the analysis in that case was really whether --
<table>
<thead>
<tr>
<th>Time</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>02:54:46PM</td>
<td>1</td>
</tr>
<tr>
<td>02:55:00PM</td>
<td>5</td>
</tr>
<tr>
<td>02:55:11PM</td>
<td>7</td>
</tr>
<tr>
<td>02:55:15PM</td>
<td>8</td>
</tr>
<tr>
<td>02:55:24PM</td>
<td>9</td>
</tr>
<tr>
<td>02:55:28PM</td>
<td>10</td>
</tr>
<tr>
<td>02:55:30PM</td>
<td>11</td>
</tr>
<tr>
<td>02:55:33PM</td>
<td>12</td>
</tr>
<tr>
<td>02:55:38PM</td>
<td>13</td>
</tr>
<tr>
<td>02:55:43PM</td>
<td>15</td>
</tr>
<tr>
<td>02:55:47PM</td>
<td>16</td>
</tr>
<tr>
<td>02:55:50PM</td>
<td>17</td>
</tr>
<tr>
<td>02:55:53PM</td>
<td>18</td>
</tr>
<tr>
<td>02:55:57PM</td>
<td>19</td>
</tr>
<tr>
<td>02:55:59PM</td>
<td>20</td>
</tr>
<tr>
<td>02:56:04PM</td>
<td>21</td>
</tr>
<tr>
<td>02:56:07PM</td>
<td>22</td>
</tr>
<tr>
<td>02:56:12PM</td>
<td>23</td>
</tr>
<tr>
<td>02:56:15PM</td>
<td>24</td>
</tr>
<tr>
<td>02:56:18PM</td>
<td>25</td>
</tr>
</tbody>
</table>

It was balancing the prosecution being -- prosecution of national security crimes for the most part being a purpose of the collection versus just a collection of foreign intelligence information. So it really didn't go into the sort of issues surrounding the prosecution of unrelated crimes, which is my central concern here.

And I think -- let me just check my notes for one thing, Your Honor.

Finally, I think that the query, as [b](6);(b)(7)(C) pointed out, if it is reasonably designed to return foreign intelligence information or evidence of a crime, that can be explained in a statement that is a relatively minimal imposition on the FBI.

I would just conclude by saying that I don't think that the FBI will voluntarily set limits on its querying procedures because law enforcement agencies tend not to take steps to restrict or limit what they can do, for obvious reasons, and that's, you know, giving them the full benefit that they're very-well-intentioned and they want to do their job as best they possibly can. But the incentive is that if you give them a program or a database or any other power, they will use it to the fullest possible extent, and I think that in this case the procedures could be tighter and more restrictive, and should be, in order to comply with the Fourth Amendment.
THE COURT: Thank you very much, Ms. Jeffress.

I'm going to see if counsel for the Court has any particular question they wanted to raise.

Your Honor, can I ask one question?

can I --

THE COURT: You can sit down.

-- ask you one follow-up question on something?

So just following up on the statement that the judge mentioned, the anecdotal statement, and this other statement in the PCLOB report, I think it's in the separate Brand and Cook part of the report: "We are unaware of any instance," this says, "in which a database query in an investigation of a nonforeign intelligence crime resulted in a hit on Section 702 information and much less a situation in which such information was used to further such an investigation of prosecution."

I think you made the point, you know, that that undercuts the notion of this being overly intrusive, but at the same time doesn't it undermine the -- I mean, how do you reconcile that with the national security purpose of the collection as a whole?

You gave a bank robbery example, or I think it was -- I can't remember exactly what it was, but --

THE COURT: Cigarettes.
Cigarette smugglers. Are there any examples where queries unrelated to foreign intelligence on the front end resulted in the acquisition of information relating to foreign intelligence? And if the answer is no, then how does this process really serve the overall national security purpose of Section 702?

So to answer your question, I don't have a smoking gun example for you, and I think that's for a couple of reasons. One is because, again, the collection that is being acquired is of the non-U.S. persons outside the United States. We would expect queries -- particularly queries not for foreign intelligence information, but instead for evidence of crime -- to very rarely respond to anything.

And for a second reason, which is it is -- querying is one tool in FBI's toolbox, and to discern that any individual query was the thing that broke open the case is often a very difficult thing to do.

That said, what we have found, again, just returning to those -- returning to the commission reports of the past, is that we do not want to limit our ability to connect the dots. We don't know beforehand, before we do the query, whether the information is going to be responsive and is going to lead to that national security angle.

And we have appropriate controls. We limit the
access. We limit the retention. We can limit the
dissemination, and we have our policy on use. We have a
variety of limitations designed, particularly designed to
protect the privacy and civil liberties of individuals, but
what we don't want to do is to balkanize our data to then
limit our ability to find that dot that is out there in the
case where it is, in fact, important. It is -- and I think
this is something that we also saw in the PCLOB report.

It wasn't that the PCLOB report thought there were
no concerns. Where they ultimately came out on this was
where are the proper places to put those protections, and we
believe the proper places are to limit those queries to
foreign intelligence information or evidence of a crime, to
limit that access, to limit the targeting to foreign
intelligence information, to limit the retention and
dissemination, to limit their use.

We've imposed all of those, but what we don't
believe we should do is limit our ability to find the dots
where we weren't expecting to find them.

Thank you, Your Honor.

I guess what I want to ask about is
federated queries, which it sounds like is the principal
means by which FBI personnel queried the 702 data. Is that
correct?

It is one of the means. So the FBI
has both a repository of information that includes FISA and some other information, for example, like national security letter information that it queries, but it also has the system -- I believe it's DIVS -- that allows these federated queries of not just the FISA information but, for example, CBP records, foreign intelligence reports, FBI's own case files. It is really those federated queries where those come into play.

So let's talk about a federated query on DIVS then.

Sure.

If it's one query that reaches into multiple data sets including the 702 data, is it the same standard for queries across all those different data sets?

It is now. So because the FISA information is one of the repositories that is queried, what you, in effect, have had is that the FISA rules now apply to all of these data sets when you conduct that query. If I conduct a query, and I have authorization to get 702 information as a result of that query, then my query needs to meet the FISA standard regardless of the fact that it might not ping any of the -- bring back any of the 702 information regardless of the fact that I was actually intending, thinking, oh, I'm looking for those CBP records or something else.
So what we have already done, because of the FISA information that's in there, is to make sure that we have this more restrictive regime.

And that's true even for FBI personnel who haven't been trained on the 702 data and so wouldn't have direct return but rather the sort of mediated process with supervisory approval that you described before?

So for FBI personnel for whom the data would not return content or metadata, for those individuals their queries would not necessarily need to meet the standard because one of the things that is in this repository are internal FBI records when someone has done like a temporary duty assignment, but they would, at most, get back a response saying there is positive foreign intelligence -- there is a positive hit in this repository that contains FISA and some other information.

And they would stop there unless they were conducting a foreign intelligence or evidence-of-a-crime-type query, and, in that case, they would have to go to a

But in any scenario, a query that reaches into the 702 data is subject to the reasonably designed to return foreign intelligence information or
evidence of a crime.

(b)(6); (b)(7)(C) If content or metadata can be returned to the person conducting the query, then it has to meet that standard each and every time.

(b)(6) Okay. And if it were withheld from (b)(1); (b)(3); (b)(7)(E)

(b)(6); (b)(7)(C) Yes.

(b)(6) But they ultimately only get it if it meets that standard after people look at it; is that right?

(b)(6); (b)(7)(C) Correct.

Just one small clarification on that when it talks (b)(1); (b)(3); (b)(7)(E)
If the answer is no, it ends there. That information goes nowhere. It doesn't go into FBI's case files. It doesn't go for permanent retention. It isn't disseminated.

If the answer is yes, and it is foreign intelligence information or evidence of a crime, it is covered by the minimization procedures and used appropriately.

Thank you.

One more question. Should it be understood that it's not sufficient for -- in order to run a query that touches on the 702 data, for it to relate to the subject of an assessment or any other type of open FBI investigation, it has to be reasonably designed to return evidence of a crime or foreign intelligence information? So it may be necessary, but it's not sufficient that it relates to an open assessment or other --

Correct.

-- category of case.

Every query that returns content or metadata has to be for an authorized purpose. That authorized purpose has to be that the query is reasonably
designed to return foreign intelligence information or evidence of a crime. That is true for every query that returns content or metadata.

(b)(6) Thank you.

THE COURT: All right. Thank you very much,

(b)(6); (b)(7)(C) I appreciate your work on that.

(b)(6); (b)(7)(C) Thank you, Your Honor.

THE COURT: Anything else?

MS. JEFFRESS: No, Your Honor. I think the government may want another word. No?

MR. EVANS: One moment, Your Honor, if you would.

THE COURT: Sure.

(Pause)

MR. EVANS: Your Honor, nothing further. Thank you.

THE COURT: All right. Thank you.

I want to thank you again, all the counsel here, for their work on the matter and the agents, but particularly Ms. Amy Jeffress, who dedicated, I know, weekends and nights to prepare and to study and understand, in a short period of time, this rather difficult and complex area and has given an excellent report of great assistance to the Court, and that's why we have an Amicus. So I appreciate that very much.

We are going to look at this. We have to consider
the certifications in the near future to look forward on
these matters. So we'll take a look at it, and let you all
know. Thank you again.

(Whereupon the hearing was
concluded at 3:07 p.m.)

CERTIFICATE OF OFFICIAL COURT REPORTER

I, (b)(6) RDR, CRR, do hereby
certify that the above and foregoing constitutes a true and
accurate transcript of my stenographic notes and is a full,
true and complete transcript of the proceedings to the best
of my ability.

Dated this 29th day of October, 2015.
GOVERNMENT'S EX PARTE SUBMISSION OF ATTORNEY GENERAL GUIDELINES (U)

In accordance with subsection 702(f)(2)(C) of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"), the United States of America, by and through the undersigned Department of Justice attorney, hereby submits ex parte the attached "Attorney General's Guidelines for the Acquisition of Foreign Intelligence Information Pursuant to the Foreign Intelligence Surveillance Act of 1978, as Amended."
These guidelines have been adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(f)(1) of the Act. (U)

Respectfully submitted,

National Security Division
United States Department of Justice

SECRET//NOFORN

SECRET//NORFORN

ACLU 16-CV-8936 (RMB) 00171
MEMORANDUM OPINION AND ORDER

This matter is before the Foreign Intelligence Surveillance Court ("FISC" or "Court") on the "Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications," which was filed on July 15, 2015 ("July 15, 2015 Submission"). For the reasons explained below, the government's request for approval is granted, subject to certain reporting requirements. The Court's approval of the certifications, amended certifications, and accompanying targeting procedures and minimization procedures is set out in a separate order that is being entered contemporaneously herewith.
I. BACKGROUND

A. The 2015 Certifications

The July 15, 2015 Submission includes certifications that have been executed by the Attorney General ("AG") and the Acting Director of National Intelligence ("DNI") pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), which is codified at 50 U.S.C. § 1881a:

Each of the certifications (collectively referred to as "the 2015 Certifications") is accompanied by the supporting affidavits of the Director of the National Security Agency ("NSA"), the Director of the Federal Bureau of Investigation ("FBI"), and the Director of the Central Intelligence Agency ("CIA"); two sets of targeting procedures, for use by the NSA and FBI respectively;¹ and four sets of minimization procedures, for use by the NSA, FBI, CIA, and the National Counterterrorism Center ("NCTC"), respectively.² The July 15, 2015 Submission also includes an explanatory memorandum prepared by the Department of Justice.

¹ The targeting procedures for each of the 2015 Certifications are identical. The targeting procedures for the NSA ("NSA Targeting Procedures") appear as Exhibit A to each of the 2015 Certifications. The targeting procedures for the FBI ("FBI Targeting Procedures") appear as Exhibit C to each of the 2015 Certifications.

² The minimization procedures for each of the 2015 Certifications are identical. The minimization procedures for the NSA ("NSA Minimization Procedures") appear as Exhibit B to each of the 2015 Certifications. The minimization procedures for the FBI ("FBI Minimization Procedures") appear as Exhibit D to each of the 2015 Certifications. The minimization procedures for the CIA ("CIA Minimization Procedures") appear as Exhibit E to each of the 2015 Certifications. The minimization procedures for the NCTC ("NCTC Minimization Procedures") appear as Exhibit G to each of the 2015 Certifications.
("DOJ") ("July 15, 2015 Memorandum"). Finally, it includes an unclassified summary of DOJ and DNI oversight of Section 702 implementation, and a summary of "notable Section 702 requirements," which have been submitted to the Court in accordance with the recommendation of the Privacy and Civil Liberties Oversight Board ("PCLOB"). See July 15, 2015 Memorandum at Tabs 1 and 2; see also PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act at 142-43 (July 2, 2014) ("PCLOB Report") (Recommendation 5).

Each of the 2015 Certifications involves "the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information."
Each of the 2015 Certifications generally proposes to continue acquisitions of foreign intelligence information that are now being conducted under certifications that were made in 2014 ("the 2014 Certifications"). See July 15, 2015 Memorandum at 2. The 2014 Certifications, approved by the FISC on August 26, 2014. The 2014 Certifications, in turn, generally renewed authorizations to acquire foreign intelligence information under a series of certifications made by the AG and DNI pursuant to Section 702 that dates back to 2008. In its July 15, 2015 Submission, the government also seeks approval of amendments to the certifications in all of the Prior 702 Dockets, such that the NSA, CIA, and FBI henceforward will apply the same minimization procedures to information obtained under prior certifications as they will to information to be obtained under the 2015 Certifications. See July 15 Memorandum at 2-3;

3 See Memorandum Opinion and Order entered on August 26, 2014 ("August 26, 2014 Opinion").

4 See These dockets, referred to as "the Prior 702 Dockets".

5 The July 15, 2015 Submission does not propose any changes to the FBI Targeting Procedures or NCTC Minimization Procedures. See July 15, 2015 Memorandum at 3.
B. The Extension of Time and the Appointment of Amicus Curiae

Before making the July 15, 2015 Submission, the government filed draft versions of the 2015 Certifications on June 15, 2015. After reviewing those drafts, the Court concluded "that this matter is likely to present one or more novel or significant interpretations of the law, which would require the Court to consider appointment of an amicus curiae" under 50 U.S.C. § 1803(i)(2). See Order issued on July 7, 2015 ("July 7, 2015 Order"), at 3. The Court further noted that the 30-day review period specified by 50 U.S.C. § 1881a(i)(1)(B) would, as a practical matter, foreclose amicus participation. Id. The Court may, however, extend that 30-day review period "as necessary for good cause in a manner consistent with national security." 50 U.S.C. § 1881a(j)(2).

To help the Court decide "whether to extend the time it would have to act on the 2015 Certifications and revised procedures in order to allow for meaningful amicus assistance in reviewing them," the Court ordered the government to "explain in writing whether – and if so, how long – an extension of the time for the Court to review the 2015 Certifications and revised procedures would be consistent with national security." July 7, 2015 Order at 4. On July 14, 2015, the Government timely filed its Response to the July 7, 2015 Order, advising that "the government assesses that an extension of 60 to 90 days . . . would be consistent with national security." See Government’s Response to the Court’s Order of July 7, 2015, filed on July 14, 2015, at 7.

On July 23, 2015, the Court found that "the need for an extension to allow for [amicus] participation constitutes ‘good cause’" for an extension under Section 1881a(j)(2). See Order
issued on July 23, 2015, at 3. Accordingly, it extended "the period for Court review under [Section 1881a(i)(1)(B)] for 90 days, such that this review must be completed no later than November 12, 2015." Id. On August 13, 2015, the Court issued an order appointing Amy Jeffress to serve as amicus curiae in this matter pursuant to 50 U.S.C. § 1803(i)(2)(B). The Court directed Ms. Jeffress to address whether the minimization procedures accompanying the 2015 Certifications meet the requirements of 50 U.S.C. § 1881a(e) and are consistent with the Fourth Amendment, see id, § 1881a(i)(3)(A), in view of the provisions of the procedures that apply to:

(i) queries of information obtained under section 702, particularly insofar as queries may be designed to return information concerning United States persons, see NSA Minimization Procedures at 7, FBI Minimization Procedures at 11-12, and CIA Minimization Procedures at 3-4; and

(ii) preservation for litigation purposes of information otherwise required to be destroyed under the minimization procedures, see NSA Minimization Procedures at 8-9, FBI Minimization Procedures at 24-25, and CIA Minimization Procedures at 10-11.

Thereafter, the Court issued an order directing Ms. Jeffress and the government to submit briefs on these issues no later than October 16, 2015. See Briefing Order issued on September 16, 2015, at 4. After both briefs were timely filed, the Court received oral argument from the

---

6 The Court wishes to thank Ms. Jeffress for her exemplary work in this matter. Her written and oral presentations were of the highest quality and extremely informative to the Court's consideration of this matter. The Court is grateful for her willingness to serve in this capacity.
amicus and counsel for the government on October 20, 2015.\textsuperscript{7}

C.\hspace{0.5em}Review of Compliance Issues

FISC review of targeting and minimization procedures under Section 702 is not confined to the procedures as written; rather, the Court also examines how the procedures have been and will be implemented.\hspace{0.5em}See, e.g., Memorandum Opinion entered on April 7, 2009, at 22-24 ("April 7, 2009 Opinion"); Memorandum Opinion entered on Aug. 30, 2013, at 6-11 ("August 30, 2013 Opinion"). Accordingly, for purposes of its review of the July 15, 2015 Submission, the Court has examined quarterly compliance reports submitted by the government\textsuperscript{8} since the most recent FISC review of Section 702 certifications and procedures was completed on August 26, 2014, as well as individual notices of non-compliance relating to implementation of Section 702. Based on its review of these submissions, the Court, through its staff, orally conveyed a number of compliance-related questions to the government. On October 8, 2015, the Court conducted a hearing to address some of the same compliance-related questions ("October 8 Hearing").

II. REVIEW OF CERTIFICATIONS \textbf{[REDACTED]} AND OF THEIR PREDECESSOR CERTIFICATIONS AS AMENDED BY THE JULY 15, 2015 SUBMISSION.

The Court must review a certification submitted pursuant to Section 702 "to determine

\textsuperscript{7} See generally Transcript of Proceedings Held Before the Honorable Thomas F. Hogan on October 20, 2015 ("October 20 Transcript").

whether [it] contains all the required elements.” 50 U.S.C. § 1881a(i)(2)(A). The Court’s examination of Certifications confirms that:

(1) the certifications have been made under oath by the AG and the Acting DNI, as required by 50 U.S.C. § 1881a(g)(1)(A), see

(2) the certifications contain each of the attestations required by 50 U.S.C. § 1881a(g)(2)(A), see

(3) as required by 50 U.S.C. § 1881a(g)(2)(B), each of the certifications is accompanied by the applicable targeting procedures and minimization procedures:

(4) each of the certifications is supported by the affidavits of appropriate national security officials, as described in 50 U.S.C. § 1881a(g)(2)(C); and

(5) each of the certifications includes an effective date for the authorization in compliance with 50 U.S.C. § 1881a(g)(2)(D) – specifically, the certifications become effective on August 14, 2015, or on the date upon which this Court issues an order concerning the certification under Section 1881a(i)(3), whichever is later, see

---

9 The 2015 Certifications were made by the Attorney General and Michael P. Dempsey, the Deputy DNI for Intelligence Integration. At the time, Mr. Dempsey was serving as Acting DNI pursuant to a Presidential Memorandum dated September 20, 2013. That Memorandum, which was issued pursuant to the Federal Vacancies Reform Act of 1998, as amended, 5 U.S.C. § 3345, et seq., provides that the Deputy DNI for Intelligence Integration “shall act as and perform the functions and duties of the [DNI] during any period in which the DNI and the Principal Deputy Director of National Intelligence have died, resigned, or otherwise become unable to perform the functions and duties of the DNI.” See Presidential Memorandum, “Designation of Officers of the Office of the Director of National Intelligence ("ODNI") to Act as Director of National Intelligence,” 78 Fed. Reg. 59,159 (Sept. 20, 2013).

10 See Affidavits of Admiral Michael S. Rogers, United States Navy, Director, NSA (designee) and Affidavit of Director, NSA; Affidavits of James B. Comey, Director, FBI (designee) and Affidavit of Director, FBI; and Affidavits of John O. Brennan, Director, CIA (designee) and Affidavit of Director, CIA.
The Court therefore finds that [redacted] contain all the required statutory elements. See 50 U.S.C. § 1881a(i)(2)(A).

Similarly, the Court has reviewed the certifications in the Prior 702 Dockets, as amended by the 2015 Certifications, and finds that they also contain all the elements required by the statute. Id. 12

III. REVIEW OF THE TARGETING AND MINIMIZATION PROCEDURES

The Court is also required, pursuant to 50 U.S.C. § 1881a(i)(2)(B) and (C), to review the targeting and minimization procedures to determine whether they are consistent with the requirements of 50 U.S.C. § 1881a(d)(1) and (e)(1). Pursuant to 50 U.S.C. § 1881a(i)(3)(A), the Court further assesses whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment.

Section 1881a(d)(1) requires targeting procedures that are “reasonably designed” to “ensure that any acquisition authorized under [the certification] is limited to targeting persons reasonably believed to be located outside the United States” and to “prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.” In addition to these statutory

11 The statement described in 50 U.S.C. § 1881a(g)(2)(E) is not required in this case because there has been no “exigent circumstances” determination under Section 1881a(c)(2).

12 The effective dates for the amendments to the certifications in the Prior 702 Dockets are the same as the effective dates for the 2015 Certifications. See [redacted].
requirements, the government uses the targeting procedures as a means of complying with Section 1881a(b)(3), which provides that acquisitions "may not intentionally target a United States person reasonably believed to be located outside the United States." See NSA Targeting Procedures at 1, 3-4, 7; FBI Targeting Procedures at 1-4. The FISC considers steps taken pursuant to these procedures to avoid targeting United States persons as relevant to its assessment of whether the procedures are consistent with the requirements of the Fourth Amendment. See Docket No. 702(i)-08-01, Memorandum Opinion entered on Sept. 4, 2008, at 14 ("September 4, 2008 Opinion").

Section 1881a(e)(1) requires minimization procedures that "meet the definition of minimization procedures under [50 U.S.C. §§] 1801(h) or 1821(4)]." The applicable statutory definition is fully set out at pages 12-14 below.

A. The NSA and FBI Targeting Procedures Comply With Statutory Requirements and Are Reasonably Designed to Prevent the Targeting of United States Persons

Under the procedures adopted by the government, NSA is the lead agency in making targeting decisions under Section 702. Pursuant to its targeting procedures, NSA may target for acquisition a particular "selector," which is typically a facility such as a telephone number or email address. The FBI Targeting Procedures come into play in cases where the government...
TOP SECRET//SI//ORCON//NOFORN

The NSA Targeting Procedures included as part of the July 15, 2015 Submission contain two revisions, neither of which raises any concern. Both changes concern the requirement that, before tasking a selector for collection under Section 702, NSA first assess that the target is expected to possess or receive, or is likely to communicate, foreign intelligence information concerning a foreign power or a foreign territory. See NSA Targeting Procedures at 4. The first change consists of new language clarifying that such assessments must be “particularized and fact-based” and must consider the “totality of the circumstances.” See id. The new language, which was added following a recommendation of the PCLOB, see PCLOB Report at 134-35 (Recommendation 1), results in no change in practice, as NSA has interpreted prior versions of the procedures to require the same particularized, fact-based assessments of the totality of the circumstances. See July 15, 2015 Memorandum at 5-6.

The second change, made in response to the same PCLOB recommendation, is the addition of language requiring NSA analysts to document each such foreign intelligence assessment. New language requires NSA analysts to “provide a written explanation of the basis for their assessment, at the time of targeting, that the target possesses, is expected to receive, and/or is likely to communicate foreign intelligence information concerning [the] foreign power or foreign territory” about which they expect to obtain foreign intelligence information pursuant to a particular targeting determination. See NSA Targeting Procedures at 8. This change, which will facilitate review and oversight of NSA targeting decisions, presents no issue under Section 1881a(d)(1).

For the reasons stated above and in the Court’s opinions in the Prior 702 Dockets, the
Court concludes that the NSA Targeting Procedures and the FBI Targeting Procedures, as written, are reasonably designed, as required by Section 1881a(d)(1): (1) to ensure that any acquisition authorized under the 2015 Certifications is limited to targeting persons reasonably believed to be located outside the United States, and (2) to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States. Moreover, for the reasons stated above and in the Court’s opinions in the Prior 702 Dockets, the Court concludes that the NSA and FBI Targeting Procedures, as written, are reasonably designed to prevent United States persons from being targeted for acquisition — a finding that is relevant to the Court’s analysis of whether those procedures are consistent with the requirements of the Fourth Amendment. See pages 36-45 below.

B. The FBI, NSA, and CIA Minimization Procedures Comply With Statutory Requirements

The FBI, NSA, and CIA all have access to “raw,” or unminimized, information obtained under Section 702. Each agency is governed by its own set of minimization procedures in its handling of Section 702 information. Under Section 1881a(i)(2)(C), the Court must determine whether the agencies’ respective minimization procedures included as part of the July 15, 2015 Submission meet the statutory definition of minimization procedures set forth at 50 U.S.C. §§ 1801(h) or 1821(4), as appropriate. Sections 1801(h) and 1821(4) define “minimization

13 The Court has already concluded that procedures identical to the FBI Targeting Procedures included as part of the July 15, 2015 Submission comply with the applicable statutory requirements. See August 26, 2014 Opinion at 12-14. There is no basis for the Court to deviate from that conclusion here.
procedures” in pertinent part as:

(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance [or physical search], to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;[14]

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in [50 U.S.C. § 1801(e)], shall not be disseminated in a manner that identifies any United States person, without such person’s consent, unless such person’s identity is necessary to understand foreign intelligence information or assess its importance; [and]

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes[.]

14 Section 1801(e) defines “foreign intelligence information” as

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or a foreign territory that relates to, and if concerning a United States person is necessary to—

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.
50 U.S.C. § 1801(h); see also id. § 1821(4).\(^{13}\)

1. **Changes to Provisions Permitting the Retention of Section 702-Acquired Information Subject to Preservation Obligations Arising from Litigation**

In 2014, the Court approved provisions permitting FBI, NSA and CIA to retain Section 702-acquired information subject to specific preservation obligations arising in litigation concerning the lawfulness of Section 702. See August 26, 2014 Opinion at 21-25. Access to information retained under these provisions is tightly restricted. See id. at 21, 23. The revised NSA and CIA Minimization Procedures accompanying the 2015 Certifications contain revisions to these “litigation hold” provisions.

The litigation hold provisions currently in effect allow NSA and CIA to retain specific Section 702-acquired information that is otherwise subject to age-off\(^{16}\) if DOJ has advised either agency in writing that such information is subject to a preservation obligation in pending or anticipated administrative, civil, or criminal litigation. See id. at 22-23. Those provisions also recognize that litigation preservation obligations can also apply to Section 702-acquired information that is subject to destruction for reasons other than the age-off requirements of the procedures – e.g., domestic communications subject to destruction under Section 5 of the NSA

\(^{15}\) The definitions of “minimization procedures” set forth in these provisions are substantively identical (although Section 1821(4)(A) refers to “the purposes . . . of the particular physical search”) (emphasis added). For ease of reference, subsequent citations refer only to the definition set forth at Section 1801(h).

\(^{16}\) For example, the NSA generally may not retain telephony and certain forms of Internet communications for “longer than five years from the expiration date of the certification authorizing the collection” unless the NSA determines that certain specified retention criteria are met. See NSA Minimization Procedures at 7. The CIA Minimization Procedures contain a similar requirement. See CIA Minimization Procedures at 2.
Minimization Procedures. See id. at 23-24. When such circumstances arise, the provisions currently in effect state that "the Government will notify the [FISC] and seek permission to retain the material as appropriate [and] consistent with the law." See id. (quoting 2014 procedures). The Court encouraged the government to consider further revision of the procedures to address such circumstances with generally applicable rules rather than on a piecemeal basis. See id. at 24.

In response to this suggestion, the government has modified the language in the NSA and CIA Minimization Procedures.
The Court agrees with amicus curiae Amy Jeffress that the revised litigation hold provisions comport with the requirements of Section 1801(h) and strike a reasonable and appropriate balance between the retention limitations reflected in FISA and the government's need to comply with its litigation-related obligations. See Brief of Amicus Curiae submitted on October 16, 2015, at 28-34 ("Amicus Brief").

2. Provisions Restricting the Retention and Use of Section 702-Acquired Information Subject to the Attorney-Client Privilege

The revised FBI, NSA and CIA Minimization Procedures all include modifications to the provisions restricting the use and dissemination of attorney-client communications that are acquired pursuant to Section 702. The FBI Minimization Procedures include three such changes. The procedures currently in effect include a provision permitting the FBI, after providing the
original copy of an attorney-client communication to DOJ for sequestration with this Court and destroying other copies, to maintain a back-up copy that is subject to strict access controls. See August 26, 2014 Opinion at 35. The first change to the FBI procedures clarifies that system administrators and technical personnel may have access to such backup copies, but not for analytical or operational purposes. See FBI Minimization Procedures at 14. The second change consists of the addition of language requiring the FBI’s Office of General Counsel to approve all disseminations that include attorney-client privileged communications. See id. at 17. The new language requires that before any such dissemination be made, reasonable efforts be undertaken to instead use other, non-privileged sources of information, and to tailor each dissemination to minimize or eliminate the disclosure of attorney-client privileged information. See id. at 17-18. The third change is the addition of a requirement that all disseminations of attorney-client privileged communications include language to advise recipients that the dissemination contains information subject to the attorney-client privilege, that the information is being disseminated “solely for intelligence or lead purposes,” and that it may not be further disseminated or used in any trial, hearing, or other proceeding without approval of the AG or the Assistant AG for National Security. See id. at 18.

The provisions of the NSA and CIA Minimization Procedures concerning attorney-client communications also have been modified. The revised language requires, among other things, the destruction of attorney-client communications that are affirmatively determined not to contain foreign intelligence information or evidence of a crime. See NSA Minimization Procedures at 10; CIA Minimization Procedures at 5.
Moreover, disseminations of privileged information must contain an appropriate caveat to protect the information from being used in a legal proceeding in the United States. See NSA Minimization Procedures at 11; CIA Minimization Procedures at 7.

The revisions to the provisions of the FBI, NSA, and CIA Minimization Procedures concerning attorney-client communications serve to enhance the protection of privileged information. The Court is satisfied that the changes present no concern under Section 1801(h).

3. **Provisions of the FBI Minimization Procedures Permitting the Retention of Back-up Copies and Encrypted Information**

The government has added new language to the FBI Minimization Procedures to permit the retention of Section 702-acquired information in “backup and original evidence systems.”
See FBI Minimization Procedures at 24. Only systems administrators and technical personnel may have access to such systems and data in them may not be viewed or used for the purpose of intelligence analysis. See id. Backup and original evidence systems are used to preserve copies of Section 702-acquired data in the form it was originally acquired. See July 15, 2015 Memorandum at 16. Such unaltered copies are unreadable without additional processing but can be used in case of emergency “to restore lost, destroyed, or inaccessible data,” or to create an “original evidence copy” for evidentiary uses (e.g., to establish chain of custody in connection with a criminal prosecution or to fulfill the government’s criminal discovery obligations, see id. at 16-17). See FBI Minimization Procedures at 24. In the event backup and original evidence systems are used to restore lost, destroyed, or inaccessible data, the FBI must apply its minimization procedures, including any applicable time limits on retention, to the restored data. See id.

The government has also added a new provision to the FBI Minimization Procedures permitting the FBI to retain Section 702-acquired information that is encrypted or believed to contain secret meaning for any period of time during which such material is subject to, or of use in, cryptanalysis or otherwise deciphering secret meaning. See id. at 25. Access to such information is restricted to FBI personnel engaged in cryptanalysis or deciphering secret meaning. See id. Nonpublicly available information concerning unconsenting United States persons retained under the provision cannot be used for any other purpose unless such use is permitted under a different provision of the minimization procedures. See id. Once information retained under this provision is decrypted or its secret meaning is ascertained, the generally-
applicable retention restrictions of the procedures apply, though the government has stated that it will calculate the age-off date from the later of the date of decryption or the date of expiration of the certification pursuant to which the information was acquired. See July 15, 2015 Memorandum at 18. 19

Neither of these new provisions precludes the Court from finding that the FBI Minimization Procedures comport with Section 1801(h). Both are narrowly tailored to serve legitimate government interests in a manner that appropriately protects nonpublicly available information concerning unconsenting United States persons.

4. Reporting Requirement for Disseminations to Private Entities or Individuals

The version of the FBI Minimization Procedures that was approved by the Court in 2014 provides that “information that reasonably appears to be foreign intelligence information, is necessary to understand foreign intelligence information or assess its importance, or is evidence of a crime” may be disseminated to “a private individual or entity in situations where the FBI determines that said private individual or entity is capable of providing assistance in mitigating serious economic harm or serious harm to life or property.” See August 26, 2014 Opinion at 19 (quoting 2014 FBI Minimization Procedures at 33). Whenever reasonably practicable, such disseminations must not include information identifying a United States person “unless the FBI reasonably believes it is necessary to enable the recipient to assist in the mitigation or prevention of the harm.” See id. (quoting 2014 FBI Minimization Procedures at 33). Such disseminations

19 To avoid confusion regarding the applicable age-off requirements, the government is encouraged to make this calculation methodology explicit in future versions of the procedures.
must be reported to DOJ within ten business days. See id. The government has retained the
foregoing language but added language requiring that disseminations pursuant to this provision
also promptly be reported to the FISC. See FBI Minimization Procedures at 37. This
modification does not alter the Court's conclusion that this provision of the procedures is
consistent with the requirements of Section 1801(h). See August 26, 2014 Opinion at 20.

5. Provisions Permitting Compliance with Specific Constitutional, Judicial or
Legislative Mandates

The NSA and CIA Minimization Procedures included as part of the July 15, 2015
Submission each contain new language stating that "[n]othing in these procedures shall prohibit
the retention, processing, or dissemination of information reasonably necessary to comply with
specific constitutional, judicial, or legislative mandates.” See NSA Minimization Procedures at
1; CIA Minimization Procedures at 4-5. These provisions were not included in the draft
procedures that were submitted to the Court in June 2015, but appear to have been added by the
government thereafter. They are not discussed in the July 15, 2015 Memorandum.

The apparent breadth of these new provisions gives the Court pause. As discussed above,
the applicable definition of "minimization procedures" requires, inter alia, "specific procedures
... that are reasonably designed in light of the purpose and technique of the particular
surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of
nonpublicly available information concerning unconsenting United States persons consistent with
the need of the United States to obtain, produce, and disseminate foreign intelligence
information.” 50 U.S.C. §§ 1801(h)(1) (emphasis added). In light of this requirement, the NSA
and CIA Minimization Procedures contain page after page of detailed restrictions on the
acquisition, retention, and dissemination, of Section 702-acquired information concerning United
States persons. A provision that would allow the NSA and CIA to deviate from any of these
restrictions based upon unspecified “mandates” could undermine the Court’s ability to find that
the procedures satisfy the above-described statutory requirement.

It appears, however, that the government does not intend to apply these provisions as
broadly as their language would arguably permit. In 2012, the government proposed a similar
 provision as part of minimization procedures to be applied by NCTC in handling certain
unminimized terrorism-related information acquired by FBI pursuant to other provisions of
FISA. In requesting approval of a provision that would allow NCTC personnel to deviate from
other requirements of its minimization procedures when “reasonably necessary to comply with
specific constitutional, judicial, or legislative mandates,” the government asserted that
“Executive Branch orders or directives will not trigger this provision, nor will general
Congressional directives that are not specific to information NCTC receives pursuant to this
motion.” See Government’s Submission of Amendments to Standard Minimization Procedures for FBI Electronic Surveillance and Physical
Search Conducted Under FISA and Submission of Revised Minimization Procedures for the
NCTC, submitted on April 23, 2012, at 31-32. The Court approved the NCTC minimization
procedures with the understanding that this provision would be applied sparingly. The Court
described the provision as permitting NCTC personnel to “retain, process or disseminate
information when reasonably necessary to fulfill specific legal requirements” and compared it to
a more narrowly-drafted provision of separate procedures that permits CIA to retain or disseminate information that is "required by law to be retained or disseminated." Memorandum Opinion and Order issued on May 18, 2012, at 11 (emphasis added).

The Court understands based on informal communications between the Court staff and attorneys for the government that NSA and CIA intend to apply the similar provisions at issue here in the same narrow manner. In any case, to avoid a deficiency under the above-described definition of "minimization procedures," the Court must construe the phrase "specific constitutional, judicial, or legislative mandates" to include only those mandates containing language that clearly and specifically requires action in contravention of an otherwise-applicable provision of the requirement of the minimization procedures. Such clear and specific language, for instance, might be found in a court order requiring the government to preserve a particular target's communications beyond the date when they would otherwise be subject to age-off under the minimization procedures. On the other hand, these provisions should not be interpreted as permitting an otherwise prohibited retention or use of information simply because that retention or use could assist the government in complying with a general statutory requirement, such as those stated at 50 U.S.C. § 1881a(b). To ensure that these provisions are being applied in a manner consistent with the Court's understanding, the government will be directed to promptly report any use thereof to the Court in writing, along with a written justification for each such
6. Provisions Concerning Queries of Information Acquired Through Collection Under Section 702

Finally, the NSA, CIA, and FBI Minimization Procedures included as part of the July 15, 2015 Submission all include revised provisions concerning queries of unminimized data acquired pursuant to Section 702. The previously-approved minimization procedures for all three agencies permit appropriately-trained personnel with access to Section 702-acquired information to query repositories containing such information, subject to certain restrictions. See PCLOB Report at 55. The terms used to conduct such queries may in some circumstances include information concerning United States persons or otherwise be expected to return information about a United States person. See id. at 55-60.

a. NSA and CIA querying provisions

The NSA and CIA Minimization Procedures accompanying the 2015 Certifications contain several important restrictions that have been carried forward from prior versions of the procedures. Most notably, all terms used to query the contents of communications acquired through Section 702, such as phone numbers or key words, must be terms “reasonably likely to return foreign intelligence information.” See NSA Minimization Procedures at 7; CIA Minimization Procedures at 3. This requirement applies to all queries of Section 702-acquired

---

20 The Court understands that the government may have added these new provisions to clarify that information acquired under Section 702 may be shared with Members of Congress or Congressional committees in connection with Congressional oversight of the program. If so, the Court would urge the government to consider replacing these broadly-worded provisions with language that is narrowly tailored to that purpose.
contents, not just queries containing United States-person identifiers. See NSA Minimization Procedures at 7; CIA Minimization Procedures at 3. Further, the NSA and CIA Minimization Procedures continue to require that both agencies maintain records of all United States-person identifiers that are used to query Section 702 data and that such records be made available for mandatory review by DOJ and ODNI. See NSA Minimization Procedures at 7; CIA Minimization Procedures at 3.21

In addition, the NSA and CIA Minimization Procedures accompanying the 2015 Certifications now also mandate that NSA and CIA prepare “a statement of facts establishing that the use of any [United States-person] identifier as a selection term is reasonably designed to return foreign intelligence information as defined in FISA,” see NSA Minimization Procedures at 7; CIA Minimization Procedures at 3. Like the records referred to above, these written justifications are provided to DOJ and ODNI to facilitate their oversight of NSA and CIA queries. See July 15, 2015 Memorandum at 20-21.22

21 The NSA Minimization Procedures also continue to preclude United States-person queries of its “upstream collection.” See NSA Minimization Procedures at 7. Such collection includes Internet communications acquired through the assistance of providers that control the “backbone” over which Internet communications are carried and is more likely than other forms of Section 702 collection to contain information of or concerning United States persons with no foreign intelligence value. See Memorandum Opinion entered on October 3, 2011, at 5 n.3, 33-41 (“October 3, 2011 Opinion”). Because only NSA receives “upstream collection,” see id. at 18 n.17, CIA and FBI are unable to query information so acquired.

22 Representatives of DOJ and ODNI conduct bi-monthly reviews at NSA and CIA to assess the agencies’ compliance with the Section 702 targeting and minimization procedures. July 15, 2015 Memorandum, Tab 1 at 2, 4. As part of those reviews, those DOJ and ODNI representatives review all United States-person identifiers approved for use in querying the (continued...)

---

Page 25
These additional requirements will result in no change in practice, as NSA and CIA already prepare and record foreign intelligence justifications for each query, which are subsequently provided to DOJ and ODNI oversight personnel. Nevertheless, adding these documentation requirements to the NSA and CIA Minimization Procedures serves to further reduce the risk that Section 702-acquired information concerning United States persons will be used, or even accessed, for improper purposes. The Court agrees with the government and Ms. Jeffress\(^{23}\) that the revised querying provisions of the NSA and CIA Minimization Procedures are consistent with the requirements of Section 1801(h).

b. **FBI querying provisions**

i. **Description of the FBI querying provisions**

The FBI Minimization Procedures also permit appropriately-trained personnel to conduct queries of systems containing Section 702 data. See FBI Minimization Procedures at 11 (queries of electronic and data storage systems); see id. at 28-29 (queries of ad hoc systems). In one respect, the queries permitted under the FBI’s procedures are broader than those allowed by the NSA and CIA Minimization Procedures. Queries by FBI personnel of Section 702-acquired data

\(^{22}\) (...continued)

contents of Section 702-acquired communications as well as the written documentation of the foreign intelligence justifications for each such query. See id. at 3, 4. When necessary to assess compliance, additional information is requested by the oversight personnel and provided by NSA, and any compliance issues are promptly reported to the FTSC. See id. at 3, 4.

\(^{23}\) See Amicus Brief at 14 ("I conclude that the NSA and CIA minimization procedures are sufficient to ensure that the use of U.S. person identifiers for th[e] purpose of [querying Section 702-acquired information] complies with the statutory requirements of Section 702 and with the Fourth Amendment.").
may be reasonably designed to “find and extract” either “foreign intelligence information” or “evidence of a crime.” See id. at 11, 28-29. Both types of queries have been explicitly permitted by the FBI Minimization Procedures since 2009.24 Unlike NSA and CIA, the FBI applies this standard to all queries of Section 702-acquired information, regardless of whether the querying term includes information concerning a United States person. See id.; see also Oct. 20 Transcript at 19-20.25 The FBI also applies this standard regardless of whether the dataset being queried

24 In [redacted], the Court approved FBI Minimization Procedures that incorporated by reference, as modified in a number of respects not relevant here, the “Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under the Foreign Intelligence Surveillance Act” which were approved by the Attorney General on October 22, 2008 and submitted to this Court in [redacted] (“October 2008 SMPs”). See [redacted], Memorandum Opinion issued on April 7, 2009, at 14-17 (“April 7, 2009 Opinion”). Section III.D of the October 2008 SMPs permitted FBI personnel to use queries that were reasonably designed “to find and extract foreign intelligence information or evidence of a crime and to minimize the extraction of third-party information.” See Oct. 2008 SMPs at 16.

25 The FBI Minimization Procedures contain a general statement that, except for certain listed provisions, “these procedures do not apply to information concerning non-United States persons.” FBI Minimization Procedures at 2. The querying provisions discussed in the text above are not among the listed exceptions. See id. Nevertheless, there are substantial quantities of information concerning United States persons within the Section 702 data subject to querying by the FBI, and it is impossible for FBI personnel to know beforehand whether or not United States-person information will be responsive to a given query of that data. Accordingly, the Court does not understand the above-described exception for “information concerning non-United States persons” to qualify the requirement that each query be reasonably designed to find and extract foreign intelligence information or evidence of a crime. In light of the FBI’s practice (continued...)

TOP SECRET//SI//ORCON//NOFORN

Page 27
TOP SECRET//SI//ORCON//NOFORN

includes the contents of communications or only metadata. See FBI Minimization Procedures at 11-12, 28-29. The FBI Minimization Procedures require that records be maintained of all queries of the Section 702 acquired data, and that such records include the term used in making each query. See id. at 11, 29. Unlike CIA and NSA, however, the FBI does not require its personnel to record their justifications for any queries. See id.

The government has added language to the querying provisions of the FBI Minimization Procedures to clarify that a search of an FBI storage system containing raw-FISA acquired information does not constitute a “query” within the meaning of the procedures if the user conducting the search does not receive access to unminimized Section 702-acquired information in response to the search. See id. at 11-12, 29. In such cases, the query results include a notification that the queried dataset contains Section 702-acquired information responsive to the query. See id. at 12 n.4.

The new language also clarifies what actions an agent or analyst without appropriate training and access to Section 702 information may take upon receiving a positive “hit” indicating the existence of (but not access to) responsive information. See FBI Minimization Procedures at 12 n.4. Such a user may request that FBI personnel with Section 702 access rerun

\[\text{\ldots continued}\]

of applying this standard to all queries of datasets including Section 702-acquired information, see October 20 Transcript at 20, the FBI also does not appear to consider the exception to apply in this regard.

\[\text{\ldots continued}\]

This can occur either because the user running the query has not been granted access to raw FISA-acquired information, or because a user who has been granted such access has chosen to limit the query such that it will not return raw FISA-acquired information. See FBI Minimization Procedures at 11-12, 29.
the query if it otherwise would be authorized by the FBI Minimization Procedures and if the request is approved by both the user’s supervisor and by a national security supervisor. See id. Generally speaking, the user without access to FISA-acquired information can be provided with access to information contained in the query results only if such information reasonably appears (based on the review of FBI personnel with authorized access to Section 702-acquired information) to be foreign intelligence information, to be necessary to understand foreign intelligence information, or to be evidence of a crime. See id. If it is “unclear,” however, whether one of these standards is met, “the user, who does not otherwise have authorized access may review the query result solely in order to assist in the determination of whether information contained within the results meets those standards.” Id. According to the government, such situations are “very rare.” See October 20 Transcript at 45.

In addition, on the PCLOB’s recommendation, see PCLOB Report at 137-38 (Recommendation 2), the government has added language to the querying provisions of the FBI Minimization Procedures to more fully describe the FBI’s querying practices.27 This language is specifically, the procedures state:

It is a routine and encouraged practice for the FBI to query databases containing lawfully acquired information, including FISA-acquired information, in furtherance of the FBI’s authorized intelligence and law enforcement activities, such as assessments, investigations and intelligence collection. Section III.D governs the conduct of such queries. Examples of such queries include, but are not limited to, queries reasonably designed to identify foreign intelligence information or evidence of a crime related to an ongoing authorized investigation or reasonably designed queries conducted by FBI personnel in making an initial decision to open an assessment concerning a threat to the national security, the prevention or protection against a Federal crime, or the collection of foreign intelligence, as authorized by the Attorney General Guidelines. These examples (continued...
descriptive and works no change to the applicable querying requirements or to the FBI's querying practices.²⁸

ii. Analysis of the FBI querying provisions

Amicus curiae Amy Jeffress has raised concerns regarding the querying provisions of the FBI Minimization Procedures. See Amicus Brief at 18-28. Ms. Jeffress does not specifically assert that the querying provisions render the procedures inconsistent with the applicable statutory definition of minimization procedures. Nevertheless, she contends that the FBI Minimization Procedures "go far beyond the purpose for which the Section 702-acquired information is collected in permitting queries that are unrelated to national security." See id. at

²⁷(...continued)

are illustrative and neither expand nor restrict the scope of the queries authorized in the language above.

FBI Minimization Procedures at 11 n.4; see also id. at 28 n.8 (similar language).

²⁸ The FBI has adopted one policy change that is not reflected in its minimization procedures. The government has imposed additional limitations on the FBI's use of Section 702-acquired information in connection with non-foreign intelligence criminal matters. These limitations, which are reflected in the ODNI's Signals Intelligence Reform 2015 Anniversary Report, are described in the report as follows:

[C]onsistent with the recommendation of the [PCLOB], information acquired under Section 702 about a U.S. person will not be introduced as evidence against that person in any criminal proceeding except (1) with the approval of the Attorney General, and (2) in criminal cases with national security implications or certain other serious crimes. This change will ensure that, if [DOJ] decides to use information acquired under Section 702 about a U.S. person in a criminal case, it will do so only for national security purposes or in prosecuting the most serious crimes.

Amicus Brief at 17 (quoting http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#section-702); see also id. at 18 (further describing policy).
19. The Court respectfully disagrees.

There is no statutory requirement that all activities involving Section 702 data serve solely a foreign intelligence national security purpose. To be sure, Section 702 was enacted to permit “the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.” 50 U.S.C. § 1881a(a) (emphasis added). But even at the time of acquisition, the statute does not require the government to have as its sole purpose obtaining foreign intelligence information. Rather, the AG and DNI need certify only that obtaining foreign intelligence information is “a significant purpose” of the acquisition. See id. § 1881a(g)(2)(v) (emphasis added).\(^\text{29}\) Under the “significant purpose” standard, an acquisition under Section 702 is permissible “even if ‘foreign intelligence’ is only a significant – not a primary – purpose” of the targeting decision. See In re Sealed Case, 310 F.3d 717, 734 (FISA Ct. Rev. 2002) (discussing 2001 amendment to Title I of FISA permitting government to conduct electronic surveillance based upon certification that obtaining foreign intelligence information is a “significant purpose of the surveillance”).\(^\text{30}\)

Nor does FISA foreclose any examination or use of information acquired pursuant to Section 702 that lacks a purpose relating to foreign intelligence. It is true that the government’s

\(^{29}\) As discussed above, each of the 2015 Certifications includes such an attestation of purpose. See [redacted].

\(^{30}\) 50 U.S.C. § 1804 (a)(6)(b) – the substance of which appeared in subsection 1804(a)(7)(B) at the time of In re Sealed Case – requires that each application for an order approving electronic surveillance under FISA contain a certification by a high-level Executive Branch official that, among other things, “a significant purpose of the surveillance is to obtain foreign intelligence information.”
minimization procedures must be "reasonably designed in light of the purpose and technique of the [collection], to minimize the . . . retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. § 1801(h)(1) (emphasis added), and must limit the dissemination of nonpublicly available information identifying unconsenting United States persons to certain circumstances, see id. § 1801(h)(2). Notwithstanding these requirements, however, FISA states that the minimization procedures must also "allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." Id. § 1801(h)(3). Hence, FISA does not merely contemplate, but expressly requires, that the government's procedures provide for the retention and dissemination of Section 702-acquired information that is evidence of crime for law enforcement purposes. This requirement applies whether or not the crime in question relates to foreign intelligence or national security. See In re Sealed Case, 310 F.3d at 731 (notwithstanding restrictions in subsections 1801(h)(1)-(2), subsection 1801(h)(3) permits "the retention and dissemination of non-foreign intelligence information which is evidence of ordinary crimes for preventative or prosecutorial purposes") (italics in original).

Ms. Jeffress acknowledges this statutory framework permits the retention and dissemination for law enforcement purposes of evidence of crimes that is discovered by queries of the Section 702-acquired data that are designed to find and extract foreign intelligence information. See October 20 Transcript at 10. She suggests, however, that it restricts queries of
the unminimized data – in particular those that are predicated on United States-person information – that are designed to elicit information about crimes unrelated to foreign intelligence. See id. But this distinction finds no support in the statutory text. Nothing in the statute precludes the examination of information that has otherwise been properly acquired through application of the targeting procedures and retained under the minimization procedures for the purpose of finding evidence of crimes, whether or not those crimes relate to foreign intelligence.

It would be a strained reading of the definition of minimization procedures to permit FBI personnel to retain and disseminate Section 702 information constituting evidence of a crime implicating a United States person for law enforcement purposes, but to prohibit them from querying Section 702 data in a manner designed to identify such evidence. And such an interpretation would lead to anomalous results: FBI personnel who came across one communication acquired under Section 702 that incriminates a United States person – perhaps because it was responsive to a query for foreign intelligence information – would be prohibited from running queries tailored to identify additional communications obtained under Section 702 pertaining to the same criminal activity, even though Section 1801(h)(3) explicitly authorizes the retention and dissemination of such information for law enforcement purposes.

Finally, the Court respectfully disagrees with Ms. Jeffress’ assertion that the FBI’s querying practices run afoul of the Foreign Intelligence Surveillance Court of Review’s admonition that “‘the FISA process cannot be used as a device to investigate wholly unrelated ordinary crimes.’” See Amicus Brief at 18 (quoting In re Sealed Case, 310 F.3d at 736)). The
Court of Review made that statement in rejecting the government's contention that "even prosecutions of non-foreign intelligence crimes are consistent with a purpose of gaining foreign intelligence information so long as the government's objective is to stop espionage or terrorism by putting an agent of a foreign power in prison." See In re Sealed Case, 310 F.3d at 735-736 (italics in original). The Court of Review concluded that it would be an "anomalous reading" of the "significant purpose" language of 50 U.S.C. § 1804(a)(6)(B) to allow the use of electronic surveillance in such a case. See id. at 736. The Court nevertheless stressed, however, that "[s]o long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution, it satisfies the significant purpose test." Id. at 735.

The FBI's use of queries designed to elicit evidence of crimes unrelated to foreign intelligence does not convert Section 702 acquisitions into "a device to investigate wholly unrelated ordinary crimes." The FBI's querying provisions apply only to information that has been acquired following application of the NSA Targeting Procedures. As discussed above, those targeting procedures require that before tasking a selector for collection, NSA first make a particularized assessment, based on the totality of the circumstances, that the user of the selector is expected to possess or receive, or is likely to communicate, foreign intelligence information concerning a foreign power or a foreign territory. See NSA Targeting Procedures at 4. This requirement ensures that at least a significant purpose of each targeting decision under Section 702 is the acquisition of foreign intelligence information. Queries of the data acquired through application of this targeting process that are designed to elicit evidence of crimes unrelated to foreign intelligence are therefore consistent with the "significant purpose" language of Section
Finally, it must be noted that the FBI Minimization Procedures impose substantial restrictions on the use and dissemination of information derived from queries that, taken together, ensure that the requirements of Section 1801(h) are satisfied. In the event that a query produces a positive hit on Section 702-acquired information, the query results can only be viewed by FBI personnel who are appropriately trained and approved to handle such information and “only for the purpose of determining whether it reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or to assess its importance, or to be evidence of a crime.” See FBI Minimization Procedures at 8. Generally, other FBI personnel who have not been trained for and granted access to FISA-acquired information are not allowed to view the query results unless the information has first been determined by appropriately cleared personnel to meet one of those standards. See FBI Minimization Procedures at 12 n.4.31 Information that is determined to meet one of those criteria can be retained for further investigation and analysis and may be disseminated only in accordance with additional restrictions. See id.; see also id. at 30-37. Before using FISA-acquired information for further investigation, analysis, or dissemination, the FBI must strike, or substitute a characterization for, information of or concerning a United States person, including that person’s identity, if it does not reasonably appear to be foreign intelligence information, to

31 In “very rare” circumstances, see October 20 Transcript at 45, FBI personnel who are not trained for and do not have access to Section 702-acquired information may view the results of a query solely to aid in the determination of whether the information constitutes foreign intelligence information or evidence of a crime. See FBI Minimization Procedures at 12 n.4.
be necessary to understand foreign intelligence information or assess its importance, or to be
evidence of a crime. See id. at 9.

Based on the foregoing, the Court concludes that the revised querying provisions of the
FBI Minimization Procedures comport with the requirements of Section 1801(h). Ms. Jeffress’
constitutional concerns about these provisions are addressed below.

7. Conclusion

For the reasons stated above and in the Court’s opinions in the Prior 702 Dockets, the
Court concludes that the NSA, FBI, and CIA Minimization Procedures satisfy the definition of
minimization procedures at Section 1801(h).

D. The Targeting and Minimization Procedures Are Consistent with the Fourth
Amendment

The Court next considers whether the targeting and minimization procedures included in
the July 15, 2015 Submission are consistent with the requirements of the Fourth Amendment.

1. The Applicable Analytical Framework

The Fourth Amendment does not require the government to obtain a warrant to conduct
surveillance “to obtain foreign intelligence for national security purposes [that] is directed against
foreign powers or agents of foreign powers reasonably believed to be located outside the United
States.” In re Directives Pursuant to Section 105B of FISA, Docket No. 08-01, Opinion at 18-19
(FISA Ct. Rev. Aug. 22, 2008) (“In re Directives”). This exception to the Fourth

32 A declassified version of the opinion in In re Directives is available at 551 F.3d 1004
(continued...)

---

TOP SECRET//SI//ORCON//NOFORN---
Amendment's warrant requirement applies even when a United States person is the target of such a surveillance. See id. at 25-26 (discussing internal Executive Branch criteria for targeting United States persons). The FISC has previously concluded that the acquisition of foreign intelligence information pursuant to Section 702 falls within this "foreign intelligence exception" to the warrant requirement of the Fourth Amendment. See September 4, 2008 Opinion at 34-36; accord United States v. Mohamud, 2014 WL 2866749 at *15-18 (D. Or. June 24, 2014).

It follows that the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment if those procedures, as implemented, are reasonable. In assessing the reasonableness of a governmental intrusion under the Fourth Amendment, the court must "balance the interests at stake" under the "totality of the circumstances." Id. at 20. The court must consider "the nature of the government intrusion and how the government intrusion is implemented. The more important the government's interest, the greater the intrusion that may be constitutionally tolerated." In re Directives at 19-20 (citations omitted).

If the protections that are in place for individual privacy interests are sufficient in light of the governmental interest at stake, the constitutional scales will tilt in favor of upholding the government's actions. If, however, those protections are insufficient to alleviate the risks of government error and abuse, the scales will tip toward a finding of unconstitutionality.

Id. at 20.

The government's national security interest in conducting acquisitions pursuant to Section 702 "is of the highest order of magnitude." September 4, 2008 Opinion at 37 (quoting

---


---

32(...continued)

(FISA Ct. Rev. 2008).
In re Directives at 20). With regard to the individual privacy interests involved, the Court has concluded, as discussed above, that the targeting procedures now before it are reasonably designed to target non-United States persons who are located outside the United States. Such persons fall outside the ambit of Fourth Amendment protection. See September 4, 2008 Opinion at 37 (citing United States v. Verdugo-Urquidez, 494 U.S. 259, 274-75 (1990)).

Nevertheless, because the government acquires under Section 702 communications to which United States persons and persons within the United States are parties, that is not the end of the matter. Such acquisitions can occur when those non-targeted persons are parties to a communication that is to or from, or that contains a reference to, a tasked selector. See September 4, 2008 Opinion at 15-20. Such communications may also be acquired when they constitute part of a larger “Internet transaction” (e.g., a transaction that also contains one or more communications that are to or from, or that contain a reference to, a tasked selector. In the latter case, the entire transaction may be unavoidably acquired by the NSA’s “upstream” collection. See October 3, 2011 Opinion at 5, 30-31.33

In the Prior 702 Dockets, the FISC concluded that earlier versions of the various agencies’ targeting and minimization procedures adequately protected the substantial Fourth

---

33 FISA minimization protects the privacy interests of United States persons in communications in which they are discussed, regardless of whether they were parties to such communications. See Section 1801(h)(1) (protecting “nonpublicly available information concerning unconsenting United States persons”) (emphasis added). In contrast, non-targets generally do not have a Fourth Amendment-protected interest in communications in which they are discussed, unless they are also parties to the communication. See Alderman v. United States, 394 U.S. 165, 174-76 (1969).
Amendment interests that are implicated by the acquisition of communications of such United States persons. See, e.g., August 26, 2014 Opinion at 38-40; August 30, 2013 Opinion at 24-25. In the FISC’s assessment, the combined effect of these procedures has been “to substantially reduce the risk that non-target information concerning United States persons or persons inside the United States will be used or disseminated” and to ensure that “non-target information that is subject to protection under FISA or the Fourth Amendment is not retained any longer than is reasonably necessary.” August 26, 2014 Opinion at 40 (internal quotation marks omitted).

2. The FBI’s Querying Practices Do Not Render the Targeting and Minimization Procedures Inconsistent with the Fourth Amendment

Amicus curiae Amy Jeffress urges the Court to reconsider its prior Fourth Amendment assessments and to reach “a different conclusion” in light of the provisions of the FBI Minimization Procedures, discussed above, permitting agents and analysts to query the Section 702-acquired information in the FBI’s possession using United States-person information for the purpose of finding evidence of crimes unrelated to foreign intelligence. See Amicus Brief at 22. Ms. Jeffress asserts that without additional safeguards, such querying is inconsistent with the requirements of the Fourth Amendment:

The FBI’s querying procedures effectively treat Section 702-acquired data like any other database that can be queried for any legitimate law enforcement purpose. The minimization procedures do not place any restrictions on querying the data using U.S. person identifiers . . . . As a result, the FBI may query the data using U.S. person identifiers for purposes of any criminal investigation or even an assessment. There is no requirement that the matter be a serious one, nor that it have any relation to national security. . . . [T]hese practices do not comply with . . . . the Fourth Amendment.

Id. at 19. According to Ms. Jeffress, the querying provisions of the FBI Minimization Procedures should be revised to “require a written justification for each U.S. person query of the database...
that explains why the query is relevant to foreign intelligence information or is otherwise justified,” or in some other manner that provides additional protection for the United States-person information in the FBI’s possession. See id. at 27.

Although the FBI’s minimization procedures have for several years expressly permitted the FBI to query unminimized Section 702-acquired data using query terms that are reasonably designed to find and extract not only foreign intelligence information but also evidence of a crime, Ms. Jeffress raises concerns that the Court has not expressly addressed in its prior Section 702 Opinions. The Court agrees with Ms. Jeffress, see id. at 21-24, that it is not bound by its prior approvals of procedures permitting such querying. Indeed, Section 702 requires the Court to assess anew whether the procedures accompanying each certification submitted to it for review are both consistent with both the applicable statutory requirements and with the Fourth Amendment. See 50 U.S.C. § 1881a(i)(2)(B)-(C), (i)(3)(A). After conducting the required reassessment, the Court concludes that the FBI’s querying practices do not render the government’s implementation of Section 702 inconsistent with the Fourth Amendment.

Ms. Jeffress contends that each query by FBI personnel of Section 702-acquired information is a “separate action subject to the Fourth Amendment reasonableness test.” See October 20 Transcript at 6; see also Amicus Brief at 24-25. The government agrees that the FBI’s querying process is relevant to the Court’s reasonableness analysis, but asserts that each query is not a “separate Fourth Amendment event” that should be independently assessed. See October 20 Transcript at 19. Rather, in the government’s view, it is “the program as a whole [that] must . . . be reasonable under the Fourth Amendment.” See id. The Court agrees with the
government and declines to depart from the analytical framework described above.

As discussed above, FISA requires the Court to assess whether "the targeting and
minimization procedures adopted in accordance with [50 U.S.C. § 1881a(d) and (e)] are
consistent . . . with the fourth amendment to the Constitution." 50 U.S.C. § 1881a(i)(3)(A). This
language directs the Court to assess the constitutionality of the framework created by the
targeting and minimization procedures. Moreover, as also discussed above, the Court of Review
made clear in In re Directives that the proper analytical approach to Fourth Amendment
reasonableness involves "balanc[ing] the interests at stake" under the "totality of the
circumstances" presented. In re Directives at 20. That approach requires the Court to weigh the
degree to which the government's implementation of the applicable targeting and minimization
procedures, viewed as whole, serves its important national security interests against the degree of
intrusion on Fourth Amendment-protected interests that results from that implementation. See
id. at 19-20.

After assessing the FBI's querying practices under the totality of circumstances, the Court
denies to deviate from its prior decisions. As discussed above, the querying provisions of the
FBI Minimization Procedures are applied only to information that has been acquired following
application of the NSA Targeting Procedures. Those procedures require that before tasking a
selector for collection, NSA first take steps to determine that the user of the selector is a non-
United States person who is reasonably believed to be located outside the United States and that
he or she is expected to possess, receive, or communicate foreign intelligence information. See
NSA Targeting Procedures at 4. These requirements direct the government's acquisitions toward
communications that are likely to yield foreign intelligence information.

Moreover, the purpose of permitting queries designed to elicit evidence of ordinary crimes is not entirely unconnected to foreign intelligence. Such queries are permitted in part to ensure that the FBI does not fail to identify the foreign-intelligence significance of information in its possession. One of the main criticisms of the government following the attacks of September 11, 2001, was its failure to identify and appropriately distribute information in its possession that could have been used to disrupt the plot. Although the queries at issue here are designed to find and extract evidence of crimes believed to be unrelated to foreign intelligence, such queries may nonetheless elicit foreign intelligence information, particularly since the Section 702 collection is targeted against persons believed to possess, receive, or communicate such information. See NSA Targeting Procedures at 4. A query designed to find and extract data regarding a [REDACTED] plot, for example, might reveal a previously unknown connection to persons believed to be funding terrorist operations on behalf of [REDACTED]. See October 20 Transcript at 20-21. Such unexpected connections may arise only rarely, but when they do arise, the foreign intelligence value of the information obtained could be substantial.

With respect to the intrusiveness of the querying process, the FBI Minimization Procedures impose substantial restrictions on the use and dissemination of information derived from queries. In the event that a query produces a positive hit on Section 702-acquired information, the query results can only be viewed by FBI personnel who are appropriately trained and approved to handle such information and "only for the purpose of determining whether it reasonably appears to be foreign intelligence information, to be necessary to understand foreign
intelligence information or to assess its importance, or to be evidence of a crime." See FBI Minimization Procedures at 8, 12 n.4. Generally, other FBI personnel who have not been trained for and granted access to FISA-acquired information are not allowed to view the query results unless the information has first been determined to meet one of these standards. See FBI Minimization Procedures at 12 n.4. Information that is determined to meet one of those criteria can be retained for further investigation and analysis and may be disseminated only in accordance with additional restrictions. See id.; see also id. at 30-37. Before using FISA-acquired information for further investigation, analysis, or dissemination, the FBI must strike, or substitute a characterization for, information of or concerning a United States person, including that person’s identity, if it does not reasonably appear to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime. See id. at 9.

Furthermore, it must be noted that only a subset of the information acquired by the government pursuant to Section 702 is subject to queries by the FBI. The FBI acquires only a “small portion” of the unminimized Section 702 collection. See October 20 Transcript at 29-30; PCLOB Report at 161 n.571 (Separate Statement By Board Members Rachel Brand and Elisebeth Collins Cook) (citing Letter from Deirdre M. Walsh, Director of Legislative Affairs, to Hon. Ron Wyden, United States Senate (June 27, 2014)). The FBI only receives collection on tasked facilities that are deemed to be relevant to an open FBI investigation. See October 20 Transcript at 30. Moreover, the FBI does not receive any unminimized information acquired through NSA’s “upstream collection” under Section 702, a form of collection that is, on
balance, more likely than others to include non-target communications of United States persons and persons located in the United States that have no foreign intelligence value. See [redacted]. Memorandum Opinion issued on November 30, 2011, at 6.

Finally, according to the government, FBI queries designed to elicit evidence of crimes unrelated to foreign intelligence rarely, if ever, produce responsive results from the Section 702-acquired data. See PCLOB Report at 59-60; id., at 162 (Separate Statement of Board Members Brand and Cook). Hence, the risk that the results of such a query will be viewed or otherwise used in connection with an investigation that is unrelated to national security appears to be remote, if not entirely theoretical. The Court is not prepared to find a constitutional deficiency based upon a hypothetical problem. Nevertheless, to reassure itself that this risk assessment is valid, the Court will require the government to report any instance in which FBI personnel receive and review Section 702-acquired information that the FBI identifies as concerning a United States person in response to a query that is not designed to find and extract foreign intelligence information. See page 78 below.

In light of the foregoing, the Court concludes that the querying provisions of the FBI Minimization Procedures strike a reasonable balance between the privacy interests of United States persons and persons in the United States, on the one hand, and the government’s national security interests, on the other. The FBI’s use of those provisions to conduct queries designed to return evidence of crimes unrelated to foreign intelligence does not preclude the Court from concluding that taken together, the targeting and minimization procedures submitted with the
2015 Certifications are consistent with the requirements of the Fourth Amendment.

E. **The Compliance and Implementation Issues Reported by the Government Do Not Preclude a Finding that the Targeting and Minimization Procedures Comply With Statutory Requirements and the Fourth Amendment**

As noted above at pages 6-7, the FISC examines the government’s implementation of, and compliance with, the targeting and minimization procedures as part of assessing whether those procedures comply with the applicable statutory (and Fourth Amendment) requirements.

In conducting this assessment, the Court is mindful that the controlling norms are ones of reasonableness, not perfection. This distinction is particularly important in the context of a large and complex endeavor such as the government’s implementation of Section 702. While in absolute terms, the scope of acquisitions under Section 702 is substantial, the acquisitions are not conducted in a bulk or indiscriminate manner. Rather, they are effected through discrete targeting decisions for individual selectors. Each targeting decision requires

---

24 See Section 1881a(d)(1) (requiring targeting procedures that are “reasonably designed” to limit targeting to “persons reasonably believed to be located outside the United States” and to “prevent the intentional acquisition” of communications to which all parties are known to be in the United States); Section 1801(h)(1) (requiring minimization procedures that are “reasonably designed” to minimize acquisition and retention, and to prohibit dissemination, of information concerning United States persons, consistent with foreign intelligence needs); United States v. Knights, 534 U.S. 112, 118 (2001) (“The touchstone of the Fourth Amendment is reasonableness . . .”).

25 For example, the NSA reports that, “on average, approximately [redacted] individual facilities” were tasked for acquisition “at any given time between June 1 and August 31, 2015.” Quarterly Report to the FISC Concerning Compliance Matters Under Section 702 of FISA, submitted on September 18, 2015, at 1 (footnote omitted) (“September 18, 2015 Compliance Report”). Facilities tasked for acquisition include [redacted].” Id. at 1 n.1. “Additionally, between June 1 and August 31, 2015, the [FBI] reports that it received and processed approximately [redacted] (continued...)
application of the pre-tasking provisions of the applicable targeting procedures. See NSA Targeting Procedures at 1-6; FBI Targeting Procedures at 1-3. For each selector while it is subject to tasking, there are post-tasking requirements designed to ascertain, for example, whether its targeted user has entered the United States. See NSA Targeting Procedures at 6-8. And pursuant to the minimization procedures, there are detailed rules concerning the retention, use, and dissemination of information obtained pursuant to Section 702. See NSA Minimization Procedures at 3-16; FBI Minimization Procedures at 5-33; CIA Minimization Procedures at 1-9.

Given the number of decisions and volume of information involved, it should not be surprising that occasionally errors are made. Moreover, the government necessarily relies on processes in performing post-tasking checks, see, e.g., August 30, 2013 Opinion at 7-9, and in acquiring, routing, storing, and when appropriate purging Section 702 information. See, e.g., April 7, 2009 Opinion at 17-22. Because of factors such as changes in communications technology or inadvertent error, these processes do not always function as intended.

It is apparent to the Court that the implementing agencies, as well as ODNI and the National Security Division ("NSD") of DOJ devote substantial resources to their compliance and oversight responsibilities under Section 702. With relatively few exceptions – one of which is

35(...continued)

36 Indeed, during the past year, NSD has provided the Court with a very detailed overview of its and ODNI's oversight efforts with respect to the Intelligence Community's implementation of Section 702. In July 2014, PCLOB recommended that the government provide the Court with random samples of tasking sheets and (NSA's and CIA's) United States person query terms to assist the Court's consideration of Section 702 certifications. PCLOB (continued...)
discussed in detail below – instances of non-compliance are identified promptly and appropriate remedial actions are taken, to include purging information that was improperly obtained or otherwise subject to destruction requirements. Accordingly, the Court’s overall assessment of the implementation of, and compliance with, the targeting and minimization procedures permits a finding that the these procedures, as implemented, satisfy the applicable statutory requirements. Nonetheless, the Court believes it is useful to discuss the following aspects of implementation and, in some respects, to direct the government to provide additional information.

1. The FBI’s Non-compliance With Attorney-Client Minimization Procedures

FISA’s definition of minimization procedures at Section 1801(h) does not, by its terms, afford any special protection to communications subject to the attorney-client privilege. Nevertheless, as discussed above, the minimization procedures under review have specific rules for handling attorney-client communications. See NSA Minimization Procedures at 10; FBI Minimization Procedures at 12-17, 29-30; CIA Minimization Procedures at 5-7. Because the FBI

36 (...continued)
Report at 141 (Recommendation 4). The government adopted this recommendation, and in January 2015 it provided the Court’s legal staff with an extensive briefing on its oversight activities, as well as sample tasking sheets and query terms. The government offered to make additional tasking sheets and query terms available to the Court. At the Court’s request, the government provided an overview of its Section 702 oversight efforts to all of the Court’s judges in May 2015, which included a review of sample tasking sheets. These briefings confirmed the Court’s earlier understanding that the government’s oversight efforts with respect to Section 702 collection are robust.

37 FISA does provide that “[n]o otherwise privileged communication obtained in accordance with, or in violation of, the provisions of [FISA] shall lose its privileged character.” 50 U.S.C. § 1806(a).
has law enforcement responsibilities and often works closely with prosecutors in criminal cases, its procedures have detailed requirements for cases in which a target is known to be charged with a federal crime. Unless otherwise authorized by the NSD, the FBI must establish a separate review team whose members “have no role in the prosecution of the charged criminal matter” to conduct the initial review of such a target’s communications. FBI Minimization Procedures at 13. When that review team identifies a privileged communication concerning the charged criminal matter, “the original record or portion thereof containing that privileged communication” is sequestered with the FISC and other copies are destroyed (save only any electronic version retained as an archival backup, access to which is restricted). Id. As discussed above, the FBI Minimization Procedures contain new provisions designed to further enhance the protection of attorney-client privileged communications. See FBI Minimization Procedures at 17-18.

At the time the Court was considering the 2014 Certifications, the government had identified [redacted] instances, discovered in the preceding six months, in which FBI case agents knew that persons targeted under Section 702 faced federal criminal charges, but had not established the required review teams. See August 26, 2014 Opinion at 35-36. The government generally attributed those instances to individual failures or confusion, rather than a “systematic issue.” Id. The Court’s Memorandum Opinion and Order issued in connection with the 2014 Certifications noted that one would expect the number of Section 702 targets charged with federal crimes to be fairly small, given that these targets are reasonably believed to be non-United States persons located outside of the United States Id. at 36. Accordingly, the Court noted that [redacted] then-recent
cases in which the FBI had not established the required review teams seemed to represent a potentially significant rate of non-compliance. Id. In light of this, the Court required, among other things, that the government make a subsequent written submission providing an assessment of the adequacy of the government’s training, guidance and oversight efforts with regard to the requirements for attorney-client privileged communications in the FBI Minimization Procedures. Id. at 42-43.

Since the Court approved the prior certifications in August 2014, the government has identified an additional [] instances in which FBI case agents knew that persons targeted under Section 702 faced federal criminal charges, but did not establish the required review teams.\textsuperscript{38} In notifying the Court of these instances, the government wrote that “[w]hile there have been isolated instances in which FBI personnel have not established review teams, the Government continues to believe that these were the result of individual failures or confusion and

not a systematic issue." Review of the individual instances indeed suggests that at least some FBI case agents are generally aware of the requirement for a review team when a Section 702 target is charged with a federal crime, but they are confused about the specific requirements of the FBI Minimization Procedures. In instances, for example, the relevant FBI case agents set up ad hoc or informal review teams wherein a case agent or a professional support employee not involved with the investigation was assigned to review communications for attorney-client privileged material prior to the case agent and team members reviewing the communications. In other instances, the relevant FBI case agents were generally aware of the requirement for a review team, but mistakenly believed that a review team is not required if the pertinent charging document is under seal or if the target is located outside of the United States.

The Court was extremely concerned about these additional instances of non-compliance, and at the October 8 Hearing on compliance matters, the Court asked the government to explain why there had been an additional instances of non-compliance in the past year. The government indicated that it had taken a two-pronged approach to improving compliance with these provisions of the minimization procedures during the preceding year. Id. at 3.

---

39 See December 19, 2015 Compliance Report at 83, 86; June 19, 2015 Compliance Report at 113; September 18, 2015 Compliance Report at 135; September 9 Preliminary Notice at 2; October 5 Preliminary Notice at 2; and October 8 Preliminary Notice at 2-3.


41 See October 8, 2015 Preliminary Compliance Notice at 2.

42 Transcript of Proceedings Held Before the Honorable Thomas F. Hogan at 3, October 8, 2015, ("October 8 Transcript").
First, the government indicated that at each of the approximately oversight reviews that NSD conducted at FBI field offices in the preceding year, NSD reminded individual case agents that a review team is required when a target is charged with a crime pursuant to the United States Code, both in individual meetings and general training sessions. Id. at 3-4. The government represented at the hearing that it was through some of these oversight reviews that it identified some of the instances of non-compliance reported to the Court during the past year. Id. at 4. In response to a question from the Court, the government also indicated that every FBI case agent is required to receive electronic training prior to receiving access to Section 702 collection, which includes training on the review team requirement. Id. at 6.

Second, the government reported that in August 2015, the FBI modified its system through which a case agent nominates a selector for collection of the Section 702 collection. Id. at 4-5. As a result of this modification, the system now asks the case agent whether the user of the relevant selector is charged with a federal crime. Id. at 4. If the agent indicates that the user is not currently charged, the system asks whether the agent expects the user to be charged in the future, and if so, when. Id. If the agent indicates that the user of a facility is currently charged or likely to be charged in the future, FBI Headquarters receives notice, and the Headquarters unit that manages Section 702 collection will reach out to the agent to ensure that a review team is established. Id. This tool also requires agents to update information about their Section 702 targets every 90 days. Id. The government represented that as a result of the modification to this system in August.
additional instances of non-compliance with the review team requirement were discovered by the time of the October 8 Hearing. Id. at 5.

Based on the measures described at the October 8 Hearing, the Court is satisfied that the government is taking appropriate measures to prevent further instances of non-compliance with the review team requirement. The Court understands that as a result of these modifications to the system – especially the requirement that case agents update information about their Section 702 targets every 90 days – remaining instances of non-compliance for currently-tasked selectors should be identified and remedied in the immediate future. The Court understands from post-hearing communications with the government that for de-tasked facilities, identifying remaining instances of non-compliance with the review team requirement will likely happen through NSD oversight reviews.

The Court does not believe that the recent instances of non-compliance with the review team requirement prevent a finding that the minimization procedures under review comply with the requirements of Section 1801(h) and the Fourth Amendment. However, the Court strongly encourages the government to try to identify any remaining instances of non-compliance as quickly as possible. The Court anticipates holding a follow-up hearing on Section 702 compliance matters in early 2016, at which time the Court will expect to receive an update on compliance with the review team requirements of the FBI Minimization Procedures. See page 79 below.

2. Failure of Access Controls in FBI’s...
acquired information under appropriately secure conditions that limit access to such information only to authorized users in accordance with” the minimization and other applicable FBI procedures. FBI Minimization Procedures at 5. Section III.B of the FBI Minimization Procedures further requires the FBI to grant access to raw Section 702-acquired information in a manner that is “consistent with the FBI’s foreign intelligence information-gathering and information-sharing responsibilities, . . . [p]ermitting access . . . only by individuals who require access in order to perform their job duties[,]” FBI Minimization Procedures at 7. It also requires users with access to raw FISA-acquired information to receive training on the minimization procedures. Id.
3.

On July 13, 2015, the Government filed an Update and Notice Regarding the National Security Agency’s (NSA) purge process for FISA-acquired information in Mission Management Systems (“July 13, 2015 Notice”). That notice indicated that the NSA had not been purging from its [redacted] database records associated with purged Section 702 collection. July 13, 2015 Notice at 3. The [redacted] database, and the question of whether the NSA had to purge the fruits of unlawful surveillance from this “mission management system,” were the subject of several opinions issued by the Court in 2010 and 2011. Because the analyses and
holdings of those opinions are relevant to the issue presented by the July 13, 2015 Notice, the Court will briefly review them.

Between June and August of 2010, the government filed several compliance notices indicating that the NSA had, under an authorization to conduct electronic surveillance [REDACTED], the Opinion and Order Regarding Fruits of Unauthorized Electronic Surveillance issued on December 10, 2010, at 1-2 ("December 2010 [REDACTED]"). The government proposed to retain the fruits of this unlawful surveillance insofar as they resided in the [REDACTED] database. Id. at 3. In making this proposal, the government argued that the Standard Minimization Procedures For Electronic Surveillance Conducted by the NSA ("NSA Electronic Surveillance SMPs") only applied to interceptions authorized by the Court and did not apply to the fruits of unlawful surveillance. Id. at 3-4. The government also argued that the criminal prohibition in 50 U.S.C. §1809(a)(2) only prohibits use or disclosure of unlawfully obtained information for investigative or analytic purposes.\(^{44}\) Id. at 6.

The Court issued an opinion in December 2010 rejecting the government's argument that the NSA Electronic Surveillance SMPs do not apply to over-collected information, noting instead that they appeared to require the destruction of at least some of the over-collected

\(^{44}\) Section 1809(a)(2) provides that "a person is guilty of an offense if he intentionally . . . discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized" by statute. 50 U.S.C. § 1809(a)(2).
information. Id. at 4-5. The Court also rejected the government’s argument that §1809(a)(2) only applies to use or disclosure of information for investigative or analytic purposes, but recognized a narrower implicit exception from this prohibition for use or disclosure of “the results of unauthorized surveillance [that] are needed to remedy past unauthorized surveillance or prevent similar unauthorized surveillance in the future.” Id. at 6-8. In recognizing this exception, the Court noted that:

Congress may be presumed not to have prohibited actions that are necessary to mitigate or prevent the harms at which Section 1809(a)(2) is addressed. But the application of this principle must be carefully circumscribed, so that it does not lead to an unjustified departure from the terms of the statute. “[W]hen Congress has spoken clearly, a court assessing the reach of the criminal statute must heed Congress’s intent as reflected in the statutory text.” Docket No. PR/TT Memorandum Opinion issued on at 113 (citing Huddleston v. United States, 415 U.S. 814, 831 (1974) (“Huddleston Opinion”).

Id. at 8 (emphasis in original). Because the Court could not ascertain whether or to what extent the over-collected information in the case might fall within this implicit exception for §1809(a)(2), the Court ordered the government to make a subsequent submission explaining why the particular information at issue in that case was needed to remedy past unauthorized surveillance or prevent similar unauthorized surveillance in the future. Id. at 8-9. After review of this submission and a hearing, the Court issued an opinion in May 2011 in which it found that the unauthorized collection in this case did not fall within the implicit narrow exception to §1809(a)(2), and that the NSA’s Electronic Surveillance SMPs required the destruction of the unauthorized collection in this case. Opinion and Order Requiring Destruction of Information Obtained by Unauthorized Electronic Surveillance issued on May 13, 2011, at 8-9 (“May 2011 Opinion”). In discussing the narrow exception to §1809(a)(2) in this opinion, the Court
noted the following:

[C]ourts should not attempt "to restrict the unqualified language of a [criminal] statute to the particular evil that Congress was trying to remedy -- even assuming that it is possible to identify that evil from something other than the text of the statute itself." Brogan v. United States, 522 U.S. 398, 403 (1998). . . . The exception recognized in the December 10, 2010 Opinion stands on narrower but firmer ground: that in limited circumstances, prohibiting use or disclosure of the results of unauthorized electronic surveillance would be "so 'absurd or glaringly unjust' . . . as to [call into] question whether Congress actually intended what the plain language of Section 1809(a)(2) "so clearly imports."

May 2011 [REDACTED] at 5 (citations omitted).

In light of the May 2011 [REDACTED], the Court was very surprised to learn from the July 13, 2015 Notice that the NSA had not been deleting from [REDACTED] Section 702 records placed on the NSA's Master Purge List ("MPL").[45] While that opinion dealt exclusively with Title I collection in a particular case, it would be difficult to conclude from its analysis and holding that Section 702 collection subject to purge should not also be deleted from [REDACTED]. Perhaps more disturbing and disappointing than the NSA's failure to purge this information for more than four years, was the government's failure to convey to the Court explicitly during that time that the NSA was continuing to retain this information in [REDACTED]. At the October 8, 2015 Hearing, the government acknowledged that it should have "more prominently and more fulsomely" explained the continued retention of this information in [REDACTED] to the Court, and that it should not have taken four years for the government to explain its proposed resolution of this issue to the Court. October 8 Transcript

[45] The July 13, 2015 Notice did indicate that the NSA had reconfigured [REDACTED] to delete prospectively records placed on the MPL, and that it would soon start purging from [REDACTED] historical records that had been placed on the MPL. July 13, 2015 Notice at 4.
TOP SECRET//SI/ORCON/NOFORN

at 26-27. As the Court explained to the government at the October 8 Hearing, it expects the government to comply with its heightened duty of candor in ex parte proceedings at all times. Candor is fundamental to this Court’s effective operation in considering ex parte submissions from the government, particularly in matters involving large and complex operations such as the implementation of Section 702.

On October 5, 2015, the government filed a supplemental notice regarding the National Security Agency’s purge process for FISA-acquired information (“October 5, 2015 Notice”). That notice indicated that since the filing of the July 13, 2015 Notice, NSA had removed from Section 702-acquired records that were marked as subject to purge. October 5, 2015 Notice at 2. However, on October 28, 2015, the government filed another supplemental notice regarding NSA’s purge processes (“October 28, 2015 Notice”) in which it indicated that a technical malfunction had rendered the aforementioned purges incomplete. October 28, 2015 Notice at 2. The October 28, 2015 Notice indicated that the NSA was “working to develop a technical solution to fix this system error in how effects purges and . . . investigating the amount of time it will take to develop and implement that fix.” Id. Given the government’s representation that the NSA is working to correct this error in the purging process, the Court does not believe the incomplete purges in this system prevent it from finding that the NSA Minimization Procedures comply with the requirements of Section 1801(h) and the Fourth Amendment. Nevertheless, the

46 More specifically, in effecting the purges, computer program had been searching for records using only identifiers on the MPL relevant to the information held in Id.
Court expects the government to resolve this issue expeditiously, and it anticipates receiving an update on this issue at a follow-up hearing on Section 702 compliance matters in early 2016. See page 79 below.

4. 

a. Introduction

As noted above, on July 13, 2015, the government filed a letter regarding the NSA’s purge processes for FISA-acquired information in NSA “mission management systems.” In addition to discussing [redacted], this letter also “serve[d] as notice pursuant to Rule 13(b) [of the FISC’s Rules of Procedure] of a compliance incident regarding FISA-acquired information subject to purge or age-off that is being retained in two of NSA’s compliance mission management systems, [redacted] and [redacted].” July 13, 2015 Notice at 2. More specifically, the letter noted that the government had “concluded that these two systems have been retaining data subject to purge and age-off in a manner that is potentially inconsistent with NSA’s FISA-related minimization procedures.” July 13, 2015 Notice at 5. Subsequent communications between the government and Court staff revealed that [redacted] and [redacted] may also have been retaining data, the use or disclosure of which could violate 50 U.S.C. § 1809(a)(2).

b. Relevant Legal Authorities

Analysis of the issues presented by the [redacted] and [redacted] disclosures requires consideration of the following legal authorities:
TOP SECRET//SI//ORCON//NOFORN

i. 50 U.S.C. § 1881a

As discussed above, Section 702, codified at 50 U.S.C. § 1881a, permits the Attorney General and the Director of National Intelligence to target non-United States persons reasonably believed to be located outside of the United States to acquire foreign intelligence information. 50 U.S.C. §1881a(a). Acquisitions under Section 702 must comply with a number of limitations, the first of which is that the government may not intentionally target any person known at the time of acquisition to be located in the United States 50 U.S.C. §1881a(b)(1). To effect this prohibition, the statute requires the adoption and use of targeting procedures that are reasonably designed to ensure that Section 702 acquisitions are limited to targeting persons reasonably believed to be located outside of the United States. 50 U.S.C. §1881a(c)(1)(A), (d)(1)(A).

Section 702 also prohibits the government from intentionally targeting a United States person reasonably believed to be outside of the United States, or acquiring any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States. 50 U.S.C. §1881a(b)(3),(4).

ii. NSA Targeting Procedures

The NSA Targeting Procedures contain a number of provisions designed to enable its compliance with the requirements and prohibitions of Section 702. Among the most important are Sections I and II. Section I of the procedures, which relates to the determination of whether a given target is a non-United States person reasonably believed to be located outside of the United States, provides that the NSA may

NSA Targeting Procedures at 1.
With respect to electronic communications, the procedures provide that the NSA may...

Section II of the NSA Targeting Procedures also provides that “after a person has been targeted for acquisition by NSA, NSA will conduct post-targeting analysis.” Id. at 6. For electronic communications, this analysis may include “[r]outinely checking all electronic communications tasked pursuant to these procedures...

...to determine if an electronic communications was accessed from inside the U.S.” Id.

iii. NSA Minimization Procedures

Section 2(e) of the NSA Minimization Procedures defines a foreign communication as one that has at least one communicant outside of the United States, and all other communications are considered domestic communications. NSA Minimization Procedures at 2. Section 3(d)(2) of the NSA Minimization Procedures also provides that “[a]ny communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be located outside the United States but is in fact located inside the United States at the time such communications were acquired ... will be treated as domestic communications ...[.]” NSA
Minimization Procedures at 9. Section 5 of the NSA Minimization Procedures provides that a domestic communication will be promptly destroyed upon recognition, unless the Director of NSA specifically determines that the sender or intended recipient had been properly targeted, and the communication satisfies one or more additional requirements (e.g., the communication is reasonably believed to contain significant foreign intelligence information). NSA Minimization Procedures at 12. Notwithstanding this destruction requirement, Section 5 also provides that "NSA may . . . use information derived from domestic communications for collection avoidance purposes, and . . . NSA may retain the communication from which such information is derived but shall restrict the further use or dissemination of the communication by placing it on the Master Purge List (MPL)." Id. at 13.

With respect to the length of time that NSA is permitted to retain Section 702 collection, Section 3(c) of the procedures provides, in relevant part, that 1) telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers may not be retained longer than five years from the expiration date of the certification authorizing the collection, unless the NSA specifically determines that each such communication meets retention standards in the procedures; 2) Internet transactions acquired through NSA’s upstream collection techniques may not be retained longer than two years from the expiration date of the certification authorizing the collection (unless NSA makes particular findings about the transaction); and 3) any Internet transactions acquired through NSA’s upstream collection techniques prior to to October 31, 2011, will be destroyed upon recognition. Id. at 7-8.
TOP SECRET//SI//ORCON//NOFORN

iv. 50 U.S.C. § 1809(a)(2)

As noted above, 50 U.S.C. § 1809(a)(2) provides that "a person is guilty of an offense if he intentionally . . . discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized" by statute. 50 U.S.C. § 1809(a)(2)

c. Background on [REDACTED] and their compliance with legal requirements

In the July 13, 2015 Notice, the government provided the following background information about [REDACTED] and [REDACTED] is a system analysts use to [REDACTED]. July 13, 2015 Notice at 6. Analysts most commonly use [REDACTED] as part of a determination of whether the facility can be properly tasked under Section 702. Id. This system provides information regarding [REDACTED]
is a tool used to perform post-tasking checks to identify indications that a Section 702 target may be located in the United States. Id. at 5. This tool

The July 13, 2015 Notice indicated that and were not compliant with several provisions of the NSA Minimization Procedures. With respect to , the notice indicated that it does not age off analyst query results within the time periods required by the NSA Minimization Procedures (i.e., within two years for upstream

47 As discussed in greater detail below, on October 21, 2015, the government—in response to an Order issued by this Court—filed the “Government’s Verified Response to the Court’s Order Dated October 14, 2015” (“Government’s October 21, 2015 Response”), in which it provided more information about and . This filing indicated that

Government’s October 21, 2015 Response at 3.

48 According to the July 13, 2015 Notice,
collection, and within five years for Internet communications acquired by or with the assistance of the FBI from Internet Service Providers), though it has aged-off all Section 702 upstream data acquired before October 31, 2011. July 13, 2015 Notice at 7. Id. The July 13, 2015 Notice indicated that the NSA does not age off records in [] in compliance with the NSA Minimization Procedures “because of the utility of these records for compliance and collection avoidance purposes.” Id. The notice further indicated that NSA compliance personnel use historical information – which presumably includes both information required to be aged-off and information associated with objects on the NSA’s MPL – to support the resolution of alerts (i.e., when a Section-702 tasked facility appears to have been accessed in the United States) and to respond to questions posed by NSD and ODNI in the course of those offices’ oversight of the Section 702 program. Id.

With respect to [], the July 13, 2015 Notice indicated that [] does not comply with the requirement in the NSA Minimization Procedures to age off telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers within five years of the expiration date of the certification authorizing
the collection. Id. at 6. Additionally, [redacted] is retained within [redacted] records even after the [redacted] have been purged from other NSA systems that directly support intelligence analysis pursuant to minimization requirements. Id. at 5. The notice indicated that instead of purging [redacted], certain fields within the records are made inaccessible to analysts and are visible only to a small number of personnel who have responsibility for system administration and compliance issues. Id. The notice indicated that the NSA has not been purging historical data or data associated with objects placed on the MPL from [redacted] "because compliance personnel use historical information [redacted] to resolve alerts." Id. By way of example, the notice described that if an [redacted] record, in combination with other analysis, indicates [redacted] that record can be used to resolve an alert (and de-task the relevant selector) more quickly in the event that the same target or a different target enters the United States and begins using a tasked selector [redacted]. Id. Additionally, [redacted] 42 The notice indicated that [redacted] is in compliance with the requirement to remove Section 702 information acquired from upstream collection within two years of the expiration date of the certification authorizing the collection. Id. Additionally, all Section 702 upstream Internet collection acquired prior to October 31, 2011, has been purged from [redacted] Id. 30 The Government's October 21, 2015 Response indicated that after a communication has been placed on the MPL, the following Section 702-acquired data is retained in [redacted] to permit more effective resolutions of future alerts: [redacted] Government's October 21, 2015 Response at 7.
Finally, the notice indicated that the resolution of prior alerts can provide context surrounding new alerts.

If this information was purged from the NSA would not have information about the prior alerts, which might result in an unnecessary delay in detasking selectors that would otherwise be purged. Id.

The Court was extremely concerned about the NSA's failure to comply with its minimization procedures — and potentially 50 U.S.C. § 1809(a)(2) — and questioned the government about these issues at the October 8 Hearing. Additionally, the Court issued an Order on October 14, 2015 ("October 14, 2015 Order"), requiring the government to make a written submission within a week describing how it justified under the NSA Minimization Procedures and § 1809(a)(2) the retention and use in the future of information otherwise subject to purge. On October 21, 2015, the government filed a timely response.

51 The Government's October 21, 2015 Response indicated that "since October 2013, NSA identified approximately instances in which prior alert information resulted in alerts being prioritized as 'urgent' and subject to priority review." Government's October 21, 2015 Response at 10.
d. Government’s Proposed Resolution of Identified Issues

The Government’s October 21, 2015 Response provided more detailed information about [redacted] and [redacted], some of which is noted above. It also indicated that the NSA will begin complying with some elements of its minimization procedures which it is currently violating. Finally, the submission included the government’s justifications under the NSA Minimization Procedures and 50 U.S.C. § 1809(a)(2) for the retention and use in [redacted] and [redacted] of other information otherwise subject to purge.

With respect to the NSA’s non-compliance with the age-off requirements in its minimization procedures, the Government’s October 21, 2015 Response indicated that the NSA will begin implementing the age-off time periods required by the procedures. Government’s October 21, 2015 Response at 13-14. With respect to the NSA’s retention in [redacted] and [redacted] of data associated with objects on the MPL, the government noted that despite the general destruction requirement for domestic communications, Section 5 of the NSA Minimization Procedures permits the NSA to use information derived from such communications for collection avoidance purposes.\footnote{Id. at 19. The government noted that the NSA has been retaining information in [redacted] and [redacted] that has been placed on the MPL for the very purpose of collection avoidance. Id.} The Government’s October 21, 2015

\footnote{Again, as noted above, Section 5 of the NSA Minimization Procedures states that “[n]otwithstanding the [general destruction requirement] above, . . . NSA may . . . use information derived from domestic communications for collection avoidance purposes, and may provide such information to the FBI and CIA for collection avoidance purposes. NSA may retain the communication from which such information is derived but shall restrict the further use or dissemination of the communication by placing it on the Master Purge List[.]” NSA Minimization Procedures at 13.}
Response also argued that keeping information in these systems that has been placed on the MPL supports the NSA’s obligations under Sections I and II of the NSA Targeting Procedures. Id. at 5, n.3, and 8, n.9. As described above, those provisions require the NSA to conduct pre- and post-tasking checks on Section 702 selectors by checking its data repositories to determine a target’s location. Id. The government noted that “foreignness determinations, both pre-tasking and post-tasking, are a fundamental element of Section 702’s statutory scheme” and “contribute significantly to the Fourth Amendment reasonableness of Section 702 collection.” Id. at 17.

Notwithstanding the government’s argument that retention of information on the MPL in [blacked out] and [blacked out] is consistent with the NSA’s procedures, the government indicated that it plans to modify its treatment of information collected under FISA and placed on the MPL to better ensure that such information is only used for collection avoidance. Id. at 14. Specifically, the government indicates that for [blacked out], if the underlying data is subject to purge, NSA will delete the underlying data from [blacked out] and analysts will only be able to access FISA-acquired or derived information in the following specific fields: [blacked out]

[blacked out]. As part of the query response, analysts will also receive notice that the evidence supporting the foreignness determination has been purged from [blacked out]. Id. at Attachment A.

With respect to [blacked out], the government indicated that going forward, if the underlying data is subject to purge, NSA will limit access to FISA-acquired or derived
The government’s submission noted that access to this information will be restricted to compliance and technical personnel, and intelligence analysts will only see a notice indicating that the information has been purged. Id. Again, the government noted that altering the way in which it treats information collected under FISA and placed on the MPL will further ensure that this information is only used for collection avoidance. Id.

The Court is persuaded by the government’s argument that Section 5 of the NSA Minimization Procedures does not prohibit the NSA from keeping data in and that is derived from domestic communications placed on the MPL for the purpose of collection avoidance. The Court also appreciates the NSA’s plan to modify its treatment of Section 702-acquired information in and that has been placed on the MPL, to further ensure that it is only used for collection avoidance. Accordingly, the information that remains of concern to the Court – at least insofar as the NSA’s compliance with its targeting and minimization procedures is concerned – is what the Court assesses to be the much smaller categories of Section 702-acquired information in and that have been placed on the MPL because of other destruction requirements under the NSA Targeting and Minimization Procedures. Examples would be incidentally acquired communications of or concerning United States persons that are clearly not relevant to the authorized purpose of the
acquisition or that do not contain evidence of a crime which may be disseminated under the minimization procedures (see Section 3(b)(1) of NSA Minimization Procedures); attorney-client communications that do not contain foreign intelligence information or evidence of a crime (see Section 4(a) of NSA Minimization Procedures); and any instances in which the NSA discovers that a United States person or a person not reasonably believed to be outside the United States at the time of targeting has been intentionally targeted under Section 702 (see Section IV of the NSA Targeting Procedures). The Court is directing the government to report on 1) how the NSA plans to comply with its targeting and minimization procedures with respect to these other categories of information in [redacted] and [redacted], or alternatively, 2) how the retention and use of these other categories of information in [redacted] and [redacted] comports with the NSA’s targeting and minimization procedures. See page 78 below. The Court also expects to hear from the government on this issue at the aforementioned follow-up hearing on Section 702 compliance matters in early 2016.

The other issue the Court directed the government to report on in its October 14, 2015 Order was how the government justified under 50 U.S.C. § 1809(a)(2) the retention and use in [redacted] and [redacted] of information otherwise subject to purge. As noted above, § 1809(a)(2) states that “a person is guilty of an offense if he intentionally . . . discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized” by statute. 50 U.S.C. § 1809(a)(2). Accordingly, a violation of § 1809(a)(2) must involve the intentional disclosure or use of information that is obtained through activity that meets the
definition of "electronic surveillance;"\textsuperscript{53} that activity must have been unauthorized; and the use or disclosure must be made with at least reason to know it was unauthorized.\textsuperscript{54}

The plain language of § 1809(a)(2) does not require the NSA to search for and identify information in \underline{[redacted]} and \underline{[redacted]} that may be subject to the criminal prohibition. It similarly does not require the NSA to destroy information in these systems that is subject to § 1809(a)(2). It does, however, prohibit the NSA from intentionally disclosing or using information under the circumstances described above. Therefore, when the NSA knows or has reason to know that a piece of information was acquired through an unauthorized electronic surveillance, it has an affirmative statutory obligation to refrain from disclosing or using it.

Notably, this Court has previously stated that the collection of "roamer communications" does not generally violate Section 702. Specifically, in the September 4, 2008 Opinion referenced above, the Court stated the following:

\textsuperscript{53} It is worth noting that 50 U.S.C. § 1827 contains analogous criminal prohibitions related to physical search, which could include the acquisition of stored data under Section 702.

\textsuperscript{54} With respect to this knowledge element, the Court has previously stated the following:

When it is not known, and there is no reason to know, that a piece of information was acquired through electronic surveillance that was not authorized by the Court's prior orders, the information is not subject to the criminal prohibition in Section 1809(a)(2). Of course, government officials may not avoid the strictures of Section 1809(a)(2) by cultivating a state of deliberate ignorance when reasonable inquiry would establish that information was indeed obtained through unauthorized electronic surveillance. \textit{See e.g., United States v. Whitehall}, 532 F.3d 746, 751 (8th Cir.) (where "failure to investigate is equivalent to 'burying one's head in the sand,'" willful blindness may constitute knowledge), \textit{cert. denied}, 129 S. Ct. 610 (2008).

\textbf{[redacted]} Opinion at 115.
There may be cases where, after properly applying the targeting procedures, the government reasonably believes at the time it acquires a communication that a target is a non-U.S. person outside the United States, when in fact the target is a U.S. person and/or is in the United States. The acquisition of such communications is properly authorized under Section 1881a notwithstanding the fact that the government is prohibited from intentionally targeting U.S. persons or persons inside the United States, or intentionally acquiring a communication when it is known that all parties thereto are inside the United States.

September 4, 2008 Opinion at 26 (emphasis in original). Accordingly, the domestic communications that the NSA acquires when non-United States person targets who are reasonably believed to be outside of the United States are in fact in the United States are not subject to § 1809(a)(2), as their acquisition was authorized under Section 702.55

As noted above, the Court recognized a narrow, implicit exception to § 1809(a)(2) in the December 2010 hearing and December 2010 hearing at 8. Specifically, the Court recognized an exception for use or disclosure of the “results of unauthorized surveillance [that] are needed to remedy past unauthorized surveillance or prevent similar unauthorized surveillance in the future.” Id. The Court made clear that this exception applied to “actions that are necessary to mitigate or prevent the very harms at which Section 1809(a)(2) is addressed.” Id. (emphasis in original).

The government made clear at the October 8 Hearing that it has not parsed through the data in [redacted] and [redacted] to determine what portion of it is subject to § 1809(a)(2).

55 A different situation would be presented if the NSA failed to detask a Section-702 tasked selector after it knew the user entered the United States. In this case, the ongoing collection of “roamer communications” would exceed the authorization to acquire communications under Section 702. See 50 U.S.C. § 1881a(a) (providing for authorization of “the targeting of persons reasonably believed to be located outside the United States”).
October 8 Transcript at 30. The government made a general argument in its written submission, however, that the retention and use in and of information that is otherwise subject to purge falls within the narrow, implicit exception to § 1809(a)(2) recognized in the December 2010 discussed above. Government’s October 21, 2015 Response at 21, 25. The Government’s October 21, 2015 Response repeatedly emphasized that the retention of information in and that has been placed on the MPL plays a significant role in preventing unauthorized surveillance in the future. See e.g., Government’s October 21, 2015 Response at 22-23, 25-27. While the Court finds it plausible that some information in and that is otherwise subject to purge may fall within the Court’s recognized exception to § 1809(a)(2), the Court is simply not in a position to ascertain what portion of that information meets the standard for the narrow exception. As described in the May 2011 the determination of whether the use or disclosure of unauthorized electronic surveillance falls within the exception to § 1809(a)(2) is a fact-driven assessment and involves an analysis of whether the use or disclosure of that specific information is “necessary to avoid similar instances of over-collection (e.g., by identifying and remedying a technical malfunction) or to remedy a prior over-collection (e.g., by aiding the identification of over-collected information in various storage systems).” May 2011 at 4-5. The Government’s October 21, 2015 Response argued that a more programmatic or categorical approach to the exception is warranted in the context of Section 702 collection. Government’s October 21, 2015 Response at 23-24, 27. That may be correct, but on the current record, the government has not made a persuasive case that all of the information that it wants to retain in
and falls within this exception. In these circumstances, the Court simply cannot conclude whether or not the government’s proposed course of action is wholly consistent with § 1809(a)(2). Nor does the Court have the authority to permit violations of § 1809(a)(2), even when they are de minimis. 56

In summary, it is likely that most Section 702 information in and that is otherwise subject to purge pertains to roamer communications, and therefore may be retained under the NSA Minimization Procedures for collection avoidance purposes and generally does not implicate § 1809(a)(2). Other Section 702 information that the government proposes to retain in and , notwithstanding generally

56 As the Court explained in the Opinion,

To be sure, this Court, like all other Article III courts, was vested upon its creation with certain inherent powers. See In re Motion for Release of Court Records, 526 F. Supp. 2d 484, 486 (FISA Ct. 2007); see also Chambers v. NASCO, Inc., 501 U.S. 32, 43 (1991) (“It has long been understood that [c]ertain implied powers must necessarily result to our Courts of justice from the nature of the their institution . . . “). It is well settled, however, that the exercise of such authority “is invalid if it conflicts with constitutional or statutory provisions.” Thomas v. Arn, 474 U.S. 140, 148 (1985). And defining crimes is not among the inherent powers of the federal courts; rather, federal crimes are defined by Congress and are solely creatures of statute. Bousley v. United States, 523 U.S. 614, 620-21 (1998); United States v. Hudson, 11 U.S. (7 Cranch) 32, 34 (1812). Accordingly, when Congress has spoken clearly, a court assessing the reach of a criminal statute must heed Congress’s intent as reflected in the statutory text. See, e.g., Huddleston v. United States, 415 U.S. 814, 831 (1974). The plain language of Section 1809(a)(2) makes it a crime for any person, acting under color of law, intentionally to use or disclose information with knowledge or reason to know that the information was obtained through unauthorized electronic surveillance. The Court simply lacks the power, inherent or otherwise, to authorize the government to engage in conduct that Congress has unambiguously prohibited.

Opinion at 113 (footnote omitted).
applicable purge requirements, is limited in nature and also would be used for collection
avoidance and other compliance-related purposes. For these reasons, the Court does not believe
that the aforementioned issues related to [REDACTED] and [REDACTED] preclude a finding that
the NSA Targeting Procedures and Minimization Procedures, taken as a whole, comply with the
applicable statutory and Fourth Amendment requirements. The Court does expect, however, to
hear more from the government about how it is applying the destruction requirements of those
procedures to Section 702 information in [REDACTED] and [REDACTED] at the compliance
hearing to be held in early 2016. Finally, the Court cannot find, at least on the current record,
that the information the government proposes to retain in [REDACTED] and [REDACTED] falls
entirely within the implicit exception to § 1809(a)(2)'s prohibition on disclosure and use.

IV. CONCLUSION

For the foregoing reasons, the Court finds that: (1) the 2015 Certifications, as well as the
certifications in the Prior 702 Dockets as amended by the 2015 Certifications, contain all the
required statutory elements; (2) the targeting and minimization procedures to be implemented
regarding acquisitions conducted pursuant to the 2015 Certifications comply with 50 U.S.C.
§1881a(d)-(e) and are consistent with the requirements of the Fourth Amendment; and (3) the
minimization procedures to be implemented regarding information acquired under prior Section
702 certifications comply with 50 U.S.C. §1881a(d)-(e) and are consistent with the requirements
of the Fourth Amendment. Orders approving the certifications, amended certifications, and use
of the accompanying procedures are being entered contemporaneously herewith.

For the reasons discussed above, it is HEREBY ORDERED as follows:
1. The government shall submit a report to the Court by December 18, 2015, describing
a) how the NSA plans to comply with its targeting and minimization procedures with respect to
the categories of information in [redacted] and [redacted] that are identified on pages 71-72
of this opinion, or alternatively, b) how the retention and use of the aforementioned categories of
information in [redacted] and [redacted] comports with the NSA’s targeting and
minimization procedures.

2. The government shall promptly submit in writing a report describing each instance in
which NSA or CIA invokes the provision of its minimization procedures stating that “[n]othing
in these procedures shall prohibit the retention, processing, or dissemination of information
reasonably necessary to comply with specific constitutional, judicial, or legislative mandates.”
See NSA Minimization Procedures at 1; CIA Minimization Procedures at 4-5. Each such report
should describe the circumstances of the deviation from the procedures and identify the specific
mandate on which the deviation was based.

3. The government shall promptly submit in writing a report concerning each instance
after December 4, 2015, in which FBI personnel receive and review Section 702-acquired
information that the FBI identifies as concerning a United States person in response to a query
that is not designed to find and extract foreign intelligence information. The report should
include a detailed description of the information at issue and the manner in which it has been or
will be used for analytical, investigative, or evidentiary purposes. It shall also identify the query
terms used to elicit the information and provide the FBI’s basis for concluding that the query is
consistent with the applicable minimization procedures.
4. The government shall provide substantive updates on each of the four compliance issues discussed herein at a hearing to be held on January 27, 2016, at 11 A.M.

ENTERED this ___ day of November, in [redacted].

Thomas F. Hogan
THOMAS F. HOGAN
Judge, United States Foreign Intelligence Surveillance Court
ORDER

For the reasons stated in the Memorandum Opinion and Order issued contemporaneously herewith, and in reliance upon the entire record in this matter, the Court finds, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that the certifications referenced above contain all the required statutory elements and that the targeting procedures and minimization procedures approved for use in connection with those certifications are consistent with the requirements of 50 U.S.C. §1881a(d)-(e) and with the Fourth Amendment.

Accordingly, it is hereby ORDERED, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that the certifications and the use of such procedures are approved.

ENTERED this __ day of November 2015, in

[Signature]

THOMAS F. HOGAN
Judge, United States Foreign Intelligence Surveillance Court

I, [Name], Chief Deputy Clerk, FISC, certify that this document is a true and correct copy of the original
Privacy and Civil Liberties Oversight Board

Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

JULY 2, 2014
Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

JULY 2, 2014
Privacy and Civil Liberties Oversight Board

David Medine, Chairman

Rachel Brand

Elisebeth Collins Cook

James Dempsey

Patricia Wald
Analysis of Treatment of Non-U.S. Persons ................................................................. 98

Part 5 POLICY ANALYSIS .................................................................................................. 103

Value of the Section 702 Program ........................................................................... 104

Privacy and Civil Liberties Implications of the Section 702 Program .......... 111

Part 6 RECOMMENDATIONS ............................................................................................ 134

Part 7 CONCLUSION ........................................................................................................ 149

ANNEXES .......................................................................................................................... 150

A. Separate Statement by Chairman David Medine and
   Board Member Patricia Wald .......................................................................................... 151

B. Separate Statement by Board Members Rachel Brand and
   Elisebeth Collins Cook .................................................................................................... 161

C. July 9, 2013 Workshop Agenda and Link to Workshop Transcript ............... 166

D. November 4, 2013 Hearing Agenda and Link to Hearing Transcript .......... 169

E. March 19, 2014 Hearing Agenda and Link to Hearing Transcript ............... 172

F. Request for Public Comments on Board Study .................................................... 175

G. Reopening the Public Comment Period ................................................................. 177

H. Index to Public Comments on www.regulations.gov ...................................... 178
Part 1:
INTRODUCTION

I. Background

Shortly after the Privacy and Civil Liberties Oversight Board (“PCLOB” or “Board”) began operation as a new independent agency, Board Members identified a series of programs and issues to prioritize for review. As announced at the Board’s public meeting in March 2013, one of these issues was the implementation of the Foreign Intelligence Surveillance Act Amendments Act of 2008.\(^1\)

Several months later, in June 2013, two classified National Security Agency (“NSA”) collection programs were first reported about by the press based on unauthorized disclosures of classified documents by Edward Snowden, a contractor for the NSA. Under one program, implemented under Section 215 of the USA PATRIOT Act, the NSA collects domestic telephone metadata (i.e., call records) in bulk. Under the other program, implemented under Section 702 of the Foreign Intelligence Surveillance Act (“FISA”), the government collects the contents of electronic communications, including telephone calls and emails, where the target is reasonably believed to be a non-U.S. person\(^2\) located outside the United States.

A bipartisan group of U.S. Senators asked the Board to investigate the two NSA programs and provide an unclassified report.\(^3\) House Minority Leader Nancy Pelosi subsequently asked the Board to consider the operations of the Foreign Intelligence Surveillance Court (“FISA court”).\(^4\) Additionally, the Board met with President Obama, who asked the Board to “review where our counterterrorism efforts and our values come into


\(^2\) Under the statute, the term “U.S. persons” includes United States citizens, United States permanent residents, and virtually all United States corporations.


tension.” In response to the requests from Congress and the President, the Board began a comprehensive study of the two NSA programs. The Board held public hearings and met with the Intelligence Community and the Department of Justice, White House, and congressional committee staff, privacy and civil liberties advocates, academics, trade associations, and technology and communications companies.

During the course of this study, it became clear to the Board that each program required a level of review that was best undertaken and presented to the public in a separate report. As such, the Board released a report on the Section 215 telephone records program and the operation of the FISA court on January 23, 2014. Subsequently, the Board held an additional public hearing and continued its study of the second program. Now, the Board is issuing the current report, which examines the collection of electronic communications under Section 702, and provides analysis and recommendations regarding the program’s implementation.

The Section 702 program is extremely complex, involving multiple agencies, collecting multiple types of information, for multiple purposes. Overall, the Board has found that the information the program collects has been valuable and effective in protecting the nation’s security and producing useful foreign intelligence. The program has operated under a statute that was publicly debated, and the text of the statute outlines the basic structure of the program. Operation of the Section 702 program has been subject to judicial oversight and extensive internal supervision, and the Board has found no evidence of intentional abuse.

The Board has found that certain aspects of the program’s implementation raise privacy concerns. These include the scope of the incidental collection of U.S. persons’ communications and the use of queries to search the information collected under the program for the communications of specific U.S. persons. The Board offers a series of policy recommendations to strengthen privacy safeguards and to address these concerns.

II. Study Methodology

In order to gain a full understanding of the program’s operations, the Board and its staff received multiple briefings on the operation of the program, including the technical

---


details and procedural rules that govern its implementation. The Board appreciates the responsiveness and open lines of communication that have been established with members of the Intelligence Community and the Department of Justice. These have enabled the Board to understand the operation of this complex program, and to fully consider the practical impact that the Board’s recommendations will have.

Building upon the previous public hearings held in July and November 2013, the Board held an additional public hearing on March 19, 2014, focused exclusively on the Section 702 program. This hearing was comprised of three panels. The first panel consisted of government representatives who provided the government’s views on Section 702. The second panel consisted of academics and privacy advocates who addressed the legal issues related to Section 702, including both statutory and constitutional matters. The third panel consisted of representatives from private industry, academics, and human rights organizations who discussed the transnational and policy issues related to Section 702. Panelists, as well as the general public, were invited to submit written comments to the Board via www.regulations.gov.

Since the unauthorized disclosures that began in 2013, much of the information that the Intelligence Community has declassified and released has related to the Section 215 program. In the preparation of this Report, the Board worked with the Intelligence Community to seek further declassification of information related to the Section 702 program. Specifically, the Board requested declassification of additional facts for use in this Report. Consistent with the Board’s goal of seeking greater transparency where appropriate, the request for declassification of additional facts to be used in this Report was made in order to provide further clarity and education to the public about the Section 702 program. The Intelligence Community carefully considered the Board’s requests and has engaged in a productive dialogue with PCLOB staff. The Board greatly appreciates the diligent efforts of the Intelligence Community to work through the declassification process, and as a result of the process, many facts that were previously classified are now available to the public.

In the course of preparing and finalizing this Report, the Board met with staff from the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, as well as staff from the House and Senate Judiciary Committees, to discuss the Section 702 program and the Board’s preliminary recommendations. The Board also presented its preliminary recommendations to senior staff at the White House. In addition, the Board provided a draft of this Report to the Intelligence Community for classification review. While the Board’s report was subject to classification review, and while the Board

---

7 See Annex E.
8 See Annex H.
considered the Intelligence Community’s comments regarding the operation of the program to ensure accuracy, none of the changes resulting from that process affected the Board’s substantive analysis and recommendations.

III. Report Organization

This Report consists of six parts. After this introduction and the Executive Summary, Part 3 contains a factual narrative that explains the development of the Section 702 program and how the program currently operates. Part 4 consists of legal analysis, including the Board’s statutory and constitutional analyses, as well as a discussion of how the program affects the legal rights of non-U.S. persons. Part 5 examines the policy implications of the program, including an assessment of its efficacy and its effect on privacy, while Part 6 outlines and explains the Board’s recommendations.

The Board presents this Report in an effort to provide greater transparency and clarity to the public regarding the government’s activities with respect to the Section 702 program. The recommendations reflect the Board’s best efforts to protect the privacy and civil liberties of the public while considering legitimate national security interests. The Board welcomes the opportunity for further discussion of these pressing issues.
In 2008, Congress enacted the FISA Amendments Act, which made changes to the Foreign Intelligence Surveillance Act of 1978 (“FISA”). Among those changes was the addition of a new provision, Section 702 of FISA, permitting the Attorney General and the Director of National Intelligence to jointly authorize surveillance conducted within the United States but targeting only non-U.S. persons reasonably believed to be located outside the United States. The Privacy and Civil Liberties Oversight Board (“PCLOB”) began reviewing implementation of the FISA Amendments Act early in 2013, shortly after the Board began operations as an independent agency. The PCLOB has conducted an in-depth review of the program now operated under Section 702, in pursuit of the Board’s mission to review executive branch actions taken to protect the nation from terrorism in order to ensure “that the need for such actions is balanced with the need to protect privacy and civil liberties.” This Executive Summary outlines the Board’s conclusions and recommendations.

I. Overview of the Report

A. Description and History of the Section 702 Program

Section 702 has its roots in the President’s Surveillance Program developed in the immediate aftermath of the September 11th attacks. Under one aspect of that program, which came to be known as the Terrorist Surveillance Program (“TSP”), the President authorized interception of the contents of international communications from within the United States, outside of the FISA process. Following disclosures about the TSP by the press in December 2005, the government sought and obtained authorization from the Foreign Intelligence Surveillance Court (“FISA court”) to conduct, under FISA, the collection that had been occurring under the TSP. Later, the government developed a statutory framework specifically designed to authorize this collection program. After the enactment and expiration of a temporary measure, the Protect America Act of 2007, Congress passed the FISA Amendments Act of 2008, which included the new Section 702 of FISA. The statute

---


provides a procedural framework for the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information.

Section 702 permits the Attorney General and the Director of National Intelligence to jointly authorize surveillance targeting persons who are not U.S. persons, and who are reasonably believed to be located outside the United States, with the compelled assistance of electronic communication service providers, in order to acquire foreign intelligence information. Thus, the persons who may be targeted under Section 702 cannot intentionally include U.S. persons or anyone located in the United States, and the targeting must be conducted to acquire foreign intelligence information as defined in FISA. Executive branch authorizations to acquire designated types of foreign intelligence under Section 702 must be approved by the FISA court, along with procedures governing targeting decisions and the handling of information acquired.

Although U.S. persons may not be targeted under Section 702, communications of or concerning U.S. persons may be acquired in a variety of ways. An example is when a U.S. person communicates with a non-U.S. person who has been targeted, resulting in what is termed “incidental” collection. Another example is when two non-U.S. persons discuss a U.S. person. Communications of or concerning U.S. persons that are acquired in these ways may be retained and used by the government, subject to applicable rules and requirements. The communications of U.S. persons may also be collected by mistake, as when a U.S. person is erroneously targeted or in the event of a technological malfunction, resulting in “inadvertent” collection. In such cases, however, the applicable rules generally require the communications to be destroyed.

Under Section 702, the Attorney General and Director of National Intelligence make annual certifications authorizing this targeting to acquire foreign intelligence information, without specifying to the FISA court the particular non-U.S. persons who will be targeted. There is no requirement that the government demonstrate probable cause to believe that an individual targeted is an agent of a foreign power, as is generally required in the “traditional” FISA process under Title I of the statute. Instead, the Section 702 certifications identify categories of information to be collected, which must meet the statutory definition of foreign intelligence information. The certifications that have been authorized include information concerning international terrorism and other topics, such as the acquisition of weapons of mass destruction.

Section 702 requires the government to develop targeting and “minimization” procedures that must satisfy certain criteria. As part of the FISA court’s review and approval of the government’s annual certifications, the court must approve these procedures and determine that they meet the necessary standards. The targeting procedures govern how the executive branch determines that a particular person is reasonably believed to be a non-U.S. person located outside the United States, and that
targeting this person will lead to the acquisition of foreign intelligence information. The minimization procedures cover the acquisition, retention, use, and dissemination of any non-publicly available U.S. person information acquired through the Section 702 program.

Once foreign intelligence acquisition has been authorized under Section 702, the government sends written directives to electronic communication service providers compelling their assistance in the acquisition of communications. The government identifies or “tasks” certain “selectors,” such as telephone numbers or email addresses, that are associated with targeted persons, and it sends these selectors to electronic communications service providers to begin acquisition. There are two types of Section 702 acquisition: what has been referred to as “PRISM” collection and “upstream” collection.

In PRISM collection, the government sends a selector, such as an email address, to a United States-based electronic communications service provider, such as an Internet service provider (“ISP”), and the provider is compelled to give the communications sent to or from that selector to the government. PRISM collection does not include the acquisition of telephone calls. The National Security Agency (“NSA”) receives all data collected through PRISM. In addition, the Central Intelligence Agency (“CIA”) and the Federal Bureau of Investigation (“FBI”) each receive a select portion of PRISM collection.

Upstream collection differs from PRISM collection in several respects. First, the acquisition occurs with the compelled assistance of providers that control the telecommunications “backbone” over which telephone and Internet communications transit, rather than with the compelled assistance of ISPs or similar companies. Upstream collection also includes telephone calls in addition to Internet communications. Data from upstream collection is received only by the NSA: neither the CIA nor the FBI has access to unminimized upstream data. Finally, the upstream collection of Internet communications includes two features that are not present in PRISM collection: the acquisition of so-called “about” communications and the acquisition of so-called “multiple communications transactions” (“MCTs”). An “about” communication is one in which the selector of a targeted person (such as that person’s email address) is contained within the communication but the targeted person is not necessarily a participant in the communication. Rather than being “to” or “from” the selector that has been tasked, the communication may contain the selector in the body of the communication, and thus be “about” the selector. An MCT is an Internet “transaction” that contains more than one discrete communication within it. If one of the communications within an MCT is to, from, or “about” a tasked selector, and if one end of the transaction is foreign, the NSA will acquire the entire MCT through upstream collection, including other discrete communications within the MCT that do not contain the selector.

Each agency that receives communications under Section 702 has its own minimization procedures, approved by the FISA court, that govern the agency’s use,
retention, and dissemination of Section 702 data. Among other things, these procedures include rules on how the agencies may “query” the collected data. The NSA, CIA, and FBI minimization procedures all include provisions permitting these agencies to query data acquired through Section 702, using terms intended to discover or retrieve communications content or metadata that meets the criteria specified in the query. These queries may include terms that identify specific U.S. persons and can be used to retrieve the already acquired communications of specific U.S. persons. Minimization procedures set forth the standards for conducting queries. For example, the NSA’s minimization procedures require that queries of Section 702–acquired information be designed so that they are “reasonably likely to return foreign intelligence information.”

The minimization procedures also include data retention limits and rules outlining circumstances under which information must be purged. Apart from communications acquired by mistake, U.S. persons’ communications are not typically purged or eliminated from agency databases, even when they do not contain foreign intelligence information, until the data is aged off in accordance with retention limits.

Each agency’s adherence to its targeting and minimization procedures is subject to extensive oversight within the executive branch, including internal oversight within individual agencies as well as regular reviews conducted by the Department of Justice (“DOJ”) and the Office of the Director of National Intelligence (“ODNI”). The Section 702 program is also subject to oversight by the FISA court, including during the annual certification process and when compliance incidents are reported to the court. Information about the operation of the program also is reported to congressional committees. Although there have been various compliance incidents over the years, many of these incidents have involved technical issues resulting from the complexity of the program, and the Board has not seen any evidence of bad faith or misconduct.

B. Legal Analysis

The Board’s legal analysis of the Section 702 program includes an evaluation of whether it comports with the terms of the statute, an evaluation of the Fourth Amendment issues raised by the program, and a discussion of the treatment of non-U.S. persons under the program.

In reviewing the program’s compliance with the text of Section 702, the Board has assessed the operation of the program overall and has separately evaluated PRISM and upstream collection. On the whole, the text of Section 702 provides the public with transparency into the legal framework for collection, and it publicly outlines the basic

---

11 As described in Part 3 of this Report, the National Counterterrorism Center (“NCTC”) has some access to Section 702 data and therefore has its own minimization procedures as well. However, the NCTC’s role in processing and minimizing Section 702 data is limited.
structure of the program. The Board concludes that PRISM collection is clearly authorized by the statute and that, with respect to the “about” collection, which occurs in the upstream component of the program, the statute can permissibly be interpreted as allowing such collection as it is currently implemented.

The Board also concludes that the core of the Section 702 program — acquiring the communications of specifically targeted foreign persons who are located outside the United States, upon a belief that those persons are likely to communicate foreign intelligence, using specific communications identifiers, subject to FISA court-approved targeting rules and multiple layers of oversight — fits within the “totality of the circumstances” standard for reasonableness under the Fourth Amendment, as that standard has been defined by the courts to date. Outside of this fundamental core, certain aspects of the Section 702 program push the program close to the line of constitutional reasonableness. Such aspects include the unknown and potentially large scope of the incidental collection of U.S. persons’ communications, the use of “about” collection to acquire Internet communications that are neither to nor from the target of surveillance, and the use of queries to search for the communications of specific U.S. persons within the information that has been collected. With these concerns in mind, this Report offers a set of policy proposals designed to push the program more comfortably into the sphere of reasonableness, ensuring that the program remains tied to its constitutionally legitimate core.

Finally, the Board discusses the fact that privacy is a human right that has been recognized in the International Covenant on Civil and Political Rights (“ICCPR”), an international treaty ratified by the U.S. Senate, and that the treatment of non-U.S. persons in U.S. surveillance programs raises important but difficult legal and policy questions. Many of the generally applicable protections that already exist under U.S. surveillance laws apply to U.S. and non-U.S. persons alike. The President’s recent initiative under Presidential Policy Directive 28 on Signals Intelligence (“PPD-28”) will further address the extent to which non-U.S. persons should be afforded the same protections as U.S. persons under U.S. surveillance laws. Because PPD-28 invites the PCLOB to be involved in its implementation, the Board has concluded that it can make its most productive contribution in assessing these issues in the context of the PPD-28 review process.

C. Policy Analysis

The Section 702 program has enabled the government to acquire a greater range of foreign intelligence than it otherwise would have been able to obtain — and to do so quickly and effectively. Compared with the “traditional” FISA process under Title I of the

---

statute, Section 702 imposes significantly fewer limits on the government when it targets foreigners located abroad, permitting greater flexibility and a dramatic increase in the number of people who can realistically be targeted. The program has proven valuable in the government’s efforts to combat terrorism as well as in other areas of foreign intelligence. Presently, over a quarter of the NSA’s reports concerning international terrorism include information based in whole or in part on Section 702 collection, and this percentage has increased every year since the statute was enacted. Monitoring terrorist networks under Section 702 has enabled the government to learn how they operate, and to understand their priorities, strategies, and tactics. In addition, the program has led the government to identify previously unknown individuals who are involved in international terrorism, and it has played a key role in discovering and disrupting specific terrorist plots aimed at the United States and other countries.

The basic structure of the Section 702 program appropriately focuses on targeting non-U.S. persons reasonably believed to be located abroad. Yet communications of, or concerning, U.S. persons can be collected under Section 702, and certain features of the program implicate privacy concerns. These features include the potential scope of U.S. person communications that are collected, the acquisition of “about” communications, and the use of queries that employ U.S. person identifiers.

The Board’s analysis of these features of the program leads to certain policy recommendations.

The government is presently unable to assess the scope of the incidental collection of U.S. person information under the program. For this reason, the Board recommends several measures that together may provide insight about the extent to which communications involving U.S. persons or people located in the United States are being acquired and utilized.

With regard to the NSA’s acquisition of “about” communications, the Board concludes that the practice is largely an inevitable byproduct of the government’s efforts to comprehensively acquire communications that are sent to or from its targets. Because of the manner in which the NSA conducts upstream collection, and the limits of its current technology, the NSA cannot completely eliminate “about” communications from its collection without also eliminating a significant portion of the “to/from” communications that it seeks. The Board includes a recommendation to better assess “about” collection and a recommendation to ensure that upstream collection as a whole does not unnecessarily collect domestic communications.

The Report also assesses the impact of queries using “United States person identifiers.” At the NSA, for example, these queries can be performed if they are deemed “reasonably likely to return foreign intelligence information.” No showing of suspicion that
the U.S. person is engaged in any form of wrongdoing is required, but procedures are in place to prevent queries being conducted for improper purposes. The Board includes two recommendations to address the rules regarding U.S. person queries.

Overall, the Board finds that the protections contained in the Section 702 minimization procedures are reasonably designed and implemented to ward against the exploitation of information acquired under the program for illegitimate purposes. The Board has seen no trace of any such illegitimate activity associated with the program, or any attempt to intentionally circumvent legal limits. But the applicable rules potentially allow a great deal of private information about U.S. persons to be acquired by the government. The Board therefore offers a series of policy recommendations to ensure that the program appropriately balances national security with privacy and civil liberties.

II. Recommendations

A. Targeting and Tasking

**Recommendation 1:** The NSA’s targeting procedures should be revised to (a) specify criteria for determining the expected foreign intelligence value of a particular target, and (b) require a written explanation of the basis for that determination sufficient to demonstrate that the targeting of each selector is likely to return foreign intelligence information relevant to the subject of one of the certifications approved by the FISA court. The NSA should implement these revised targeting procedures through revised guidance and training for analysts, specifying the criteria for the foreign intelligence determination and the kind of written explanation needed to support it. We expect that the FISA court’s review of these targeting procedures in the course of the court’s periodic review of Section 702 certifications will include an assessment of whether the revised procedures provide adequate guidance to ensure that targeting decisions are reasonably designed to acquire foreign intelligence information relevant to the subject of one of the certifications approved by the FISA court. Upon revision of the NSA’s targeting procedures, internal agency reviews, as well as compliance audits performed by the ODNI and DOJ, should include an assessment of compliance with the foreign intelligence purpose requirement comparable to the review currently conducted of compliance with the requirement that targets are reasonably believed to be non-U.S. persons located outside the United States.

B. U.S. Person Queries

**Recommendation 2:** The FBI’s minimization procedures should be updated to more clearly reflect the actual practice for conducting U.S. person queries, including the frequency with which Section 702 data may be searched when making routine queries as part of FBI
assessments and investigations. Further, some additional limits should be placed on the FBI’s use and dissemination of Section 702 data in connection with non–foreign intelligence criminal matters.

**Recommendation 3:** The NSA and CIA minimization procedures should permit the agencies to query collected Section 702 data for foreign intelligence purposes using U.S. person identifiers only if the query is based upon a statement of facts showing that it is reasonably likely to return foreign intelligence information as defined in FISA. The NSA and CIA should develop written guidance for agents and analysts as to what information and documentation is needed to meet this standard, including specific examples.

**C. FISA Court Role**

**Recommendation 4:** To assist in the FISA court’s consideration of the government’s periodic Section 702 certification applications, the government should submit with those applications a random sample of tasking sheets and a random sample of the NSA’s and CIA’s U.S. person query terms, with supporting documentation. The sample size and methodology should be approved by the FISA court.

**Recommendation 5:** As part of the periodic certification process, the government should incorporate into its submission to the FISA court the rules for operation of the Section 702 program that have not already been included in certification orders by the FISA court, and that at present are contained in separate orders and opinions, affidavits, compliance and other letters, hearing transcripts, and mandatory reports filed by the government. To the extent that the FISA court agrees that these rules govern the operation of the Section 702 program, the FISA court should expressly incorporate them into its order approving Section 702 certifications.

**D. Upstream and “About” Collection**

**Recommendation 6:** To build on current efforts to filter upstream communications to avoid collection of purely domestic communications, the NSA and DOJ, in consultation with affected telecommunications service providers, and as appropriate, with independent experts, should periodically assess whether filtering techniques applied in upstream collection utilize the best technology consistent with program needs to ensure government acquisition of only communications that are authorized for collection and prevent the inadvertent collection of domestic communications.
Recommendation 7: The NSA periodically should review the types of communications acquired through “about” collection under Section 702, and study the extent to which it would be technically feasible to limit, as appropriate, the types of “about” collection.

E. Accountability and Transparency

Recommendation 8: To the maximum extent consistent with national security, the government should create and release, with minimal redactions, declassified versions of the FBI’s and CIA’s Section 702 minimization procedures, as well as the NSA’s current minimization procedures.

Recommendation 9: The government should implement five measures to provide insight about the extent to which the NSA acquires and utilizes the communications involving U.S. persons and people located in the United States under the Section 702 program. Specifically, the NSA should implement processes to annually count the following: (1) the number of telephone communications acquired in which one caller is located in the United States; (2) the number of Internet communications acquired through upstream collection that originate or terminate in the United States; (3) the number of communications of or concerning U.S. persons that the NSA positively identifies as such in the routine course of its work; (4) the number of queries performed that employ U.S. person identifiers, specifically distinguishing the number of such queries that include names, titles, or other identifiers potentially associated with individuals; and (5) the number of instances in which the NSA disseminates non-public information about U.S. persons, specifically distinguishing disseminations that includes names, titles, or other identifiers potentially associated with individuals. These figures should be reported to Congress in the NSA Director’s annual report and should be released publicly to the extent consistent with national security.

F. Efficacy

Recommendation 10: The government should develop a comprehensive methodology for assessing the efficacy and relative value of counterterrorism programs.
III. **Separate Statements**

Following the Board’s recommendations, the Report includes two separate statements.

**A. Separate Statement of Chairman David Medine and Board Member Patricia Wald**

Chairman David Medine and Member Patricia Wald wrote jointly to recommend requiring restrictions additional to those contained in Recommendation 3 with regard to U.S. person queries conducted for a foreign intelligence purpose. They also recommended that minimization procedures governing the use of U.S. persons’ communications collected under Section 702 should require the following:

1. No later than when the results of a U.S. person query of Section 702 data are generated, U.S. persons’ communications should be purged of information that does not meet the statutory definition of foreign intelligence information relating to U.S. persons. This process should be subject to judicial oversight.

2. Each U.S. person identifier should be submitted to the FISA court for approval before the identifier may be used to query data collected under Section 702, for a foreign intelligence purpose, other than in exigent circumstances or where otherwise required by law. The FISA court should determine, based on documentation submitted by the government, whether the use of the U.S. person identifier for Section 702 queries meets the standard that the identifier is reasonably likely to return foreign intelligence information as defined under FISA.

In addition, they wrote to further explain their views regarding Recommendation 2. Specifically, they believe that the additional limits to be placed on the FBI’s use and dissemination of Section 702 data in connection with non–foreign intelligence criminal matters should include the requirement that the FBI obtain prior FISA court approval before using identifiers to query Section 702 data to ensure that the identifier is reasonably likely to return information relevant to an assessment or investigation of a crime.

---

13 U.S. person communications may also be responsive to queries using non-U.S. person identifiers.

14 This review would not be necessary for queries seeking communications of U.S. persons who are already approved as targets for collection under Title I or Sections 703/704 of FISA and identifiers that have been approved by the FISA court under the “reasonable articulable suspicion” standard for telephony metadata under Section 215. It would also not be necessary if the query produces no results or the analyst purges all results from the given query as not containing foreign intelligence.

15 Subsequent queries using a FISA court–approved U.S. person identifier would not require court approval.
The statement also responds to the separate statement by Members Brand and Cook.

B. Separate Statement by Board Members Rachel Brand and Elisebeth Collins Cook

Board Members Rachel Brand and Elisebeth Collins Cook wrote separately to emphasize the Board’s unanimous bottom-line conclusion that the core Section 702 program is clearly authorized by Congress, reasonable under the Fourth Amendment, and an extremely valuable and effective intelligence tool. They further wrote to explain their proposal for FBI queries of Section 702 data, which would not place limitations on the FBI’s ability to include its FISA data within the databases *queried* in non–foreign intelligence criminal matters. They explain their view that querying information already in the FBI’s possession is a relatively non-intrusive investigative tool, and the discovery of potential links between ongoing criminal and foreign intelligence investigations is potentially critical to national security. Instead, they would require an analyst who has not had FISA training to seek supervisory approval before *viewing* responsive 702 information, to ensure that the information continues to be treated consistent with applicable statutory and court-imposed restrictions. They also would require higher-level Justice Department approval before Section 702 information could be used in the investigation or prosecution of a non–foreign intelligence crime.

The statement also responds to the separate statement by Chairman Medine and Member Wald.
Part 3:  
DESCRIPTION AND HISTORY

I. Genesis of the Section 702 Program

As it exists today, the Section 702 program can trace its lineage to two prior intelligence collection programs, both of which were born of counterterrorism efforts following the attacks of September 11, 2001. The first, and more well-known, of these two efforts was a program to acquire the contents of certain international communications, later termed the Terrorist Surveillance Program (“TSP”). In October 2001, President George W. Bush issued a highly classified presidential authorization directing the NSA to collect certain foreign intelligence by electronic surveillance in order to prevent acts of terrorism within the United States, based upon a finding that an extraordinary emergency existed because of the September 11 attacks. Under this authorization, electronic surveillance was permitted within the United States for counterterrorism purposes without judicial warrants or court orders for a limited number of days. President Bush authorized the NSA to (1) collect the contents of certain international communications, a program that was later referred to as the TSP, and (2) collect in bulk non-content information, or “metadata,” about telephone and Internet communications. The acquisition of telephone metadata was the forerunner to the Section 215 calling records program discussed in a prior report by the Board.

The President renewed the authorization for the NSA’s activities in early November 2001. Thereafter, the authorization was renewed continuously, with some modifications and constrictions to the scope of the authorized collection, approximately every thirty to sixty days until 2007. Each presidential authorization included the finding that an extraordinary emergency continued to exist justifying ongoing warrantless surveillance. Key members of Congress and the presiding judge of the Foreign Intelligence Surveillance Court (“FISC” or “FISA court”) were briefed on the existence of the program. The collection of communications content and bulk metadata under these presidential authorizations became known as the President’s Surveillance Program. According to a 2009 report by the inspectors general of several defense and intelligence agencies, over time, “the program


See Dec. 21 DNI Announcement, supra.
became less a temporary response to the September 11 terrorist attacks and more a permanent surveillance tool."

In December 2005, the *New York Times* published articles revealing the TSP, i.e., the portion of the President’s Surveillance Program that involved intercepting the contents of international communications. In response to these revelations, President Bush confirmed the existence of the TSP, and the Department of Justice issued a “white paper” outlining the legal argument that the President could authorize these interceptions without obtaining a warrant or court order. Notwithstanding this legal argument, the government decided to seek authorization under the Foreign Intelligence Surveillance Act (“FISA”) to conduct the content collection that had been occurring under the TSP. In January 2007, the FISC issued orders authorizing the government to conduct certain electronic surveillance of telephone and Internet communications carried over listed communication facilities where, among other things, the government made a probable cause determination regarding one of the communicants, and the email addresses and telephone numbers to be tasked were reasonably believed to be used by persons located outside the United States.

The FISC’s order, referred to as the “Foreign Telephone and Email Order,” in effect replaced the President’s authorization of the TSP, and the President made no further reauthorizations of the TSP. When the government sought to renew the January 2007 Foreign Telephone and Email Order, however, a different judge on the FISC approved the program, but on a different legal theory that required changes in the collection program. Specifically, in May 2007 the FISC approved a modified version of the Foreign Telephone and Email Order in which the court, as opposed to the government, made probable cause determinations regarding the particular foreign telephone numbers and email addresses that were to be used to conduct surveillance under this program. Although the modified

---

18 *See Unclassified Report on the President’s Surveillance Program, prepared by the Office of Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency, and the Office of the Director of National Intelligence, at 31 (2009).*


21 *See Dec. 21 DNI Announcement, supra.*


23 2008 Mukasey Decl., *supra,* at ¶ 37.

24 2008 Mukasey Decl., *supra,* at ¶ 38 & n.20.

25 2008 Mukasey Decl., *supra,* at ¶ 38.
Foreign Telephone and Email Order permitted the government to add newly discovered telephone numbers and email addresses without an individual court order in advance, the government assessed that the restrictions of the order, particularly after the May 2007 modifications, was creating an “intelligence gap.”

Separate from, but contemporaneous with, the TSP and the Foreign Telephone and Email Orders, a second collection effort was being undertaken. Specifically, the government used the then-existing FISA statute to obtain individual court orders to compel private companies to assist the government in acquiring the communications of individuals located overseas who were suspected of engaging in terrorism and who used United States–based communication service providers. The government stated that it and the Foreign Intelligence Surveillance Court (FISC) expended “considerable resources” to obtain court orders based upon a probable cause showing that these overseas individuals met the legal standard for electronic surveillance under FISA, i.e., that the targets were agents of a foreign power (such as an international terrorist group) and that they used the specific communication facilities (such as email addresses) regarding which the government was seeking to conduct electronic surveillance. The persons targeted by these efforts were located outside the United States, and the communications being sought were frequently with others who were also located outside the United States.

Drafting applications that demonstrated satisfaction of this probable cause standard, the government has asserted, slowed and in some cases prevented the acquisition of foreign intelligence information. The government has not disclosed the scale of this second effort to target foreign individuals using traditional FISA electronic surveillance authorities, but in the years following the passage of the Protect America Act of 2007 and the FISA Amendments Act of 2008, which eliminated the requirement for the

---

26 2008 Mukasey Decl., supra, at ¶ 38.
27 See S. Rep. No. 110-209, at 5 (2007) (stating that “the DNI informed Congress that the decision . . . had led to degraded capabilities”); Eric Lichtblau, James Risen, and Mark Mazzetti, Reported Drop in Surveillance Spurred a Law, NEW YORK TIMES (Aug. 11, 2007) (reporting on Administration interactions with Congress that led to the enactment of the Protect America Act, including reported existence of an “intelligence gap”).
government to seek such individual orders, the total number of FISA electronic surveillance applications approved by the FISC dropped by over forty percent.\footnote{Compare 2007 \textit{ANNUAL FISA REPORT} (2,371 Title I FISA applications in 2007), \textit{available at} http://www.fas.org/irp/agency/doi/fisa/2007rept.pdf with 2009 \textit{ANNUAL FISA REPORT} (1,329 Title I FISA applications in 2009), \textit{available at} http://www.fas.org/irp/agency/doi/fisa/2009rept.pdf.}

In light of the perceived growing inefficiencies of obtaining FISC approval to target persons located outside the United States, in the spring of 2007 the Bush Administration proposed modifications to FISA.\footnote{See S. Rep. No. 110-209, at 2, 5 (noting Administration’s submission of proposed modifications in April 2007); \textit{see generally} May 2007 Wainstein Statement, \textit{supra}; Statement of J. Michael McConnell, Director of National Intelligence, Before the Senate Select Committee on Intelligence (May 1, 2007), \textit{available at} http://www.intelligence.senate.gov/070501/mcconnell.pdf.} Reports by the Director of National Intelligence to Congress that implementation of the FISC’s May 2007 modifications to the Foreign Telephone and Email Order had resulted in “degraded” acquisition of communications, combined with reports of a “heightened terrorist threat environment,” accelerated Congress’ consideration of these proposals.\footnote{See S. Rep. No. 110-209, at 5.} In August 2007, Congress enacted and the President signed the Protect America Act of 2007,\footnote{Pub. L. No. 110-55; 121 Stat. 552 (2007) ("Protect America Act").} a legislative forerunner to what is now Section 702 of FISA. The Protect America Act was a temporary measure that was set to expire 180 days after its enactment.\footnote{Protect America Act § 6(c).}

The government transitioned the collection of communications that had been occurring under the Foreign Telephone and Email Orders (previously the TSP) and some portion of the collection targeting persons located outside the United States that had been occurring under individual FISA orders to directives issued under the Protect America Act.\footnote{2008 Mukasey Decl., \textit{supra}, at ¶ 13 & n.22.} The Protect America Act expired in February 2008,\footnote{See Protect America Act—Extension, Pub. L. No. 110-182, 122 Stat. 605 (2008) (extending Protect America Act for two weeks).} but existing Protect America Act certifications remained in effect until they expired.\footnote{Protect America Act § 6.}

Act replaced the expired Protect America Act provisions with the new Section 702 of FISA. The authorities and limitations of Section 702 are discussed in detail in this Report. In addition to Section 702, the FISA Amendments Act of 2008 also enacted Sections 703 and 704 of FISA, which required judicial approval for targeting U.S. persons located abroad in order to acquire foreign intelligence information.43

After passage of the FISA Amendments Act, the government transitioned the collection activities that had been conducted under the Protect America Act to Section 702.44 Section 702, as well as the other provisions of FISA enacted by the FISA Amendments Act, were renewed in December 2012, and are currently set to expire in December 2017.45

II. Statutory Structure: What Does Section 702 Authorize?

The Foreign Intelligence Surveillance Act is a complex law, and Congress’ authorization of surveillance under Section 702 of FISA is no exception. In one sentence, the statutory scope of Section 702 can be defined as follows: Section 702 of FISA permits the Attorney General and the Director of National Intelligence to jointly authorize the (1) targeting of persons who are not United States persons, (2) who are reasonably believed to be located outside the United States, (3) with the compelled assistance of an electronic communication service provider, (4) in order to acquire foreign intelligence information.46 Each of these terms is, to various degrees, further defined and limited by other aspects of FISA. Congress also imposed a series of limitations on any surveillance conducted under Section 702. The statute further specifies how the Attorney General and Director of National Intelligence may authorize such surveillance, as well as the role of the FISC in reviewing these authorizations. This section describes this complex statutory framework.

A. Statutory Definitions and Limitations

Our description of Section 702’s statutory authorization begins by breaking down the four-part sentence above.

First, Section 702 authorizes the targeting of persons.47 FISA does not define what constitutes “targeting,” but it does define what constitutes a “person.” Persons are not only

43 50 U.S.C. §§ 1881b, 1881c.
44 2008 Mukasey Decl., supra, at ¶ 40 & n.22.
47 50 U.S.C. § 1881a(a).
individuals, but also groups, entities, associations, corporations, or foreign powers. The definition of “person” is therefore broad, but not limitless: a foreign government or international terrorist group could qualify as a “person,” but an entire foreign country cannot be a “person” targeted under Section 702. In addition, the persons whom may be targeted under Section 702 may not intentionally include United States persons. “United States persons” or “U.S. persons” are United States citizens, United States permanent residents (green card holders), groups substantially composed of United States citizens or permanent residents, and virtually all United States corporations. As is discussed in detail below, the NSA targets persons by tasking “selectors,” such as email addresses and telephone numbers. The NSA must make determinations (regarding location, U.S. person status, and foreign intelligence value) about the users of each selector on an individualized basis. It cannot simply assert that it is targeting a particular terrorist group.

Second, under Section 702 the non-U.S. person target must also be “reasonably believed to be located outside the United States.” A “reasonable belief” is not defined in FISA, but Section 702 does require that targeting procedures (described in further detail below) be adopted to ensure that Section 702 acquisition is limited to targets reasonably believed to be located outside the United States. Electronic surveillance targeting persons believed to be located in the United States is not permitted by Section 702, whether the persons in question are U.S. persons or not.

Third, under Section 702 this targeting of non-U.S. persons reasonably believed to be located outside the United States occurs with the compelled assistance of an “electronic communication service provider.” FISA defines electronic communication service providers to include a variety of telephone, Internet service, and other communications providers. As further described below, electronic communication service providers are

48 50 U.S.C. §§ 1801(m), 1881(a). The term “foreign power” is a defined term in FISA; it includes international terrorist groups, foreign governments, and entities not substantially composed of United States persons that are engaged in the proliferation of weapons of mass destruction.


50 50 U.S.C. § 1881a(b)(3).
51 50 U.S.C. § 1801(i).
compelled to provide this assistance in conducting Section 702 acquisition through directives issued by the Attorney General and the Director of National Intelligence. Given the nature of the Internet, communications generated and delivered through communication services offered directly to individuals by one entity may be acquired as they cross the network of another provider without the knowledge of the consumer-facing provider. This concept is further described in the discussion below regarding upstream collection.

Fourth, and finally, this targeting of non-U.S. persons reasonably believed to be located outside the United States must be conducted to acquire foreign intelligence information. Non-U.S. persons may be targeted under Section 702 only if the government has reason to believe that those persons possess, are expected to receive, or are likely to communicate foreign intelligence information. Foreign intelligence information concerning non-U.S. persons is defined in FISA as information that relates to the ability of the United States to protect against an actual or potential attack by a foreign power; sabotage, international terrorism, or the proliferation of weapons of mass destruction by a foreign power; or clandestine intelligence activities by a foreign power.

56 There is some conflicting language in Section 702 on the precise standard on this point. Section 1881a(a) states that a Section 702 authorization must be “...to acquire foreign intelligence information.” This authority, however, must be governed by a certification, and the certification need only state that “a significant purpose of the acquisition is to obtain foreign intelligence information.” 50 U.S.C. § 1881a(g)(2)(A)(v). See also SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, AUGUST 2013, at A-2 (“AUGUST 2013 SEMIANNUAL ASSESSMENT”) (noting that the Section 702 Attorney General Guidelines implement the statutory requirement that a “significant purpose of the acquisition is to obtain foreign intelligence information,” 50 U.S.C. § 1881a(g)(2)(A)(v), by requiring that Section 702 targeting occur only with respect to persons assessed to possess foreign intelligence information or who are reasonably likely to receive or communicate foreign intelligence information), available at http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issu ed%20pursuant%20to%20Sect%20702%20of%20FISA.pdf; see also NSA DIRECTOR OF CIVIL LIBERTIES AND PRIVACY OFFICE REPORT: NSA’S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702, at 5 (April 16, 2014) (“NSA DCLPO REPORT”), available at http://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf.

57 NSA DCLPO REPORT, supra, at 3.

58 50 U.S.C. § 1801(e)(1). For information concerning a U.S. person, the information must be “necessary” for this purpose. Specifically, this provision states foreign intelligence information is defined as:

[I]nformation that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against —

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.
intelligence information concerning non-U.S. persons is also defined as information that relates to the national defense or security of the United States or the conduct of the foreign affairs of the United States, but only insofar as that information concerns a foreign power (such as international terrorist groups or foreign governments) or foreign territory. The term “foreign territory” is undefined by the statute. As noted below, in authorizing Section 702 acquisition, the Attorney General and Director of National Intelligence specify the categories of foreign intelligence information that the United States government is seeking to acquire.

In addition to defining the scope of the Section 702 authorization, Congress specified limitations on the government’s authority to engage in Section 702 targeting. As previously mentioned, U.S. persons may not be intentionally targeted. In addition, the government is prohibited under the law from intentionally targeting “any person known at the time of acquisition to be located in the United States.” These two rules taken together — that the target must be both a non-U.S. person and someone reasonably believed to be located abroad — are often referred to as the “foreignness” requirement.

The government is also prohibited from engaging in what is generally referred to as “reverse targeting,” which would occur if the government were to intentionally target persons reasonably believed to be located outside the United States “if the purpose of the acquisition is to target a particular, known person reasonably believed to be in the United States.” In addition to this explicit prohibition against reverse targeting persons located in the United States, the government reads the statutory prohibition against targeting U.S. persons to also prohibit the reverse targeting of U.S. persons. In other words, the ban on reverse targeting prohibits the government from targeting a non-U.S. person outside the United States when the real interest is to collect the communications of a person in the United States or of any U.S. person, regardless of location.

Under Section 702, the government also “may not intentionally acquire communications as to which the sender and all intended recipients are known at the time

50 U.S.C. § 1801(e)(2). Specifically, this provision states foreign intelligence information is also defined as:

[I]nformation with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to —

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

50 U.S.C. § 1881a(b)(1).

50 U.S.C. § 1881a(b)(2).

See PCLOB March 2014 Hearing Transcript, supra, at 89-92.
of the acquisition to be located in the United States.”\(^{63}\) Finally, Section 702 contains a limitation (and a reminder) that any acquisition must always be conducted consistent with the requirements of the Fourth Amendment to the Constitution.\(^{64}\)

**B. Section 702 Certifications**

The Attorney General and the Director of National Intelligence authorize Section 702 targeting in a manner substantially different than traditional electronic surveillance under FISA. To authorize traditional FISA electronic surveillance, an application approved by the Attorney General must be made to the FISC.\(^{65}\) This individualized application must include, among other things, the identity (if known) of the specific target of the electronic surveillance; facts justifying a probable cause finding that this target is a foreign power or agent of a foreign power and uses (or is about to use) the communication facilities or places at which electronic surveillance is being directed;\(^{66}\) minimization procedures governing the acquisition, retention, and dissemination of non-publicly available U.S. person information acquired through the electronic surveillance; and a certification regarding the foreign intelligence information sought.\(^{67}\) If the FISC judge who reviews the government’s application determines that it meets the required elements — including that there is probable cause that the specified target is a foreign power or agent of a foreign power and that the minimization procedures meet the statutory requirements — the judge will issue an order authorizing the requested electronic surveillance.\(^{68}\)

Section 702 differs from this traditional FISA electronic surveillance framework both in the standards applied and in the lack of individualized determinations by the FISC. Under the statute, the Attorney General and Director of National Intelligence make annual certifications authorizing the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information, without specifying to the FISC the particular non-U.S. persons who will be targeted.\(^{69}\) Instead of identifying particular individuals to be targeted under Section 702, the certifications identify categories of foreign intelligence information regarding which the Attorney

---

\(^{63}\) 50 U.S.C. § 1881a(b)(4).

\(^{64}\) 50 U.S.C. § 1881a(b)(5).

\(^{65}\) 50 U.S.C. § 1804(a). FISA also grants additional authority to conduct emergency electronic surveillance without first making an application to the FISC. 50 U.S.C. § 1805(e).

\(^{66}\) But see 50 U.S.C. § 1805(c)(3) (permitting electronic surveillance orders “in circumstances where the nature and location of each of the facilities or places at which surveillance will be directed is unknown”)

\(^{67}\) 50 U.S.C. §§ 1804(a), 1805(a).

\(^{68}\) 50 U.S.C. § 1805(a), (c), (d).

\(^{69}\) 50 U.S.C. § 1881a(a); NSA DCLPO REPORT, supra, at 2 (noting that Section 702 certifications do not require “individualized determination” by the FISC).
General and Director of National Intelligence authorize acquisition through the targeting of non-U.S. persons reasonably believed to be located abroad. There also is no requirement that the government demonstrate probable cause to believe that a Section 702 target is a foreign power or agent of a foreign power, as is required under traditional FISA. Rather, the categories of information being sought must meet the definition of foreign intelligence information described above. The government has not declassified the full scope of the certifications that have been authorized, but officials have stated that these certifications have authorized the acquisition of information concerning international terrorism and other topics, such as the acquisition of weapons of mass destruction.

While individual targets are not specified, Section 702 certifications must instead contain “targeting procedures” approved by the Attorney General that must be “reasonably designed” to ensure that any Section 702 acquisition is “limited to targeting persons reasonably believed to be located outside the United States” and prevents the “intentional acquisition” of wholly domestic communications. The targeting procedures specify the manner in which the Intelligence Community must determine whether a person is a non-U.S. person reasonably believed to be located outside the United States who possesses (or is likely to possess or receive) the types of foreign intelligence information authorized by a certification. The process by which individuals are permitted to be targeted pursuant to the targeting procedures is discussed in detail below. In addition, the Attorney General and Director of National Intelligence must also attest in the certification that the Attorney General has adopted additional guidelines to ensure compliance with both these and the other statutory limitations on the Section 702 program. Most critically, these Attorney General Guidelines explain how the government implements the statutory prohibition against reverse targeting.

While only non-U.S. persons may be intentionally targeted, the information of or concerning U.S. persons may be acquired through Section 702 targeting in a variety of ways, such as when a U.S. person is in communication with a non-U.S. person Section 702

---

70 See 50 U.S.C. § 1881a(g)(2)(A)(v) (requiring Attorney General and Director of National Intelligence to attest that a significant purpose of the acquisition authorized by the certification is to acquire foreign intelligence information); PCLOB March 2014 Hearing Transcript, supra, at 8-9 (statement of Robert Litt, General Counsel, ODNI) (stating that certifications “identify categories of information that may be acquired”); NSA DCLPO REPORT, supra, at 2 (noting the “annual topical certifications” authorized by Section 702).

71 PCLOB March 2014 Hearing Transcript at 13 (statement of Robert Litt, General Counsel, ODNI) (stating that the Section 702 program has been an important source of information “not only about terrorism, but about a wide variety of other threats to our nation”); id. at 59 (statement of Rajesh De, General Counsel, NSA) (stating that there are certifications on “counterterrorism” and “weapons of mass destruction”); id. at 68 (statement of James A. Baker, General Counsel, FBI) (“[T]his program is not limited just to counterterrorism.”).


target, because two non-U.S. persons are discussing a U.S. person, or because a U.S. person was mistakenly targeted. Section 702 therefore requires that certifications also include “minimization procedures” that control the acquisition, retention, and dissemination of any non–publicly available U.S. person information acquired through the Section 702 program. As discussed below, the minimization procedures include different procedures for handling U.S. person information depending on the circumstances of how it was acquired. Along with the targeting procedures, the minimization procedures contain the government’s core privacy and civil liberties protections and are more fully discussed throughout this Report.

C. FISC Review

The government’s Section 702 certifications, targeting procedures, and minimization procedures (but not the Attorney General Guidelines) are all subject to review by the FISC. In addition to the required procedures and guidelines, the Section 702 certifications are accompanied by affidavits of national security officials that further describe to the FISC the government’s basis for assessing that the proposed Section 702 acquisition will be consistent with the applicable statutory authorization and limits. Through court filings or the testimony of witnesses at hearings before the FISC, the government also submits additional information explaining how the targeting and minimization procedures will be applied and describing the operation of the program in a way that defines its scope.

The FISC’s review of the Section 702 certifications has been called “limited” by scholars, privacy advocates, and in one instance, shortly after the FISA Amendments Act

---

75 50 U.S.C. § 1881a(d)(2), (e)(2), (i). The Attorney General Guidelines must, however, be submitted to the FISA court. 50 U.S.C. § 1881a(f)(2)(C). Section 702 does have a provision permitting the Attorney General and the Director of National Intelligence to authorize acquisition prior to judicial review of a certification under certain exigent circumstances. 50 U.S.C. § 1881a(c)(2). To date, the Attorney General and the Director of National Intelligence have never exercised this authority.
77 See AUGUST 2013 SEMIANNUAL ASSESSMENT, supra, at A-1 to A-2.
78 See, e.g., Bates October 2011 Opinion, supra, at 5-9, 2011 WL 10945618, at *2-4 (describing 2011 government filings with, and testimony before, the FISA court); id. at 15-16, 2011 WL 10945618, at *5 (describing representations made to the FISA court in prior Section 702 certifications).
was passed, by the FISC itself. In certain respects, this characterization is accurate. Unlike traditional FISA applications, the FISC does not review the targeting of particular individuals. Specifically, although the Section 702 certifications identify the foreign intelligence subject matters regarding which information is to be acquired, the FISC does not see or approve the specific persons targeted or the specific communication facilities that are actually tasked for acquisition. As such the government does not present evidence to the FISC, nor does the FISC determine — under probable cause or any other standard — that the particular individuals being targeted are non-U.S. persons reasonably believed to be located outside the United States who are being properly targeted to acquire foreign intelligence information. Instead of requiring judicial review of these elements, Section 702 calls upon the FISA court only to decide whether the targeting procedures are reasonably designed to ensure compliance with certain limitations and that the minimization procedures satisfy certain criteria (described below). The FISC is not required to independently determine that a significant purpose of the proposed acquisition is to obtain foreign intelligence information, although the foreign intelligence purpose of the collection does play a role in the court’s Fourth Amendment analysis.

In other respects, however, the FISC’s role in the Section 702 program is more extensive. The FISC reviews both the targeting procedures and the minimization procedures, the core set of documents that implement Section 702’s statutory requirements and limitations. With respect to the targeting procedures, the FISC must


82 See The Intelligence Community’s Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, at 2 (2012) (describing differences between targeting individuals under traditional FISA electronic surveillance provisions and targeting pursuant to Section 702). This document accompanied a 2012 letter sent by the Department of Justice and the Office of the Director of National Intelligence to the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence urging the reauthorization of Section 702. See Letter from Kathleen Turner, Director of Legislative Affairs, ODNI, and Ronald Weich, Assistant Attorney General, Office of Legislative Affairs, DOJ to the Honorable Dianne Feinstein, Chairman, Senate Committee on Intelligence, et. al. (May 4, 2012), available at http://www.dni.gov/files/documents/Ltr%20to%20HPSCI%20Chairman%20Rogers%20and%20Ranking%20Member%20Ruppersberger_Scan.pdf.

83 50 U.S.C. § 1881a(i)(2).

84 Additionally, if the FISC determines that a Section 702 certification and related documents are insufficient on Constitutional or statutory grounds, the FISC cannot itself modify the certification and related documents governing the Section 702 program, but instead must issue an order to the government to either correct any deficiencies identified by the FISC within 30 days or to cease (or not begin) implementation of the certification. 50 U.S.C. § 1881a(i)(3)(B).

determine that they “are reasonably designed” to “ensure” that targeting is “limited to targeting persons reasonably believed to be located outside the United States.” The FISC also must determine that the targeting procedures are reasonably designed to prevent the intentional acquisition of wholly domestic communications. In addition, the FISC must also review the proposed minimization procedures under the same standard of review that is required in traditional FISA electronic surveillance and physical search applications. The FISC must find that such minimization procedures are “specific procedures” that are “reasonably designed” to control the acquisition, retention, and dissemination of non–publicly available U.S. person information. Each time the FISC reviews a Section 702 certification, the FISC must also determine whether the proposed Section 702 acquisition as provided for, and restricted by, the targeting and minimization procedures complies with the Fourth Amendment. After conducting its analysis, the FISC must issue a written opinion explaining the reasons why the court has held that the proposed targeting and minimization procedures do, or do not, comply with statutory and Fourth Amendment requirements.

The FISC has held that it cannot make determinations in a vacuum regarding whether targeting and minimization procedures are “reasonably designed” to meet the statutory requirements and comply with the Fourth Amendment. To the contrary, the FISC “has repeatedly noted that the government’s targeting and minimization procedures must be considered in light of the communications actually acquired,” and that “[s]ubstantial implementation problems can, notwithstanding the government’s intent, speak to whether the applicable targeting procedures are ‘reasonably designed’ to acquire only the communications of non-U.S. persons outside the United States.” Therefore, although the FISC reviews the targeting procedures, minimization procedures, and related affidavits that

89 50 U.S.C. § 1801(h).
91 50 U.S.C. § 1881a(i)(3)(C). While FISC judges may write opinions explaining their orders with regard to other aspects of FISA, the statutory requirement for an opinion explaining the rationale of all orders approving Section 702 certifications is unique within FISA. Though not required by FISA, FISC Rule of Procedure 18(b)(1) also requires FISC judges to provide a written statement of reasons for any denials of the government’s other FISA applications. See United States Foreign Intelligence Surveillance Court Rules of Procedure (“FISC Rule of Procedure”), Rule 18(b)(1), available at http://www.uscourts.gov/uscourts/rules/FISC2010.pdf.
are submitted with a Section 702 certification, the court’s review is not limited to the four corners of those documents. The FISC also takes into consideration additional filings by the government to supplement or clarify the record, responses to FISC orders to supplement the record,\(^93\) and the sworn testimony of witnesses at hearings.\(^94\)

Commitments regarding how the targeting and minimization procedures will be implemented that are made to the FISC in these representations have been found to be binding on the government. For example, during the consideration of the first Section 702 certification in 2008, the government stated that the targeting procedures impose a requirement that analysts conduct "due diligence" in determining the U.S. person status of any Section 702 target, even though the phrase "due diligence" is not explicitly found in the text of the NSA targeting procedures. The FISC incorporated the government's representation regarding due diligence into its opinion, and the government has subsequently reported to Congress and the FISC — as incidents of noncompliance — instances in which the Intelligence Community conducted insufficient due diligence that resulted in the targeting of a U.S. person.\(^95\)

In evaluating the Section 702 certifications, the court also considers additional filings required by the FISC’s Rules of Procedure. One such rule requires the government to notify the FISA court whenever the government discovers a material misstatement or omissions in a prior filing with the court.\(^96\) Another rule mandates that the government report to the FISA court incidents of noncompliance with targeting or minimization procedures previously approved by the court.\(^97\) In a still-classified 2009 opinion, the FISC held that the judicial review requirements regarding the targeting and minimization procedures required that the FISC be fully informed of every incident of noncompliance.

\(^93\) See FISC Rule of Procedure 5(c) (stating that the FISC Judges have the authority to order any party to a proceeding to supplement the record by “furnish[ing] any information that the Judge deems necessary”).

\(^94\) FISC Rule of Procedure 17.

\(^95\) See August 2013 Semiannual Assessment, supra, at 29 (describing incidents and stating "In each of these incidents, all Section 702–acquired data was purged. Together, these [redacted] instances represent isolated instances of insufficient due diligence that do not reflect the [redacted] of taskings that occur during the reporting period.").

\(^96\) See FISC Rule of Procedure 13(a).

\(^97\) See FISC Rule of Procedure 13(b); Semiannual Assessment of Compliance with Procedures and Guidelines Issues Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, May 2010, at 22 ("May 2010 Semiannual Assessment") (discussing requirements under Rule 10(c), the predecessor to Rule 13(b) in the prior set of FISC Rules of Procedure), available at http://www.dni.gov/files/documents/FAA/SAR%20May%202010%20Final%20Release%20with%20Exemptions.pdf. The government also provides the FISC the Semiannual Section 702 Joint Assessment, portions of the Section 707 Semiannual report, and a separate quarterly report to the FISC, all of which describe scope, nature, and actions taken in response to compliance incidents. See The Intelligence Community’s Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, supra, at 5; 50 U.S.C. § 1881a(l)(1).
with those procedures. In the 2009 opinion, the court analyzed whether several errors in applying the targeting and minimization procedures that had been reported to the court undermined either the court’s statutory or constitutional analysis. (The court concluded that they did not.)

In addition to identifying errors that could impact the sufficiency of the targeting and minimization procedures, these compliance notices play an additional role in informing the FISC regarding how the government is in fact applying the targeting and minimization procedures. Specifically, the compliance notices must state both the type of noncompliance that has occurred and the facts and circumstances relevant to the incident. In doing so, representations to the FISA court have in essence created a series of precedents regarding how the government is interpreting various provisions of its targeting and minimization procedures, which informs the court’s conclusions regarding whether those procedures — as actually applied by the Intelligence Community to particular, real-life factual scenarios — comply with Section 702’s statutory requirements and the Fourth Amendment. For example, while the 2008 FISC opinion incorporated the government’s commitment to apply due diligence in determining the U.S. person status of potential targets, notices of non-compliance filed by the government reflect that the government interprets the targeting procedures to also require due diligence in determining the location of potential targets. Similarly, the government has filed letters clarifying aspects of its “post-tasking” process, which are discussed further below, and it has reported — as compliance incidents — instances when its performance of the post-tasking process has not complied with those representations. The government’s interpretations of the targeting and minimization procedures reflected in these compliance filings, however, are not necessarily formally endorsed or incorporated into the FISC’s subsequent opinions. In the Board’s opinion Intelligence Community personnel applying these procedures months or years later may not be aware of the interpretive gloss arising from prior interactions between the government and the FISC on these procedures.

Former FISC Presiding Judge John Bates’ October 3, 2011 opinion provides both an example of the scope of the FISA court’s review of Section 702 certifications in practice and an illustration of what actions the court can take if it determines that the government has not satisfied the court’s expectations to be kept fully, accurately, and timely informed. In April 2011, the government filed multiple Section 702 certifications with the FISC. In early May 2011, however, the government filed a letter with the court (under a FISC procedural rule regarding material misstatements or omissions) acknowledging that the scope of the NSA’s “upstream” collection (described below) was more expansive than

98 FISC Rule of Procedure 13(b).
previously represented to the court.100 As a result of the filing, the FISC expressed serious concern that the upstream collection, as described by the government, may have exceeded the scope of collection previously approved by the FISC and what could be authorized under Section 702. The FISC therefore ordered the government to respond to a number of questions regarding the upstream collection program.101 Throughout the summer of 2011, the government continued to supplement the record in response to the FISA court’s concerns with a number of filings, including by conducting and reporting to the court the results of a statistical sample of the NSA’s acquisition of upstream collection.102 The government’s supplemental filings discussed both factual matters, such as how many domestic communications were being acquired as a result of the manner in which the government was conducting upstream collection, as well as the government’s legal interpretations regarding how the NSA’s minimization procedures should be applied to such acquisition.103 The FISA court also met with the government and held a hearing to ask additional questions of NSA and Department of Justice personnel.104

Based on this record, Judge Bates ultimately held that in light of the new information, portions of the NSA minimization procedures met neither the requirements of FISA nor the Fourth Amendment and ordered the government to correct the deficient procedures or cease Section 702 upstream collection.105 The government subsequently modified the NSA minimization procedures to remedy the deficiencies identified by the FISA court.106 The FISC continued to have questions, however, regarding upstream collection that had been acquired prior to the implementation of these modified NSA minimization procedures.107 The government took several actions with regard to this past upstream collection, and ultimately decided to purge it all.108

---

D. Directives

As noted above, Section 702 targeting may occur only with the assistance of electronic communication service providers. Once Section 702 acquisition has been authorized, the Attorney General and the Director of National Intelligence send written directives to electronic communication service providers compelling the providers’ assistance in the acquisition. Providers that receive a Section 702 directive may challenge the legality of the directive in the FISC. The government may likewise file a petition with the FISC to compel a provider that does not comply with a directive to assist the government’s acquisition of foreign intelligence information. The FISC’s decisions regarding challenges and enforcement actions regarding directives are appealable to the Foreign Intelligence Surveillance Court of Review (“FISCR”), and either the government or a provider may request that the United States Supreme Court review a decision of the FISCR.

III. Acquisition Process: How Does Section 702 Surveillance Actually Work?

Once a Section 702 certification has been approved, non-U.S. persons reasonably believed to be located outside the United States may be targeted to acquire foreign intelligence information within the scope of that certification. The process by which non-U.S. persons are targeted is detailed in the next section. This section describes how Section 702 acquisition takes place once an individual has been targeted.

A. Targeting Persons by Tasking Selectors

The Section 702 certifications permit non-U.S. persons to be targeted only through the “tasking” of what are called “selectors.” A selector must be a specific communications facility that is assessed to be used by the target, such as the target’s email address or telephone number. Thus, in the terminology of Section 702, people (non-U.S. persons reasonably believed to be located outside the United States) are targeted; selectors (e.g., email addresses, telephone numbers) are tasked. The users of any tasked selector are

111 U.S.C. § 1881a(h)(5).
112 U.S.C. § 1881a(h)(6). However, as noted in the Board’s Section 215 report, to date, only two cases have been appealed to the FISCR. One, In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (FISA Ct. Rev. 2008), involved a directive under the Protect America Act, the predecessor to Section 702, but none have involved Section 702. Nor has the U.S. Supreme Court ever considered the merits of a FISA order or ruled on the merits of any challenge to FISA.

113 See AUGUST 2013 JOINT ASSESSMENT, supra, at A-2; NSA DCLPO REPORT, supra, at 4; The Intelligence Community’s Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, supra, at 3.
considered targets — and therefore only selectors used by non-U.S. persons reasonably believed to be located abroad may be tasked. The targeting procedures govern both the targeting and tasking process.

Because such terms would not identify specific communications facilities, selectors may not be key words (such as “bomb” or “attack”), or the names of targeted individuals (“Osama Bin Laden”). Under the NSA targeting procedures, if a U.S. person or a person located in the United States is determined to be a user of a selector, that selector may not be tasked to Section 702 acquisition or must be promptly detasked if the selector has already been tasked.

Although targeting decisions must be individualized, this does not mean that a substantial number of persons are not targeted under the Section 702 program. The government estimates that 89,138 persons were targeted under Section 702 during 2013.

Once a selector has been tasked under the targeting procedures, it is sent to an electronic communications service provider to begin acquisition. There are two types of Section 702 acquisition: what has been referred to as “PRISM” collection and “upstream” collection. PRISM collection is the easier of the two acquisition methods to understand.

**B. PRISM Collection**

In PRISM collection, the government (specifically, the FBI on behalf of the NSA) sends selectors — such as an email address — to a United States–based electronic communications service provider (such as an Internet service provider, or “ISP”) that has been served a directive. Under the directive, the service provider is compelled to give the communications sent to or from that selector to the government (but not communications that are only “about” the selector, as described below). As of mid-2011, 91 percent of the

---

114 NSA DCLPO REPORT, *supra*, at 4; PCLOB March 2014 Hearing Transcript, *supra*, at 57 (statement of Rajesh De, General Counsel, NSA) (noting that a name cannot be tasked).

115 NSA DCLPO REPORT, *supra*, at 6.

116 OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE STATISTICAL TRANSPARENCY REPORT REGARDING USE OF NATIONAL SECURITY AUTHORITIES: ANNUAL STATISTICS FOR CALENDAR YEAR 2013, at 1 (June 26, 2014), available at http://www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY2013.pdf. In calculating this estimate, the government counted two known people using one tasked email address as two targets and one person known to use two tasked email addresses as one target. The number of targets is an estimate because the government may not be aware of all of the users of a particular tasked selector.

117 The Intelligence Community’s Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3. *See also* PCLOB March 2014 Hearing Transcript at 70 (statement of Rajesh De, General Counsel, NSA) (noting any recipient company “would have received legal process”).

118 PCLOB March 2014 Hearing Transcript at 70; *see also* NSA DCLPO REPORT, *supra*, at 5.
Internet communications that the NSA acquired each year were obtained through PRISM collection.\textsuperscript{119}

The government has not declassified the specific ISPs that have been served directives to undertake PRISM collection, but an example using a fake United States company (“USA-ISP Company”) may clarify how PRISM collection works in practice: The NSA learns that John Target, a non-U.S. person located outside the United States, uses the email address “johntarget@usa-ISP.com” to communicate with associates about his efforts to engage in international terrorism. The NSA applies its targeting procedures (described below) and “tasks” johntarget@usa-ISP.com to Section 702 acquisition for the purpose of acquiring information about John Target’s involvement in international terrorism. The FBI would then contact USA-ISP Company (a company that has previously been sent a Section 702 directive) and instruct USA-ISP Company to provide to the government all communications to or from email address johntarget@usa-ISP.com. The acquisition continues until the government “detasks” johntarget@usa-ISP.com.

The NSA receives all PRISM collection acquired under Section 702. In addition, a copy of the raw data acquired via PRISM collection — and, to date, only PRISM collection — may also be sent to the CIA and/or FBI.\textsuperscript{120} The NSA, CIA, and FBI all must apply their own minimization procedures to any PRISM-acquired data.\textsuperscript{121}

Before data is entered into systems available to trained analysts or agents, government technical personnel use technical systems to help verify that data sent by the provider is limited to the data requested by the government. To again use the John Target example above, if the NSA determined that johntarget@usa-ISP.com was not actually going to be used to communicate information about international terrorism, the government would send a detasking request to USA-ISP Company to stop further Section 702 collection on this email address. After passing on the detasking request to USA-ISP Company, the government would use its technical systems to block any further Section 702 acquisition from johntarget@usa-ISP.com to ensure that Section 702 collection against this address was immediately terminated.


\textsuperscript{121} NSA 2011 Minimization Procedures, supra, § 6(c).
C. Upstream Collection

The NSA acquires communications from a second means, which is referred to as upstream collection. Upstream collection is different from PRISM collection because the acquisition occurs not with the compelled assistance of the United States ISPs, but instead with the compelled assistance (through a Section 702 directive) of the providers that control the telecommunications backbone over which communications transit. The collection therefore does not occur at the local telephone company or email provider with whom the targeted person interacts (which may be foreign telephone or Internet companies, which the government cannot compel to comply with a Section 702 directive), but instead occurs “upstream” in the flow of communications between communication service providers.

Unlike PRISM collection, raw upstream collection is not routed to the CIA or FBI, and therefore it resides only in NSA systems, where it is subject to the NSA’s minimization procedures. CIA and FBI personnel therefore lack any access to raw data from upstream collection. Accordingly, they cannot view or query such data in CIA or FBI systems.

The upstream acquisition of telephone and Internet communications differ from each other, and these differences affect privacy and civil liberty interests in varied ways. Each type of Section 702 upstream collection is discussed below. In conducting both types of upstream acquisition, NSA employs certain collection monitoring programs to identify anomalies that could indicate that technical issues in the collection platform are causing data to be overcollected.

---

122 The Intelligence Community’s Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, supra, at 3-4; see also PCLOB March 2014 Hearing Transcript, supra, at 26 (statement of Rajesh De, General Counsel, NSA) (“The second type of collection is the shorthand referred to as upstream collection. Upstream collection refers to collection from the, for lack of a better phrase, Internet backbone rather than Internet service providers.”).

123 See PCLOB March 2014 Hearing Transcript, supra, at 26 (statement of Rajesh De, General Counsel, NSA) (“This type of collection upstream fills a particular gap of allowing us to collect communications that are not available under PRISM collection.”).

124 The Intelligence Community’s Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, supra, at 4.

125 See PCLOB March 2014 Hearing Transcript, supra, at 27 (statement of Rajesh De, General Counsel, NSA).

126 AUGUST 2013 SEMIANNUAL ASSESSMENT, supra, at 29.
1. Upstream Collection of Telephone Communications

Like PRISM collection, the upstream collection of telephone communications begins with the NSA’s tasking of a selector. The same targeting procedures that govern the tasking of an email address in PRISM collection also apply to the tasking of a telephone number in upstream collection. Prior to tasking, the NSA therefore is required to assess that the specific telephone number to be tasked is used by a non-U.S. person reasonably believed to be located outside the United States from whom the NSA assesses it may acquire the types of foreign intelligence information authorized under one of the Section 702 certifications. Once the targeting procedures have been applied, the NSA sends the tasked telephone number to a United States electronic communication service provider to initiate acquisition. The communications acquired, with the compelled assistance of the provider, are limited to telephone communications that are either to or from the tasked telephone number that is used by the targeted person. Upstream telephony collection therefore does not acquire communications that are merely “about” the tasked telephone number.

2. Upstream Collection of Internet “Transactions”

The process of tasking selectors to acquire Internet transactions is similar to tasking selectors to PRISM and upstream telephony acquisition, but the actual acquisition is substantially different. Like PRISM and upstream telephony acquisition, the NSA may only target non-U.S. persons by tasking specific selectors to upstream Internet transaction collection. And, like other forms of Section 702 collection, selectors tasked for upstream Internet transaction collection must be specific selectors (such as an email address), and may not be key words or the names of targeted individuals.

Once tasked, selectors used for the acquisition of upstream Internet transactions are sent to a United States electronic communication service provider to acquire communications that are transiting through circuits that are used to facilitate Internet

127 PCLOB March 2014 Hearing Transcript, supra, at 26 (statement of Rajesh De, General Counsel, NSA); id. at 51-53 (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ).

128 NSA DCLPO REPORT, supra, at 6.

129 PCLOB March 2014 Hearing Transcript, supra, at 53-54 (statements of Rajesh De, General Counsel, NSA, and Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ).


131 NSA DCLPO REPORT, supra, at 4-5.

132 NSA DCLPO REPORT, supra, at 4; PCLOB March 2014 Hearing Transcript, supra, at 57 (statement of Rajesh De, General Counsel, NSA) (noting that a name cannot be tasked).
communications, what is referred to as the “Internet backbone.” The provider is compelled to assist the government in acquiring communications across these circuits. To identify and acquire Internet transactions associated with the Section 702–tasked selectors on the Internet backbone, Internet transactions are first filtered to eliminate potential domestic transactions, and then are screened to capture only transactions containing a tasked selector. Unless transactions pass both these screens, they are not ingested into government databases. As of 2011, the NSA acquired approximately 26.5 million Internet transactions a year as a result of upstream collection.

Upstream collection acquires Internet transactions that are “to,” “from,” or “about” a tasked selector. With respect to “to” and “from” communications, the sender or a recipient is a user of a Section 702–tasked selector. This is not, however, necessarily true for an “about” communication. An “about” communication is one in which the tasked selector is referenced within the acquired Internet transaction, but the target is not necessarily a participant in the communication. If the NSA therefore applied its targeting procedures to task email address “JohnTarget@example.com,” to Section 702 upstream collection, the NSA would potentially acquire communications routed through the Internet backbone that were sent from email address JohnTarget@example.com, that were sent to JohnTarget@example.com, and communications that mentioned JohnTarget@example.com in the body of the message. The NSA would not, however, acquire communications simply because they contained the name “John Target.” In a still-classified September 2008 opinion, the FISC agreed with the government’s conclusion that the government’s target when it acquires an “about” communication is not the sender or recipients of the communication, regarding whom the government may know nothing, but instead the targeted user of the Section 702–tasked selector. The FISC’s reasoning relied upon language in a congressional report, later quoted by the FISA Court of Review, that the

133 The Intelligence Community’s Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, supra, at 3-4.


135 See, e.g., October 2011 Opinion, supra, at 15-16, 2011 WL 10945618, at *5-6 (describing the government’s representations regarding upstream collection in the first Section 702 certification the FISC reviewed).

“target” of a traditional FISA electronic surveillance “is the individual or entity . . . about whom or from whom information is sought.”

There are technical reasons why “about” collection is necessary to acquire even some communications that are “to” and “from” a tasked selector. In addition, some types of “about” communications actually involve Internet activity of the targeted person. The NSA cannot, however, distinguish in an automated fashion between “about” communications that involve the activity of the target from communications that, for instance, merely contain an email address in the body of an email between two non-targets.

In order to acquire “about” communications while complying with Section 702’s prohibition on intentionally acquiring known domestic communications, the NSA is required to take additional technical steps that are not required for other Section 702 collection. NSA is required to use other technical means, such as Internet protocol (“IP”) filters, to help ensure that at least one end of an acquired Internet transaction is located outside the United States. If, for example, a person located in Chicago sent an email to a friend in Miami that mentioned the tasked selector “JohnTarget@example.com,” the IP filters (or comparable technical means) are designed to prevent the acquisition of this communication. The IP filters, however, do not operate perfectly, and may fail to filter out a domestic communication before it is screened against tasked selectors. A United States-based user, for example, may send a communication (intentionally or otherwise) via a foreign server even if the intended recipient is also in the United States. As such, the FISC has noted the government’s concession that in the ordinary course of acquiring single communications, wholly domestic communications could be acquired as much as 0.197% of the time. While this percentage is small, the FISA court estimated in 2011 that the

---

137 See In re Sealed Case, 310 F. 3d 717, 740 (FISA Ct. Rev. 2002) (quoting H.R. Rep. 95-1283, at 73 (1978)); see also PCLOB March 2014 Hearing Transcript, supra, at 55 (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ) (confirming the FISC had held that targeting includes communications about a particular selector that are not necessarily to or from that selector).

138 Bates October 2011 Opinion, supra, at 37-38, 2011 WL 10945618, at *12 (describing the types of acquired Internet transactions and noting that a subset involve transactions of the target).


140 Bates October 2011 Opinion, supra, at 33, 2011 WL 10945618, at *11 (regarding the “technical measures” that NSA uses to prevent the acquisition of upstream collection of domestic communications); NSA DCLPO REPORT, supra, at 5-6 (acknowledging that IP filters are used to prevent the acquisition of domestic communications).

141 December 2011 Joint Statement, supra, at 7 (acknowledging measures to prevent acquisition of domestic communications “are not perfect”).


overall number of communications the government acquires through Section 702 upstream collection could result in the government acquiring as many as tens of thousands of wholly domestic communications per year.144

In addition, wholly domestic communications could also be acquired because they were embedded in a larger multi-communication transaction ("MCT"), the subject of the next section.

3. Upstream Collection of Internet Communications: Multi-Communication Transactions ("MCTs")

While the NSA's upstream collection is intended to acquire Internet communications, it does so through the acquisition of Internet transactions. The difference between communications and transactions is a significant one, and the government's failure to initially distinguish and account for this distinction caused the FISA court to misunderstand the nature of the collection for over two years, and later to find a portion of the Section 702 program to be unconstitutional.

The NSA-designed upstream Internet collection devices acquire transactions as they cross the Internet. An Internet transaction refers to any set of data that travels across the Internet together such that it may be understood by a device on the Internet.145 An Internet transaction could consist of a single discrete communication, such as an email that is sent from one server to another. Such communications are referred to as single communication transactions (SCTs).146 Of the upstream Internet transactions that the NSA acquired in 2011, approximately ninety percent were SCTs.147

In other instances, however, a single Internet transaction might contain multiple discrete communications. These transactions are referred to as MCTs.148 If a single discrete communication within an MCT is to, from, or about a Section 702–tasked selector, and at least one end of the transaction is foreign, the NSA will acquire the entire MCT.149

If the acquired MCT is a transaction between the Section 702 target (who is assessed to be a non-U.S. person located outside the United States and is targeted to acquire foreign intelligence information falling under one of the approved certifications) and a server, then

all of the discrete communications acquired within the MCT are also communications to or from the target. Based on a statistical sample conducted by the NSA, the FISC estimated that as of 2011 the NSA acquired between 300,000 and 400,000 such MCTs every year (i.e., MCTs where the “active user,”\textsuperscript{150} was the target him or herself).\textsuperscript{151}

When the acquired MCT is not a transaction between the target and the server, but instead a transaction between another individual and a server that happens to include a Section 702 tasked selector, the MCT may “include communications that are not about a tasked selector and may have no relationship, or no more than an incidental relationship to the [tasked] selector.”\textsuperscript{152} These non-target MCTs break down into three categories. Based on the NSA’s statistical study, the FISC estimated that (as of 2011) the NSA acquired at least 1.3 million MCTs each year where the user who caused the transaction to occur was not the target, but was located outside the United States.\textsuperscript{153} Using this same statistical analysis, the FISA court estimated that the NSA would annually acquire an additional approximately 7,000 to 8,000 MCTs of non-targeted users who were located in the United States, and between approximately 97,000 and 140,000 MCTs each year where NSA would not be able to determine whether the user who caused the transaction to occur was located inside or outside the United States.\textsuperscript{154}

The NSA’s acquisition of MCTs is a function of the collection devices it has designed. Based on government representations, the FISC has stated that the “NSA’s upstream Internet collection devices are generally incapable of distinguishing between transactions containing only a single discrete communication to, from, or about a tasked selector and transactions containing multiple discrete communications, not all of which are to, from, or about a tasked selector.”\textsuperscript{155} While some distinction between SCTs and MCTs can be made with respect to some communications in conducting acquisition, the government has not been able to design a filter that would acquire only the single discrete communications within transactions that contain a Section 702 selector. This is due to the constant changes in the protocols used by Internet service providers and the services provided.\textsuperscript{156} If time

---

\textsuperscript{150} The “active user” is the actual human being who is interacting with a server to engage in an Internet transaction.


\textsuperscript{152} December 2011 Joint Statement, \textit{supra}, at 7.


\textsuperscript{154} Bates October 2011 Opinion, \textit{supra}, at 38-40, 2011 WL 10945618, at *12. With respect to this last category, the unidentified user could be the Section 702 target. \textit{Id.} at 38, 40-41, 2011 WL 10945618, at *12.

\textsuperscript{155} Bates October 2011 Opinion, \textit{supra}, at 31, 2011 WL 10945618, at *10. In 2011, the NSA was able to determine that approximately 90 percent of all upstream Internet transactions consisted of SCTs as the result of a post-acquisition statistical sample that required a manual review. \textit{Id.} at 34 n.32, 2011 WL 10945618, at *11.

were frozen and the NSA built the perfect filter to acquire only single, discrete communications, that filter would be out-of-date as soon as time was restarted and a protocol changed, a new service or function was offered, or a user changed his or her settings to interact with the Internet in a different way. Conducting upstream Internet acquisition will therefore continue to result in the acquisition of some communications that are unrelated to the intended targets.

The fact that the NSA acquires Internet communications through the acquisition of Internet transactions, be they SCTs or MCTs, has implications for the technical measures, such as IP filters, that the NSA employs to prevent the intentional acquisition of wholly domestic communications. With respect to SCTs, wholly domestic communications that are routed via a foreign server for any reason are susceptible to Section 702 acquisition if the SCT contains a Section 702 tasked selector. With respect to MCTs, wholly domestic communications also may be embedded within Internet transactions that also contain foreign communications with a Section 702 target. The NSA’s technical means for filtering domestic communications cannot currently discover and prevent the acquisition of such MCTs.

Because of the greater likelihood that upstream collection of Internet transactions, in particular MCTs, will result in the acquisition of wholly domestic communications and extraneous U.S. person information, there are additional rules governing the querying, retention, and use of such upstream data in the NSA minimization procedures. These additional procedures are discussed below.


As is discussed above, the government targets persons under Section 702 by tasking selectors — communication facilities, such as email addresses and telephone numbers — that the government assesses will be used by those persons to communicate or receive foreign intelligence information that falls within one of the authorized Section 702 certifications. Under Section 702, this targeting process to determine which persons are (1) non-U.S. persons, that are (2) reasonably believed to be located outside the United States, who will (3) use the tasked selectors to communicate or receive foreign intelligence

157 Bates October 2011 Opinion, supra, at 34-35, n.32 & n.33; id. at 45, 2011 WL 10945618, at *11 ("[T]he government readily concedes that NSA will acquire a wholly domestic “about” communication if the transaction containing the communication is routed through an international Internet link being monitored by NSA or is routed through a foreign server.")


159 See, e.g., AUGUST 2013 SEMIANNUAL ASSESSMENT, supra, at A-2.
information is governed by targeting procedures. While the targeting procedures are subject to judicial review by the FISC, individual targeting determinations made under these targeting procedures are not reviewed by the FISC (but are subject to internal Executive oversight, as detailed below).

Both the NSA and FBI have targeting procedures that govern the process by which persons may be targeted under Section 702. While some information has been released by the government, neither the NSA nor the FBI targeting procedures have been declassified in full. The NSA’s Section 702 targeting procedures take primary importance because only the NSA may initiate Section 702 collection. The FBI’s Section 702 targeting procedures, which are discussed further below, are applied to certain selectors only after the NSA has previously determined under the NSA targeting procedures that these selectors qualify for Section 702 targeting. Although the NSA initiates all Section 702 targeting, and thus makes all initial decisions pursuant to its targeting procedures regarding whether a person qualifies for Section 702 targeting under one of the Section 702 certifications, the CIA and FBI have processes to “nominate” targets to the NSA for Section 702 targeting. It is the NSA, however, that must make the determination whether to initiate targeting.

Section 702 targeting begins when an NSA analyst discovers or is informed of a foreign intelligence lead — specifically, information indicating that a particular person may possess or receive the types of foreign intelligence information described within one of the Section 702 certifications. Lead information could come from any of multiple sources, including human intelligence, signals intelligence or other sources such as law enforcement information. Because Section 702 acquisition is selector-based, the NSA analyst must also

---

162 NSA DCLPO REPORT, supra, at 2, 4-5.
163 AUGUST 2013 SEMIANNUAL ASSESSMENT, supra, at 6, 9.
164 See The Intelligence Community’s Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, supra, at 3 (noting that “NSA takes the lead in targeting and tasks both telephone and electronic communications selectors to acquire communications); AUGUST 2013 SEMIANNUAL ASSESSMENT, supra, at 6 (“[A]ll Section 702 targeting is initiated pursuant to the NSA’s targeting procedures.”).
165 The Intelligence Community’s Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, supra, at 3.
166 AUGUST 2013 SEMIANNUAL ASSESSMENT, supra, at A-8, A-12.
167 NSA DCLPO REPORT, supra, at 4.
discover or be informed of a specific selector used by this potential target that could be tasked to PRISM and/or upstream collection.\textsuperscript{168}

Having identified a potential person to target through the tasking of a selector, the NSA analyst must then apply the targeting procedures. These procedures require the NSA analyst to make a determination regarding the assessed location and non-U.S. person status of the potential target (the \textit{foreignness determination})\textsuperscript{169} and whether the target possesses and/or is likely to communicate or receive foreign intelligence information authorized under an approved certification (the \textit{foreign intelligence purpose determination}).\textsuperscript{170}

\textbf{A. Foreignness Determination}

With respect to the \textit{foreignness determination}, the NSA analyst is required to assess whether the target of the acquisition is a non-U.S. person reasonably believed to be located outside the United States based upon the totality of the circumstances available.\textsuperscript{171} This analysis begins with a review of the initial lead information, which must be examined to determine whether it indicates either the location or the U.S. person status of the potential target.\textsuperscript{172} At times, the lead information itself will state where the target is assessed to be located and their U.S. person status. In other instances, this information may only enable an analyst to infer location or U.S. person status. In either case, the Section 702 targeting determination may not be made upon the lead information alone. Instead, the NSA analyst must check multiple sources and make a determination based on the totality of the circumstances available to the analyst.\textsuperscript{173}

The government has stated that in making this foreignness determination the NSA targeting procedures inherently impose a requirement that analysts conduct “due diligence” in identifying these relevant circumstances. What constitutes due diligence will

\textsuperscript{168} NSA DCLPO REPORT, supra, at 4.

\textsuperscript{169} PCLOB March 2014 Hearing Transcript, \textit{supra}, at 41 (statement of Rajesh De, General Counsel, NSA) (stating that “foreignness determination” is a “shorthand for referring to the determination that [the target] is a non-U.S. person reasonably located to be abroad”).

\textsuperscript{170} PCAOB March 2014 Hearing Transcript, \textit{supra}, at 61 (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ) (describing individualized foreign intelligence purpose determination which must be documented as part of the tasking process).

\textsuperscript{171} NSA DCLPO REPORT, \textit{supra}, at 4; PCLOB March 2014 Hearing Transcript, \textit{supra}, at 42 (statement of Rajesh De, General Counsel, NSA) (noting that foreignness determination is a “totality of the circumstances” test).

\textsuperscript{172} The Intelligence Community’s Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, \textit{supra}, at 3.

\textsuperscript{173} NSA DCLPO REPORT, \textit{supra}, at 4; PCLOB March 2014 Hearing Transcript, \textit{supra}, at 41 (statement of Rajesh De, General Counsel, NSA) (in describing foreignness determination, stating that “an analyst must take into account all available information. . . [A]n analyst cannot ignore any contrary information to suggest that that is not the correct status of the person.”)
vary depending on the target; tasking a new selector used by a foreign intelligence target with whom the NSA is already quite familiar may not require deep research into the target’s (already known) U.S. person status and current location, while a great deal more effort may be required to target a previously unknown, and more elusive, individual. As previously discussed above, a failure by an NSA analyst to conduct due diligence in identifying relevant circumstances regarding the location and U.S. person status of a Section 702 target is a reportable compliance incident to the FISC.

After conducting due diligence and reviewing the totality of the circumstances, the NSA analyst is required to determine whether the information indicates that the target is a non-U.S. person reasonably believed to be located outside the United States.\textsuperscript{174} The government has stated, and the Board’s review has confirmed, that this is not a “51% to 49% test.”\textsuperscript{175} If there is conflicting information indicating whether a target is located in the United States or is a U.S. person, that conflict must be resolved and the user must be determined to be a non-U.S. person reasonably believed to be located outside the United States prior to targeting.\textsuperscript{176}

While conflicting information must be resolved, the standard for making the foreignness determination is not a probable cause standard. Through the application of the NSA targeting procedures over the years and interactions with and between and among NSA personnel and external DOJ/Office of the Director of National Intelligence (“ODNI”) overseers, a common understanding has been developed regarding what constitutes a sufficient basis for determining that a potential Section 702 target is a non-U.S. person reasonably believed to be located outside the United States. The NSA targeting procedures include a process for assessing non-U.S. person’s status. This determination may not be made unless the analyst has first undertaken due diligence.

In 2013, the DOJ undertook a review designed to assess how often the foreignness determinations that the NSA made under the targeting procedures as described above turned out to be wrong — i.e., how often the NSA tasked a selector and subsequently realized after receiving collection from the provider that a user of the tasked selector was either a U.S. person or was located in the United States. The DOJ reviewed one year of data and determined that 0.4% of NSA’s targeting decisions resulted in the tasking of a selector that, as of the date of tasking, had a user in the United States or who was a U.S. person. As is discussed in further detail below, data from such taskings in most instances must be

\textsuperscript{174} See PCLOB March 2014 Hearing Transcript, \textit{supra}, at 40-42 (statement of Rajesh De, General Counsel, NSA).

\textsuperscript{175} PCLOB March 2014 Hearing Transcript, \textit{supra}, at 40-41 (statement of Rajesh De, General Counsel, NSA).

\textsuperscript{176} NSA DCLPO REPORT, \textit{supra}, at 4; PCLOB March 2014 Hearing Transcript, \textit{supra}, at 40-42 (statement of Rajesh De, General Counsel, NSA).
purged. The purpose of the review was to identify how often the NSA’s foreignness determinations proved to be incorrect. Therefore, the DOJ’s percentage does not include instances where the NSA correctly determined that a target was located outside the United States, but post-tasking, the target subsequently traveled to the United States.

B. Foreign Intelligence Purpose Determination

In addition to the foreignness determination, the NSA analyst must also make a foreign intelligence purpose determination. Specifically, the NSA targeting procedures require that the NSA determine that tasking the selector will be likely to acquire one of the types of foreign intelligence information identified in a Section 702 certification. In making this determination, the NSA analyst must identify the specific foreign power or foreign territory concerning which the foreign intelligence information is being sought. The NSA targeting procedures include a non-exclusive list of factors that the NSA will consider in determining whether the tasking of a selector will be likely to result in foreign intelligence information falling within one of the Section 702 certifications.

C. Documentation Requirements

The NSA targeting procedures contain documentation requirements with respect to aspects of the foreignness and foreign intelligence purpose determinations. Analysts are required under the NSA targeting procedures to cite the specific documents and communications that led them to assess that the Section 702 target is located outside the United States. As a practical matter, these citations are accompanied by a narrative explaining what the documents and communications indicate with regard to the location of the target. In other words, with respect to the determination regarding the location of the target, analysts must “show their work.” Although analysts are required under the targeting procedures to conduct an analysis regarding why the targeting of the individual will result in obtaining foreign intelligence information under the Section 702 certifications, analysts are not required to document (i.e., show their work) this foreign intelligence purpose determination in the same manner as they are required to document the foreignness determination. With respect to the foreign intelligence purpose, the NSA targeting procedures require the analyst only to “identify” the foreign power or foreign territory regarding which the foreign intelligence information is to be acquired. By policy, but not as a requirement of the targeting procedures, the NSA also requires that all taskings be accompanied by a very brief statement (typically no more than one sentence

177 NSA DCLPO REPORT, supra, at 4.
178 See AUGUST 2013 SEMIANNUAL ASSESSMENT, supra, at A-5 (noting that the identified foreign power or foreign territory must be documented).
179 AUGUST 2013 SEMIANNUAL ASSESSMENT, supra, at A-5; see also NSA DCLPO REPORT, supra, at 4-5.
180 AUGUST 2013 SEMIANNUAL ASSESSMENT, supra, at A-5.
long) that further explains the analyst’s rationale for assessing that tasking the selector in question will result in the acquisition of the types of foreign intelligence information authorized by the Section 702 certifications.\textsuperscript{181}

In the Board’s view, this reduced documentation regarding the foreign intelligence purpose determination results in a less rigorous review by the NSA’s external overseers of the foreign intelligence purpose determinations than the NSA’s foreignness determination. Also as a matter of NSA policy, as opposed to a requirement in the NSA targeting procedures, NSA analysts document the assessed non-U.S. person status of the target, but analysts do not separately document the basis for this non-U.S. person determination. In general, however, the non-U.S. person analysis is based upon same information that underlies the determination regarding the target’s location.

D. Approvals

Once analysts have documented their determinations in an NSA tasking database,\textsuperscript{182} the tasking request undergoes two layers of review before actual Section 702 acquisition is initiated.\textsuperscript{183} Two different senior NSA analysts must review the documentation accompanying the tasking request to ensure that it meets all of the requirements of the NSA targeting procedures.\textsuperscript{184} Both NSA senior analysts receive additional training to review tasking requests.\textsuperscript{185} Both senior analysts may also request additional information prior to approving or denying the Section 702 tasking request.\textsuperscript{186} Both senior analysts are required to review all aspects of the tasking before approving the tasking request.\textsuperscript{187}

Once the tasking request receives all of the necessary approvals, it is sent to one or more electronic communication service providers that have received a Section 702 directive in order to initiate Section 702 acquisition.\textsuperscript{188} The tasking request, however, is subjected to further post-tasking review by the DOJ/ODNI review team,\textsuperscript{189} as is discussed in the “External Oversight” section below.

\textsuperscript{181} See generally PCLOB March 2014 Hearing Transcript, \textit{supra}, at 59 (statement of Rajesh De, General Counsel, NSA) (discussing foreign intelligence purpose determination and noting that it must be "documented in a targeting rationale document").

\textsuperscript{182} August 2013 Semiannual Assessment, \textit{supra}, at A-5.

\textsuperscript{183} NSA DCLPO REPORT, \textit{supra}, at 5.

\textsuperscript{184} NSA DCLPO REPORT, \textit{supra}, at 5.

\textsuperscript{185} NSA DCLPO REPORT, \textit{supra}, at 5.

\textsuperscript{186} NSA DCLPO REPORT, \textit{supra}, at 5.

\textsuperscript{187} NSA DCLPO REPORT, \textit{supra}, at 5.

\textsuperscript{188} NSA DCLPO REPORT, \textit{supra}, at 5.

\textsuperscript{189} NSA DCLPO REPORT, \textit{supra}, at 5; AUGUST 2013 SEMIANNUAL ASSESSMENT, \textit{supra}, at 6-7.
E. CIA and FBI Nominations

The CIA and FBI have both developed processes to nominate selectors to the NSA to be tasked for Section 702 acquisition.\(^\text{190}\) The NSA evaluates the CIA and FBI nominations under the same targeting procedures and using the same processes that are described above. It is the NSA that is ultimately responsible for the tasking of such facilities. In order to ensure that the NSA’s foreignness and foreign intelligence purpose determinations regarding the CIA and FBI nominations are made on accurate and current information, both the CIA and FBI have implemented internal requirements prior to formally nominating a selector to the NSA for acquisition. For example, the CIA nominations are reviewed and approved by the targeting officer’s first line manager, a legal officer, a senior operational manager, and the CIA’s FISA Program office prior to being exported to the NSA.\(^\text{191}\) These internal procedures are in addition to the NSA documentation and approval requirements required for all taskings.

F. FBI Targeting Procedures

The FBI’s targeting procedures govern certain aspects of the PRISM program; specifically, requests for certain communications for selectors that have already been determined by the NSA to have met its targeting procedures. As the NSA has already made a foreignness determination with respect to any selector for which the FBI will be acquiring communications, the FBI’s role in targeting is substantially different than that of the NSA.\(^\text{192}\) Instead of establishing the required information to indicate that a Section 702 target is a non-U.S. person reasonably believed to be located outside the United States who is likely to communicate or receive foreign intelligence information, the FBI targeting procedures are intended to “provide additional assurance that the users of tasked accounts are non-United States persons located outside the United States.”\(^\text{193}\) The FBI targeting procedures therefore require the FBI to both review the NSA’s foreignness determinations\(^\text{194}\) and review information available to the FBI. FBI personnel who process tasking requests receive training in both the FBI targeting procedures and a detailed set of standard operating procedures that describe the steps that the FBI must take to ensure that they

---

\(^{190}\) See supra footnote 1664 and accompanying text.

\(^{191}\) August 2013 Semiannual Assessment, supra, at A-8; see also August 2013 Semiannual Assessment at 36 (describing compliance incident related to an FBI nomination that stemmed from reliance on an unsupported fact).

\(^{192}\) The Intelligence Community’s Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, supra, at 3.


\(^{194}\) The Intelligence Community’s Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, supra, at 3.
have conducted due diligence in looking for information that may alter or affect the NSA’s foreignness assessment.\footnote{August 2013 Semiannual Assessment, supra, at 36, A-11 to A-12.}

\section*{V. Post-Tasking Review and Related Reporting and Purging Requirements}

In addition to defining the process by which Section 702 tasking will be initiated, the NSA targeting procedures also impose additional post-tasking requirements designed to ensure that the users of tasked selectors remain non-U.S. persons located outside the United States and that acquisition against the selector continues only insofar as the government assesses that the tasking is likely to acquire foreign intelligence information within one of the authorized Section 702 certifications. The manner in which the post-tasking checks required by the NSA targeting procedures will be implemented has been supplemented by additional filings by the government with the FISC. The government has reported to the FISA court and Congress as compliance incidents instances in which its implementation of the required post-tasking checks did not correspond with these additional representations to the court.

NSA analysts are required to routinely review at least a sample of the Section 702–acquired communications for selectors that they have tasked to ensure that the selectors remain properly tasked.\footnote{August 2013 Semiannual Assessment, supra, at A-4; NSA DCLPO Report, supra, at 6.} The NSA has developed automated systems to remind analysts to review collection from email addresses and comparable selectors within five business days after the first instance that data is acquired for a particular tasked selector, and at least every 30 days thereafter; comparable systems have to-date not been implemented with respect to Section 702 acquisition of upstream telephony collection. The analysts review the content to verify that the selector is associated with the foreign intelligence target, as well as look for any information indicating that a user of the selector is a U.S. person or located in the United States.\footnote{NSA DCLPO Report, supra, at 6; see also PCLOB March 2014 Hearing Transcript, supra, at 42 (statement of Rajesh De, General Counsel, NSA) (noting that “analysts have an affirmative obligation to periodically revisit the foreignness determination”)}

The NSA also requires analysts to re-verify at least once a year that each selector continues to be tasked in order to acquire the types of foreign intelligence information specified in the certification under which the selector is tasked. The CIA and FBI have each implemented their own comparable policies and practices mandating that analysts, agents, and officers initially review and periodically verify data acquired from selectors nominated by the CIA and FBI to ensure the selectors remain properly tasked for Section 702 acquisition.
In addition to this content review, the NSA is required to conduct routine post-tasking checks of all Section 702–tasked selectors.\textsuperscript{198}

If it is determined that a user of a tasked selector is either in the United States or is a U.S. person, the selector is required to be promptly detasked from Section 702 acquisition (i.e., all Section 702 acquisition directed at that selector must be terminated).\textsuperscript{199} Any other Section 702–tasked selectors assessed to be used by the individual determined to be a U.S. person or located in the United States must also be promptly detasked.\textsuperscript{200} Additionally, selectors must be detasked if the government determines that it will not obtain the types of foreign intelligence information authorized under the Section 702 certifications.\textsuperscript{201} Failure to detask a selector from Section 702 acquisition after it has been (or, based on the available information, should have been) determined to be ineligible for further Section 702 acquisition is a compliance incident that must be reported first to the DOJ and ODNI, and in turn to the FISC and Congress.\textsuperscript{202}

If it is learned that a tasked selector is being used by a U.S. person or person located in the United States, the data acquired from the selector while it was being used by the U.S. person or person located in the United States is subject to purge, with limited exceptions.\textsuperscript{203} If the data was acquired as a result of a compliance incident — because, for example, there was an error in the tasking (e.g., typographical error, lack of due diligence tasking, etc.); an error in detasking (insufficiently prompt detasking); or an overproduction by the provider — the acquired communications must be purged.\textsuperscript{204} In cases where there is no underlying compliance incident but a user is determined to be a U.S. person or a person located in the United States (e.g., the government had a reasonable, but ultimately mistaken, belief that a target was located outside the United States), a purge of acquired communications is also required.\textsuperscript{205}

\textsuperscript{198} \textit{August 2013 Semiannual Assessment}, supra, at 6.
\textsuperscript{199} NSA DCLPO REPORT, supra, at 6; see also NSA October 2011 Minimization Procedures, supra, § 3(d)(1).
\textsuperscript{200} NSA DCLPO REPORT, supra, at 6; see also NSA October 2011 Minimization Procedures, supra, § 3(d)(1).
\textsuperscript{201} NSA DCLPO REPORT, supra, at 6.
\textsuperscript{202} \textit{See August 2013 Semiannual Assessment, supra, at 7} (noting that the NSA must report all instances in which a target is found to be located in the United States, but that such incidents are only compliance incidents if the NSA “knew or should have known the target was in the United States during the collection period”); \textit{id. at 25-27, 29, 33} (describing the category of detasking incidents and specific detasking incidents); NSA DCLPO REPORT, supra, at 3 (summarizing reporting process).
\textsuperscript{203} NSA DCLPO REPORT, supra, at 8.
\textsuperscript{204} See, e.g., PCLOB March 2014 Hearing Transcript, supra, at 72.
\textsuperscript{205} \textit{August 2013 Semiannual Assessment, supra, at A-12} (noting that all of the agency minimization procedures require purges when a target is discovered to be a U.S. person or person located in the United States, with limited exceptions).
Certain exceptions apply, however, in instances where the communications were not acquired as the result of a violation of the targeting or minimization procedures. The NSA minimization procedures permit the Director (or Acting Director) of the NSA to waive, on a communication-by-communication basis, specific communications determined to contain "significant foreign intelligence information" or information that is not foreign intelligence information but is "evidence of a crime.\textsuperscript{206} The CIA and FBI standards for executing a waiver are similar. Additionally, and notwithstanding the general purge requirement and the specific waiver exceptions, the NSA may also inform the FBI that a target has entered the United States so that the FBI may seek traditional FISA electronic surveillance of the target or take other lawful investigative steps.\textsuperscript{207} The NSA may also retain and disclose to the FBI and CIA certain technical data for collection avoidance purposes.\textsuperscript{208}

VI. Minimization and Related Requirements: What Are the Limitations Regarding How the Data is Acquired, Who May View It, How Long It Is Retained, and with Whom It May be Shared?

Minimization is one of the most confusing terms in FISA. Like traditional FISA electronic surveillance and physical search,\textsuperscript{209} Section 702 requires that all acquired data be subject to "minimization procedures."\textsuperscript{210} Minimization procedures are best understood as a set of controls on data to balance privacy and national security interests. Specifically, under FISA, minimization procedures must be "specific procedures . . . that are reasonably designed in light of the purpose and technique of the particular surveillance to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."\textsuperscript{211} Minimization procedures must also contain special limitations on the dissemination of U.S.

\textsuperscript{206} NSA October 2011 Minimization Procedures, supra, § 5(1) and (2). The NSA’s minimization procedures also allow for the Director of the NSA to waive the purge of a communication that is assessed to contain "technical data base information," “information necessary to understand or assess a communications security vulnerability,” or “information pertaining to a threat of serious harm to life or property.” NSA October 2011 Minimization Procedures § 5(3), (4). To date, no waivers have been granted under these additional provisions.

\textsuperscript{207} NSA October 2011 minimization procedures, supra, § 5.

\textsuperscript{208} NSA October 2011 minimization procedures, supra, § 5.

\textsuperscript{209} See 50 U.S.C. §§ 1805(a)(3) and 1824(a)(3).

\textsuperscript{210} 50 U.S.C. § 1881a(e).

\textsuperscript{211} 50 U.S.C. 1801(h)(1) (emphasis added).
person identities with respect to certain types of foreign intelligence information,\textsuperscript{212} as well as allow for the retention and dissemination of evidence of a crime to law enforcement entities.\textsuperscript{213} These statutory requirements oblige the Attorney General to adopt procedures that balance the at times competing interests in protecting the privacy of U.S. persons and the Intelligence Community’s production of foreign intelligence information to meet national security requirements. In addition, although the minimization procedures must be designed to protect U.S. persons’ privacy, the procedures will at times provide controls on data that protect the privacy of non-U.S. persons as well.

This section describes the controls imposed by the Section 702 minimization procedures on acquisition, access (and related training requirements), querying, retention (and purging), and dissemination. The NSA’s 2011 Section 702 minimization procedures have been publicly released.\textsuperscript{214} Minimization procedures for the CIA, FBI, and National Counterterrorism Center ("NCTC")\textsuperscript{215} have not been publicly released to date, though some information regarding these procedures has been declassified. Although the minimization procedures for each agency have many similarities, there are differences between the agencies’ minimization procedures that are related to the different authorities of the respective agencies and the way each uses the Section 702–acquired data.\textsuperscript{216} Some of these differences impact privacy concerns.

All Section 702–acquired data, both content and metadata, is subject to the Section 702 minimization procedures.\textsuperscript{217}

**A. Acquisition**

The minimization procedures of agencies that conduct acquisition — in the case of Section 702, the NSA and FBI — must contain provisions that minimize the acquisition of U.S. person information consistent with the authorized purpose of the collection. The first minimization of the acquisition of U.S. person information, however, stems from the targeting requirements imposed by the statute itself. As an initial matter, Section 702

\textsuperscript{212} 50 U.S.C.\textsuperscript{a}§ 1801(h)(2) (further limiting dissemination of U.S. person identities with regard to foreign intelligence information as defined by § 1801(e)(2), but not § 1801(e)(1)).

\textsuperscript{213} 50 U.S.C.\textsuperscript{a}§ 1801(h)(3).


\textsuperscript{215} As described below, the NCTC’s role in processing and minimizing Section 702 data is limited. See August 2013 Joint Assessment, supra, at 4 n.2.

\textsuperscript{216} PCLOB March 2014 Hearing Transcript, supra, at 18-19 (discussion between David Medine, Chairman, PCLOB, and Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ).

\textsuperscript{217} PCLOB March 2014 Hearing Transcript, supra, at 19.
prohibits the intentional targeting of U.S. persons, the intentional targeting of persons located in the United States, reverse targeting, or the intentional acquisition of communications known to be wholly domestic at the time of acquisition. Each of these statutory requirements is designed to reduce, though not eliminate, the acquisition of U.S. person information.

The NSA minimization procedures therefore start with a requirement that Section 702 collection be conducted in accordance with the Section 702 certification, and “in a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose.” This mandate applies to both the NSA’s acquisition and the technical assistance provided by the FBI in acquiring communications. Affidavits accompanying the certifications, witness testimony in hearings before the FISC, and additional filings before the court describe how the NSA and FBI will actually conduct the acquisition in a manner that the government believes will be reasonably designed to minimize the acquisition of information that is irrelevant to the acquisition of the foreign intelligence information specified in the Section 702 certifications. These representations detail the method and techniques by which the collection of PRISM and upstream collection is conducted, as described above. A failure to implement the acquisition in a manner that reasonably limits the collection to the authorized purpose of the Section 702 certifications can, and has, led to incidents of noncompliance with the minimization procedures that have been reported to the FISC and Congress.

In addition to actually acquiring the data, certain technical actions must be undertaken at or just after the acquisition stage in order to facilitate later compliance with other minimization rules. For example, data-tagging Section 702-acquired data at, or just after, acquisition is also employed to effectuate other access and routing controls, certain

---

218 50 U.S.C. § 1881a(a), (b).
219 NSA October 2011 Minimization Procedures, supra, § 3(a).
220 See NSA October 2011 Minimization Procedures, supra, § 2(a) (defining “acquisition” as “the collection by NSA or the FBI through electronic means of a non-public communication to which it is not an intended party”).
221 See, e.g., Bates October 2011 Opinion, supra, at 5-10, 2011 WL 10945618, at *2-3 (describing various government submissions regarding how the government conducts Section 702 upstream collection); id. at 15-16, 2011 WL 10945618, at *5 (describing comparable descriptions in prior dockets); id. at 29-41, 2011 WL 10945618, at *9-13 (further describing government descriptions regarding how the government conducts Section 702 upstream collection).
222 See AUGUST 2013 SEMIANNUAL ASSESSMENT, supra, at 31 (describing “compliance incidents during this reporting period [that] resulted in NSA’s systems overcollecting data beyond what was authorized under the Section 702 certifications”).
controls limiting the scope of queries, and age-off and purge requirements. Each of these controls is discussed further below.

**B. Access and Training**

Although the minimization process begins with acquisition, FISA-acquired data that has yet to be reviewed and evaluated by a human being is still referred to by the government as being “unminimized” or “raw” data. The NSA, CIA, and FBI are the three Intelligence Community agencies that have access to such unminimized Section 702–acquired data. Each agency limits access to unminimized Section 702–acquired data to personnel who have been trained to apply their respective agency’s minimization procedures. To enforce these restrictions, all unminimized Section 702–acquired data must be stored in repositories with access controls designed to prevent unauthorized access of the data by those within or outside of the relevant agency.

The NSA’s core access and training requirements are found in the NSA’s targeting procedures, which have not been released to the public. NSA analysts are required to undergo mandatory training and must pass a test regarding the requirements of the Section 702 minimization procedures (among other legal requirements) prior to receiving access to unminimized Section 702–acquired data.

The CIA’s minimization procedures similarly limit access to unminimized Section 702–acquired data to analysts who have received training in the CIA minimization procedures. The CIA conducts in-person training regarding its minimization procedures before its personnel receive access to Section 702 data repositories and also embeds FISA-trained attorneys with CIA personnel to answer questions on the application of those minimization procedures to actual collection.

The FBI has created a mandatory online training course that must be taken before FBI agents or analysts are granted access to repositories of unminimized Section 702–acquired data. The Department of Justice’s National Security Division ("NSD") and the FBI also conduct in-person trainings at FBI field offices.

---

227 *August 2013 Semiannual Assessment*, supra, at 14 and A-12; see also PCLOB March 2014 Hearing Transcript at 86 (statement of James A. Baker, General Counsel, FBI) (confirming that access controls exists for FBI systems holding Section 702–acquired data).
228 *August 2013 Semiannual Assessment*, supra, at 14.
When an analyst, agent, or officer is granted access to unminimized Section 702–acquired data after receiving the requisite training, this does not mean that the agent or analyst has access to all such data. Agencies separate acquired data as a security measure. Furthermore, the CIA and FBI do not have copies of all Section 702–acquired data as neither agency receives all PRISM data acquired by the NSA, nor does either agency receive upstream collection.229

In addition to these general access and training requirements, the NSA’s minimization procedures impose supplemental requirements with respect to certain Internet transactions. When the “active user” (i.e., the actual human being who is interacting with a server to engage in an Internet transaction) associated with an MCT is either reasonably believed to be located in the United States, or when the NSA cannot determine where the active user is located, the NSA must segregate the MCT in a special access-controlled repository.230 Only analysts who have been trained in how to review such communications to identify any wholly domestic communications within such MCTs are permitted access to this repository.231 A multi-communication transaction may not be moved out of the special-access repository or otherwise used unless it has been determined that none of the discrete communications that make up the MCT are wholly domestic communications.232 If an MCT within this repository is determined to contain a wholly domestic communication, it must be destroyed upon recognition.233 The CIA and FBI do not have access to any unminimized Section 702–acquired upstream collection.234

Separately, certain access and training requirements are imposed by the NCTC’s Section 702 minimization procedures. The NCTC does not have access to unminimized Section 702–acquired data.235 The NCTC has, however, been provided access to certain FBI systems that contain Section 702–acquired data that has been minimized to meet the FBI’s dissemination standard. Minimization in this context means that any nonpublicly available Section 702–acquired U.S. person information in these FBI systems has been determined to either be foreign intelligence information, necessary to understand or assess the importance of foreign intelligence information, or evidence of a crime.236 U.S. person information that is evidence of a crime but is not otherwise foreign intelligence

230 NSA October 2011 Minimization Procedures, supra, § 3(b)(5)(a).
231 NSA October 2011 Minimization Procedures, supra, § 3(b)(5)(a)(1).
233 NSA October 2011 Minimization Procedures, supra, § 3(b)(5)(a)(1)(a).
235 AUGUST 2013 SEMIANNUAL ASSESSMENT, supra, at 4 n.2.
236 AUGUST 2013 SEMIANNUAL ASSESSMENT, supra, at 4 n.2.
information, however, may only be disseminated for law enforcement purposes, and the NCTC is not a law enforcement agency. The NCTC Section 702 minimization procedures require NCTC personnel who have been granted access to these FBI systems to first be trained to not use, retain, or disseminate purely law enforcement information, and to purge any such Section 702–acquired information from NCTC systems if it has been ingested.

C. Querying the Acquired Data

The NSA, CIA, and FBI’s Section 702 minimization procedures all permit these agencies to query unminimized Section 702–acquired information. A “query” refers to any instance where data is searched using a specific term or terms for the purpose of discovering or retrieving unminimized Section 702–acquired content or metadata. A query “term” or “identifier” is just like a search term that is used in an Internet search engine — the term could be, for example, an email address, a telephone number, a key word or phrase, or a specific identifier that an agency has assigned to an acquired communication. Queries are conducted using one or more of such terms or identifiers. Section 702 queries are of data that has already been acquired through the tasking of selectors as described above. A query therefore does not cause the government to collect any new communications, but queries do permit the government to more efficiently search through and discover information in the data the government has already acquired.

An aspect common to the implementation of the query provisions in all of the Section 702 minimization procedures is that an analyst or agent only receives unminimized Section 702–acquired data as a result of a query if that analyst or agent has the appropriate training and authorization to access the Section 702 data. Different agencies accomplish this in different ways. For example, the CIA limits access to the database containing unminimized Section 702–acquired data to personnel who have received training in the CIA’s Section 702 minimization procedures, thereby preventing untrained individuals from conducting queries of this data. The NSA, on the other hand, often stores data acquired from multiple legal authorities in a single data repository. Instead of limiting access to whole databases, the NSA tags each acquired communication with the legal authority under which it was acquired, and then has systems that prevent an analyst from accessing or querying data acquired under a legal authority for which the analyst does not have the

---

238 August 2013 Semiannual Assessment, supra, at 4 n.2.
239 August 2013 Semiannual Assessment, supra, at 4 n.2.
240 See, e.g., NSA DCLPO Report, supra, at 6; NSA October 2011 Minimization Procedures, supra, § 3(b)(6).
241 PCLOB March 2014 Hearing Transcript, supra, at 29-31 (statements of Rajesh De, General Counsel, NSA and Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ).
requisite training. At the FBI, an agent or analyst who conducts a “federated query” across multiple databases, but who does not have Section 702 training, would not receive the Section 702–acquired information as the result of a query. The agent or analyst would, however, be notified in their query results of the fact that there is responsive information to their query in a database containing unminimized Section 702–acquired information to which he or she does not have access. In order to gain access to this information, the analyst or agent would need to either take the requisite training to gain access to the Section 702 information or contact a fellow agent or analyst who had the requisite training to determine whether the responsive results can be disseminated pursuant to the minimization procedures.

The NSA’s intelligence analysts conduct at times complex queries across large data sets. The NSA’s minimization procedures require that queries of unminimized Section 702–acquired information be designed such that they are “reasonably likely to return foreign intelligence information.” This prohibition against overbroad queries (such as a query for the term “river” across all Section 702–acquired data with no other limiting query terms) or queries conducted for purposes other than to identify foreign intelligence information (such as an analyst’s query to find information about a girlfriend) applies to all of the NSA queries of unminimized Section 702–acquired information, not just queries containing U.S. person identifiers. NSA analysts receive training regarding how to use multiple query terms or other query discriminators (like a date range) to limit the information that is returned in response to their queries of the unminimized data. Through various means, the NSA systems record all queries of unminimized Section 702–acquired data, and these records are subject to audit.

Additional rules apply when an NSA analyst wants to use a U.S. person identifier — i.e., a query term associated with a specific U.S. person, such as an email address or telephone number — to query unminimized Section 702–acquired data. U.S. person identifiers are prohibited from being used to query the NSA’s Section 702 upstream collection of Internet transactions. In contrast, the NSA’s upstream telephony collection

---

242 See NSA DCLPO REPORT, supra, at 6-7.
243 NSA October 2011 Minimization Procedures, supra, § 3(b)(6).
244 See NSA DCLPO REPORT, supra, at 6-7 (discussing general query restrictions prior to detailing the additional requirements with regard to U.S. person identifiers).
245 NSA DCLPO REPORT, supra, at 6-7; see also NSA October 2011 Minimization Procedures, supra, § 3(b)(6) (noting that “other discriminators” may be used in constructing queries).
246 NSA DCLPO REPORT, supra, at 7.
247 NSA October 2011 Minimization Procedures, supra, § 3(b)(6).
and PRISM data may be queried using U.S. person identifiers if those U.S. person identifiers have been approved pursuant to internal NSA procedures.\footnote{\textit{NSA October 2011 Minimization Procedures, supra}, § 3(b)(6).}

The NSA’s internal procedures treat queries of metadata and content using U.S. person identifiers differently.\footnote{\textit{NSA DCLPO REPORT, supra}, at 7.} The NSA’s internal procedures require that queries of metadata using a U.S. person identifier be conducted only in a system or systems that require analysts to document the basis for their metadata query prior to conducting the query. Analysts are trained prior to using such systems. The NSA reported that it conducted approximately 9,500 metadata queries using U.S. person identifiers in 2013. In reviewing these queries, the NSD and ODNI have found that this number is likely substantially overinclusive of the actual number of U.S. person metadata queries conducted because many query terms that had been labeled as U.S. person identifiers proved on further analysis to not be identifiers of U.S. persons.

With respect to content queries using U.S. person identifiers, the NSA’s internal procedures take a white-listing approach. Specifically, content queries using U.S. person identifiers are not permitted unless the U.S. person identifiers have been pre-approved (i.e., added to a white list) through one of several processes, several of which incorporate other FISA processes. For example, the NSA has approved the use of content queries using identifiers of U.S. persons currently subject to FISC-approved electronic surveillance under Section 105 or targeting under Section 704. U.S. person identifiers can also be approved by NSA’s Office of General Counsel after a showing is made regarding why the proposed use of the U.S. person identifier would be “reasonably likely to return foreign intelligence information;” all approvals to use U.S. person identifiers to query content must be documented.\footnote{\textit{NSA October 2011 Minimization Procedures, supra}, § 3(b)(6); \textit{NSA DCLPO REPORT, supra}, at 7.} In 2013, the NSA approved 198 U.S. person identifiers to be used as content query terms. The NSA minimization procedures mandate that the DOJ’s National Security Division and ODNI conduct oversight of the NSA’s U.S. person queries. The NSD and ODNI’s oversight of the NSA and other agencies queries is further detailed below.

The CIA’s minimization procedures similarly permit the CIA to query unminimized Section 702–acquired data using U.S. person identifiers to discover foreign intelligence information.\footnote{\textit{Bates October 2011 Opinion, supra}, at 25, 2011 WL 10945618, at *8; \textit{AUGUST 2013 SEMIANNUAL ASSESSMENT, supra}, at 13.} The CIA’s minimization procedures require that all queries of unminimized content, whether or not a U.S. person identifier is used in the query, must be “reasonably designed to find and extract foreign intelligence information.” The CIA minimization procedures state that the CIA must keep records of all such content queries.
In implementing its query provision, the CIA has not required its personnel to seek pre-approval of U.S. person content queries, but it does record who conducts those queries and requires analysts to both identify any U.S. person identifiers used as query terms and to write a contemporaneous foreign intelligence justification for any query of unminimized Section 702–acquired content using a U.S. person identifier.\footnote{August 2013 Semiannual Assessment, supra, at 8 ("NSD and ODNI also review CIA’s written justifications for all queries using United States person identifiers of the content of unminimized Section 702-acquired communications.")}. The CIA’s content queries, for example, involve U.S. persons located overseas that intelligence indicates may be engaged in facilitating international terrorism.

In 2013, the CIA conducted approximately 1,900 content queries using U.S. person identifiers. Approximately forty percent of these content queries were at the request of other U.S. intelligence agencies. Some identifiers were queried more than once; the CIA has advised that approximately 1,400 unique identifiers were queried during this period. The NSD and ODNI are required under the CIA minimization procedures to review these records.

Metadata queries are treated differently under the CIA’s minimization procedures. The CIA minimization procedures do not contain a standard for conducting metadata queries, although the statute and internal CIA procedures do require that queries may not be conducted for an unauthorized purpose (such as trying to find information about a love interest). If the CIA did identify any metadata associated with the individual, however, the CIA is permitted to conduct a further query into the underlying content only if the query is to identify foreign intelligence information, and the CIA may only disseminate the results of content or metadata queries to the requesting entity if the dissemination of information was otherwise permissible under the CIA’s minimization procedures, as described below. The CIA does not track how many metadata-only queries using U.S. person identities have been conducted.

The FBI minimization procedures also permit the FBI to query unminimized Section 702–acquired data.\footnote{PCLOB March 2014 Hearing Transcript, supra, at 86 (statement of James A. Baker, General Counsel, FBI) (noting that the FBI queries such data).} Stemming from its role as both a foreign intelligence and a law enforcement agency, the FBI’s minimization procedures differ from the NSA and CIA’s procedures insofar as they permit the FBI to conduct reasonably designed queries “to find and extract” both “foreign intelligence information” and “evidence of a crime.” Although, consistent with 50 U.S.C. § 1806(a), any use of Section 702–acquired information regarding United States or non-U.S. persons may only be used for lawful purposes, the requirement that queries be reasonably designed to identify foreign intelligence information or evidence...
of a crime applies only to U.S. person information. The “reasonably designed” standard applies to both content and metadata queries.

The FBI is required under its minimization procedures to maintain records of all terms used to query content. These records identify the agent or analyst who conducted the query, but do not identify whether the query terms are U.S. person identifiers. Although the FBI’s minimization procedures do not require the FBI to keep records of metadata-only queries, such queries are conducted in the same databases that contain the content collection; therefore, such metadata queries are also recorded. The NSD and ODNI conduct oversight reviews of both the content and metadata queries, as described below.

Because they are not identified as such in FBI systems, the FBI does not track the number of queries using U.S. person identifiers. The number of such queries, however, is substantial for two reasons.

First, the FBI stores electronic data obtained from traditional FISA electronic surveillance and physical searches, which often target U.S. persons, in the same repositories as the FBI stores Section 702–acquired data, which cannot be acquired through the intentional targeting of U.S. persons. As such, FBI agents and analysts who query data using the identifiers of their U.S. person traditional FISA targets will also simultaneously query Section 702–acquired data.

Second, whenever the FBI opens a new national security investigation or assessment, FBI personnel will query previously acquired information from a variety of sources, including Section 702, for information relevant to the investigation or assessment. With some frequency, FBI personnel will also query this data, including Section 702–acquired information, in the course of criminal investigations and assessments that are unrelated to national security efforts. In the case of an assessment, an assessment may be initiated “to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence information.”\footnote{The Attorney General’s Guidelines for Domestic FBI Operations § II.A, available at http://www.justice.gov/ag/readingroom/guidelines.pdf.} If the agent or analyst conducting these queries has had the training required for access to unminimized Section 702–acquired data, any results from the Section 702 data would be returned in these queries. If an agent or analyst does not have access to unminimized Section 702–acquired data — typically because this agent or analyst is assigned to non-national security criminal matters only — the agent or analyst would not be able to view the unminimized data, but would be notified that data responsive to the query exists and could request that an agent or analyst with the proper training and access to review the unminimized Section 702–acquired data. Anecdotally, the FBI has advised the Board that it
is extremely unlikely that an agent or analyst who is conducting an assessment of a non-national security crime would get a responsive result from the query against the Section 702–acquired data.

D. Retention and Purging

FISA also requires that the retention of nonpublicly available U.S. person information be minimized consistent with the need of the United States to obtain, produce, and disseminate information.255 As such, the NSA, CIA, and FBI’s minimization procedures contain provisions regarding when unminimized data must be aged off agency systems, what data must be purged upon recognition, and what types of evaluated information may be retained indefinitely.256 Data that has been evaluated and determined to contain either no U.S. person information or only U.S. person information that meets the standard for permanent retention is referred to as “minimized information.”

With a notable exception, unminimized Section 702–acquired data must be aged off of the NSA and CIA systems no later than five years after the expiration of the Section 702 certification under which that data was acquired.257 Unminimized Internet transactions acquired through the NSA’s upstream collection, however, must be aged off of the NSA systems no later than two years after the expiration of the Section 702 certification under which the data has been acquired.258 The CIA and FBI do not receive, and therefore do not retain, such upstream collection. The FBI’s minimization procedures alone distinguish between acquired data that have not been reviewed and those that have not been determined to meet the retention standard. As with the NSA and CIA, Section 702–acquired communications that have not been reviewed must be aged off FBI systems no later than five years after the expiration of the Section 702 certifications under which the data was acquired. Data that was reviewed but not yet determined to meet the retention standard in the FBI minimization procedures may be kept for a longer retention period subject to additional access controls.

With respect to all of the agencies, extensions from these age-off requirements may be sought from a high-level agency official. Other limited exceptions apply, such as to communications that are still being decrypted.259

256 Although the minimization procedures themselves do not place an outer limit regarding how long such information may be retained, general rules regarding the retention of federal records apply to this data.
257 See, e.g., NSA October 2011 Minimization Procedures, supra, § 3(c)(1); NSA DCLPO REPORT, supra, at 8.
258 NSA October 2011 Minimization Procedures, supra, § 3(c)(1); NSA DCLPO REPORT, supra, at 8.
259 See, e.g., NSA October 2011 Minimization Procedures, supra, § 6(a)(1)(a).
As government personnel engage in the process of evaluating communications, the minimization procedures impose certain requirements requiring communications to be purged upon recognition. As described above, if data has been acquired as a result of a compliance incident, such as a typographical error in the tasking or a failure to detask a selector before a target’s known travel to the United States, any identifiable data acquired as a result of the compliance incident is purged. When a compliance incident is discovered, each agency has a process to discover and destroy data subject to purge. The agencies also must coordinate such purges to ensure that all agencies are both aware of instances when a purge is required and use the same parameters to identify data subject to purge.

Whether or not the communications were acquired as a result of a compliance incident, purges are required whenever a user of a tasked selector has been determined to be a U.S. person or located in the United States at any point during the acquisition. These purge requirements, and the exceptions to these requirements, have been detailed above. In addition, the NSA’s minimization procedures include additional purge-upon-recognition requirements due to the possibility that the NSA’s upstream collection of Internet transactions could acquire domestic communications to which a user of a tasked selector is not a communicant. Such upstream-acquired Internet transactions must be destroyed upon recognition if it is determined that the transactions contain U.S. person information but do not contain any information that meets the NSA’s long-term retention standards (discussed further below). MCTs must also be destroyed upon recognition if it is determined that a single, discrete communication within the MCT is a wholly domestic communication.

The NSA’s minimization procedures also contain the following provision:

Personnel will exercise reasonable judgment in determining whether information acquired must be minimized and will destroy inadvertently

---

260 See, e.g., PCLOB March 2014 Hearing Transcript, supra, at 72.
263 AUGUST 2013 SEMIANNUAL ASSESSMENT, supra, at A-12 (noting that all of the agency minimization procedures require purges when a target is discovered to be a U.S. person or person located in the United States, with limited exceptions).
264 NSA October 2011 Minimization Procedures, supra, § 3(c)(2).
265 NSA October 2011 Minimization Procedures, supra, § 3(b)(5)(a)(1)(a) (requiring destruction of segregated MCTs determined to contain a wholly domestic communication) and § 3(b)(5)(b)(1) (requiring a determination regarding whether a single communication within an MCT is a wholly domestic communication before it is used); Bates November 2011 Opinion, supra, at 9, 2011 WL 10947772, at *4 (incorporating government’s representation in a filing that if the discrete communication within an MCT is determined to be a wholly domestic communication, it must be destroyed).
acquired communications of or concerning a United States person at the earliest practicable point in the processing cycle at which such communication can be identified either: as clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or, as not containing evidence of a crime which may be disseminated under these procedures.\textsuperscript{266}

While it is not entirely clear what constitutes an “inadvertently acquired communication” here, the NSA's general counsel has stated that “[i]f information is determined to not have foreign intelligence value then it is required to be purged.”\textsuperscript{267} The NSA's general counsel, however, clarified that it is often “difficult to determine the foreign intelligence value of any particular piece of information.”\textsuperscript{268} An NSA analyst would need to determine not only that a communication is not currently of foreign intelligence value to him or her, but also would not be of foreign intelligence value to any other present or future foreign intelligence need. Thus, in practice, this requirement rarely results in actual purging of data.

Neither the CIA nor FBI's minimization procedures have comparable requirements that a communication containing U.S. person information be purged upon recognition that the communication contains no foreign intelligence information; instead the CIA and FBI rely solely upon the overall age-off requirements found in their minimization procedures.

Section 702–acquired data that is not subject to purge upon recognition may be retained effectively indefinitely (i.e., need not be aged off of agency systems) if an agency determines that the data meets the retention standard in its minimization procedures. A communication is sometimes described as having been “minimized” or “retained” if the communication has been determined to meet this retention standard.

The NSA’s minimization procedures permit the NSA to retain communications (other than wholly domestic communications) in generally the same situations where the NSA is permitted to disseminate (i.e., disclose) these communications to the consumers of the NSA’s intelligence reports.\textsuperscript{269} Specifically, the NSA may retain communications where the information identifiable to a U.S. person is, for example, “necessary to understand the foreign intelligence information or assess its importance,” indicates that U.S. person “may be the target of intelligence activities” by a foreign government, or “the communication indicates that the United States person may be engaging international terrorist...
activities.” The NSA may also retain a communication containing U.S. person information if the communication is reasonably believed to contain evidence of a crime and the NSA has or will disseminate that evidence to a federal law enforcement entity. The NSA may also retain communications beyond the normal age-off period if it is still decrypting the communication or using the communication to decrypt other communications.

The NSA minimization procedures do not separately place any limitations on the retention of communications that contain no U.S. person information, but they do contain a reminder that any such communications may be retained only in accordance with other laws, regulations, and policy (for example, the general definitions and restrictions regarding the NSA’s authorities provided in Executive Order 12333 and related documents).

The retention standard in the CIA’s Section 702 minimization procedures is comparable to the standard found in the NSA’s minimization procedures. The CIA may indefinitely retain “minimized” communications. In order to “minimize” the communication, the CIA must remove any U.S. person information from the communication unless the information is publicly available, the U.S. person has consented to retention of the information, or the CIA must determine that the U.S. person information is necessary or may reasonably become necessary to understand foreign intelligence information. The CIA minimization procedures contain various categories of information considered to either be foreign intelligence information or information that is necessary to understand foreign intelligence information. Once “minimized,” the communications may be retained in repositories that are still restricted to CIA personnel, but not necessarily CIA personnel who have been trained in the CIA minimization procedures. The CIA minimization procedures also permit the retention of data that is retained because it has been reported to a federal law enforcement agency as evidence of a crime.

The FBI Section 702 minimization procedures permit acquired communications to be retained indefinitely if the communications either contain no U.S. person information or if the communications contain information that “reasonably appears to be foreign intelligence information, [is] necessary to understand foreign intelligence information or assess its importance, or [is] evidence of a crime.” Before further using this communication, the FBI is required to “mask” any U.S. person information within the communication that does not satisfy one of these three criteria. The FBI is also separately required to retain

---

270 NSA October 2011 Minimization Procedures, supra, § 6(a)(2), (b).
271 NSA October 2011 Minimization Procedures, supra, § 6(a)(3), (b)(8).
272 NSA October 2011 Minimization Procedures, supra, § 6(a)(1).
reviewed information that reasonably appears to be exculpatory or that reasonably appears to be discoverable in a criminal proceeding.

E. Use and Dissemination

Restrictions in FISA and the minimization procedures contain limitations on the use and dissemination of Section 702–acquired information. “Dissemination” of FISA-acquired information generally refers to the reporting of acquired information outside of an intelligence agency, though broad accessibility of information within an agency can also constitute dissemination.274

Section 702 acquisition is governed by almost all of the same restrictions on use that apply to traditional FISA electronic surveillance.275 These statutory restrictions apply to both U.S. person information and non-U.S. person information. Specifically, all Section 702 information may be used or disclosed only for lawful purposes.276 Use of Section 702–acquired information in a criminal proceeding must be authorized by the Attorney General.277 Any person whose communications have been acquired pursuant to Section 702, whether or not he or she was a target of the acquisition and whether or not he or she is a U.S. person, must be notified by the government before any information obtained from or derived from Section 702 acquisition is used against him or her in any legal proceeding in the United States.278 Such an individual is referred to as an “aggrieved person.” An aggrieved person may move to suppress the evidence that was obtained from or derived from Section 702 acquisition on the grounds that the information was unlawfully acquired or that the Section 702 acquisition otherwise did not conform with the Attorney General and Director of National Intelligence’s authorization.279

The agencies’ minimization procedures and practices impose additional restrictions on the use and dissemination of Section 702–acquired data. The NSA’s minimization procedures permit the NSA to disseminate U.S. person information if the NSA deletes any information that could identify the U.S. person (a process referred to as “masking”).280 Alternatively, the NSA may disseminate the U.S. person’s identity for one of a specific list of reasons, including that the U.S. person has consented to the dissemination, the specific

274 See H.R. Rep. No. 95-1283, at 59 (discussing minimization within agencies).
275 50 U.S.C. § 1881e(a) (stating that information acquired under Section 702 shall be governed under virtually all of the use restrictions found in 50 U.S.C. § 1806).
278 50 U.S.C. § 1806(c), (d).
279 50 U.S.C. § 1806(e).
280 NSA October 2011 Minimization Procedures, supra, § 6 (b).
information about the U.S. person is already publicly available, the U.S. person’s identity is necessary to understand foreign intelligence information, or the communication contains evidence of a crime and is being disseminated to law enforcement authorities. As a matter of practice and policy, the NSA typically masks all information that could identify a U.S. person in its reports.\textsuperscript{281} Consumers of NSA reports, such as other federal agencies, may then request that the U.S. person identity be “unmasked,” a request that the NSA approves if the user has a “need to know” and disseminating the U.S. person identity would be consistent with the NSA’s minimization procedures.\textsuperscript{282}

Generally, dissemination of communications that contain no U.S. person information are governed by other laws, regulation, and policies (such as Executive Order 12333 and related implementing regulations), but not by the minimization procedures.\textsuperscript{283} These further restrictions outside the minimization procedures, for example, require that the NSA generate intelligence reports only to meet specific intelligence requirements established by the government.\textsuperscript{284} These regulations and policies also contain restrictions regarding what information (U.S. person information or otherwise) may be shared with foreign governments.\textsuperscript{285}

In response to Judge Bates’ opinion finding that a previous version of the NSA’s minimization procedures did not meet Fourth Amendment or statutory requirements, the NSA’s minimization procedures now also impose additional restrictions on the use of MCTs. Specifically, before a discrete communication contained within an MCT can be used in an intelligence report, FISA application, or to engage in further Section 702 targeting, the NSA analyst must determine if the discrete communication contains a tasked selector.\textsuperscript{286} If not, and the communication is to or from an identifiable U.S. person or person located in the United States, that discrete communication may only be used to protect against an immediate threat to life, such as a hostage situation.\textsuperscript{287}

The CIA’s minimization procedures permit the CIA to disseminate U.S. person information if any information that identifies the U.S. person is masked in the dissemination. The CIA may also disseminate U.S. person information in a manner that identifies the U.S. person if that person’s identity is necessary to understand foreign information.

\begin{itemize}
  \item \textsuperscript{281} NSA DCLPO REPORT, supra, at 7.
  \item \textsuperscript{282} NSA DCLPO REPORT, supra, at 7-8; NSA October 2011 Minimization Procedures, supra, §§ 6(b) and 7.
  \item \textsuperscript{283} NSA October 2011 Minimization Procedures, supra, § 7.
  \item \textsuperscript{284} See generally Exec. Order No. 12333 §§ 1.3(b)(4) and 1.6(f).
  \item \textsuperscript{285} NSA October 2011 Minimization Procedures, supra, § 3(b)(5)(b)(2).
  \item \textsuperscript{286} NSA October 2011 Minimization Procedures, supra, § 3(b)(5)(b)(2)(c).
\end{itemize}
intelligence information or (if concerning an attack by a foreign power, sabotage by a foreign power, international terrorism or the international proliferation of weapon of mass destruction by a foreign power, or clandestine intelligence activities by a foreign power) may become necessary to understand the foreign intelligence information. The CIA may further disseminate evidence of a crime to federal law enforcement authorities.

The FBI's minimization procedures permit the FBI to disseminate Section 702–acquired U.S. person information that reasonably appears to be foreign intelligence information or is necessary to understand foreign intelligence information. Disseminations concerning the national defense or security of the United States or the conduct of foreign affairs of the United States are permitted to identify U.S. persons only if necessary to understand the foreign intelligence information or to assess its importance. The FBI is also permitted to disseminate U.S. person information that reasonably appears to be evidence of a crime to law enforcement authorities. The FBI's minimization procedures incorporate certain guidelines, already otherwise applicable to the FBI, regarding the dissemination of information to foreign governments.288

VII. Internal Agency Oversight and Management of the Section 702 Program

In addition to the training programs previously described, each of the agencies subject to targeting or minimization procedures has developed a corresponding compliance program to evaluate and oversee compliance with these procedures, as well as facilitate the reviews by external overseers.289 Any incidents of noncompliance that have been identified either by these compliance programs or that are otherwise discovered by the agencies must be reported to the DOJ and ODNI, who in turn must report these incidents to Congress and the FISC,290 as discussed in the next section.

The NSA's use of the Section 702 authorities are internally overseen by various NSA entities, including the NSA's Office of the Director of Compliance (“ODOC”), NSA's Office of General Counsel (“OGC”), embedded compliance elements within NSA’s directorates (in

288 NSA October 2011 Minimization Procedures, supra, § 3(b)(5)(b)(2)(c).
289 See AUGUST 2013 SEMIANNUAL ASSESSMENT, supra, at A-6 to A-8 (discussing NSA oversight program); id. at A-9 (discussing CIA oversight program); id. at A-11 to A-12 (discussing FBI oversight program). See generally id. at 4-5 n.2 (noting that no incidents of noncompliance have been reported by the NCTC and that the NSA and ODNI would be conducting a review of the NCTC’s compliance in the following reporting period).
290 AUGUST 2013 SEMIANNUAL ASSESSMENT, supra, at 28 (noting that the semiannual report required by Section 707 is given to both Congress and the FISC and describes all incidents of noncompliance); 50 U.S.C. § 1881f(b)(1)(G) (requiring all incidents of noncompliance with the targeting procedures, minimization procedures, and Attorney General Guidelines, as well as any incidents of noncompliance by a provider, to be reported in the Section 707 Report); FISC Rule of Procedure 13(b) (requiring incidents of noncompliance to be reported to the FISC).
particular, the Signals Intelligence Directorate’s Oversight and Compliance (“O&C”) section), and — as of early 2014 — the NSA’s new Director of Civil Liberties and Privacy Office (“DCLPO”). Each of these organizations has different, but related, roles. The NSA’s ODOC is responsible for NSA-wide compliance efforts and conducts periodic risk assessments to identify potential systemic incidents of noncompliance with the NSA targeting or minimization procedures. For example, the ODOC conducted a risk assessment regarding how effective the NSA’s purge practices had been in removing data required to be purged from the NSA’s systems. Particularly important in light of errors and misunderstandings that have led to compliance issues in Section 702 and other programs, such as the MCT issue discussed above, ODOC also coordinates programs intended to ensure that factual representations made to the FISC are accurate and that interpretations of how the targeting and minimization procedures are to be applied in practice are consistent both within the NSA and between the NSA and its overseers.

The NSA’s O&C section and OGC conduct more granular oversight of the Section 702 program. The O&C section conducts spot checks of individual targeting decisions, queries of acquired data, and disseminations for compliance with the NSA’s targeting and minimization procedures. The O&C section and OGC also offer compliance-related guidance regarding targeting decisions, investigate and report potential incidents of noncompliance with the procedures and other legal requirements, and provide remedial training when an incident investigation reveals that the incident was caused by an avoidable error. The O&C section and OGC also facilitate the reviews conducted by the DOJ and ODNI that are described below.

The NSA appointed its first Director of Civil Liberties and Privacy while the Board was conducting its review of the Section 702 program. The Director’s office is not, as of yet, involved in periodic Section 702 programmatic reviews. The Director’s first public report, however, was issued in April 2014 and described in an unclassified manner aspects of the NSA’s implementation of the Section 702 program.

The CIA’s internal compliance program is managed by the CIA’s FISA Program Office and the CIA’s OGC. These entities conduct oversight of the CIA’s day-to-day use of the Section 702 authorities by, for example, conducting pre-tasking reviews of the CIA

292 August 2013 Semiannual Assessment, supra, at A-7 to A-8.
295 See generally NSA DCLPO Report, supra, at 9.
296 August 2013 Semiannual Assessment, supra, at 7.
nominations to the NSA regarding proposed new selectors to be tasked for Section 702 acquisition. The FISA Program Office also oversees whether current and proposed systems handle Section 702–acquired data in compliance with the minimization procedures. The FISA Program Office additionally conducts reviews regarding whether Section 702 selectors remain properly tasked. The CIA’s OGC has attorneys embedded with CIA personnel to answer specific targeting, querying, retention, and dissemination questions. Finally, the CIA FISA program office and the CIA OGC facilitate the reviews conducted by the DOJ and ODNI that are described below.

Several sub-organizations within the FBI are responsible for conducting internal oversight over the Bureau’s Section 702 activities. The FBI’s OGC, in particular its National Security Law Branch, is responsible for providing legal advice regarding the application of the FBI targeting and minimization procedures. The FBI’s Exploitation Threat Section (“XTS”) takes the lead in reviewing the FBI’s nominations to the NSA for proposed Section 702 tasking. Various sub-organizations within the Bureau are responsible for reviewing and monitoring compliance with the FBI targeting and minimization procedures.

As described above, the NCTC’s role in the Section 702 program is minimal. The NCTC has assigned legal and program personnel to oversee the implementation of its minimization procedures.

Incidents of noncompliance with the targeting or minimization procedures that are identified by any of these internal compliance efforts, or that are otherwise self-identified by the agencies, must be reported to the DOJ and ODNI. Historically, most identified compliance incidents have been discovered as a result of self-reporting or via the internal compliance programs. Once an incident has been identified and reported, the internal

---

302 August 2013 Semiannual Assessment, supra, at A-12.
303 August 2013 Semiannual Assessment, supra, at 7 (regarding the NSA’s reporting of incidents), 10 (regarding reporting of incidents by the FBI Office of General Counsel), A-7 (regarding the NSA’s reporting via the NSA Office of General Counsel), and A-9 (regarding reporting of incidents by the CIA Office of General Counsel).
304 See August 2013 Semiannual Assessment, supra, at 7 (stating that most incidents “are identified by NSA analysts or by NSA’s internal compliance program”); id. at 25 (noting that most compliance incidents involve the NSA targeting or minimization procedures); id. at 28 (advising that the “volume” of NSA incidents is robust enough such that pattern and trend analysis is more fruitful than is the case with other compliance matters).
compliance programs are also involved in implementing remedial actions, such as purging and retraining as required.\textsuperscript{305}

In addition to reporting incidents of noncompliance, as an additional prophylactic measure the NSA is required under its targeting procedures to report any instance in which a user of a Section 702–tasked selector is determined to have been in the United States while the selector was tasking.\textsuperscript{306} Should the CIA or FBI determine that a user of a Section 702 selector is a U.S. person or located in the United States, the CIA and FBI report this to the NSA, which in addition to promptly detasking the selector, sends a report to the DOJ and ODNI. This reporting requirement applies whether or not the NSA assesses that this acquisition occurred as the result of a compliance incident. For example, if the NSA correctly assessed that a target was a non-U.S. person located abroad, but unbeknownst to the NSA (and not reasonably predictable based on information available to the NSA), the target subsequently entered the United States, no compliance incident would have occurred. The NSA would be required to promptly detask the target’s selectors from Section 702 acquisition upon recognition and purge data acquired while the user was in the United States, but no incident of noncompliance with the targeting or minimization procedures would have occurred. This is because the NSA assessed that the target was a non-U.S. person reasonably believed to be located outside the United States up until the time that the NSA detasked the selector from Section 702 acquisition. Nonetheless, the NSA would be required to report such an incident to the DOJ and ODNI. As described below, the DOJ and ODNI investigate such incidents and will request additional information in order to make their own determination regarding whether a compliance incident did or did not occur.\textsuperscript{307}

Additionally, but separately, the statute also requires each agency that conducts Section 702 acquisition to conduct an annual review of the Section 702 program.\textsuperscript{308} These annual reviews must be sent to the Senate Select Committee on Intelligence, Senate Committee on the Judiciary, House Permanent Select Committee on Intelligence, and House Judiciary Committee (hereinafter, “the Congressional Committees”), the FISC, Attorney General, and Director of National Intelligence.\textsuperscript{309} The annual reviews must report the number of disseminations of U.S. person identities made, the number of U.S. person identities that were subsequently unmasked, and the number of Section 702 targets that

\begin{itemize}
  \item \textsuperscript{305} See, e.g., NSA DCLPO REPORT, supra, at 9 (regarding various remedies implemented by NSA after an incident is discovered); AUGUST 2013 SEMIANNUAL ASSESSMENT, supra, at A-13 (describing elements of the purge process).
  \item \textsuperscript{306} AUGUST 2013 SEMIANNUAL ASSESSMENT, supra, at 7.
  \item \textsuperscript{307} AUGUST 2013 SEMIANNUAL ASSESSMENT, supra, at 7.
  \item \textsuperscript{308} 50 U.S.C. § 1881a(l)(3).
  \item \textsuperscript{309} 50 U.S.C. § 1881a(l)(3).
\end{itemize}
were subsequently determined to be located in the United States.\textsuperscript{310} The agency reviews must also evaluate whether foreign intelligence information is being acquired under the Section 702 program and whether the minimization procedures adequately minimize the acquisition, retention, and dissemination of U.S. person information consistent with the United States’ foreign intelligence needs.\textsuperscript{311} The CIA receives Section 702 acquisition but does not actually conduct any acquisition. As such, the CIA does not conduct an annual review; some information regarding the CIA’s use of the program, however, is included in the NSA’s annual report.

\section*{VIII. External Oversight of the Section 702 Program}

In enacting Section 702, Congress mandated additional external layers of oversight, each resulting in reports made to Congress and the FISC. This Section describes the targeting and minimization reviews conducted by the DOJ’s National Security Division (“NSD”) and the ODNI, the reports issued by the inspectors general, and additional oversight activities conducted by the FISC and the Congressional Committees.

\subsection*{A. NSD/ODNI Targeting Reviews}

As is discussed above, the NSA is required under its targeting procedures to document every targeting decision made under its targeting procedures. The record of each targeting decision, known as a tasking sheet, includes (1) the specific selector to be tasked,\textsuperscript{312} (2) citations to the specific documents and communications that led the NSA to determine that the target is reasonably believed to be located outside the United States,\textsuperscript{313} (3) a narrative describing the contents of these specific documents and communications, (4) a statement regarding the assessed U.S. person status of the target, and (5) a statement identifying the foreign power or foreign territory regarding which the foreign intelligence information is to be acquired.\textsuperscript{314}

The NSD conducts a post-tasking review of every tasking sheet provided by the NSA;\textsuperscript{315} the ODNI reviews a sample of these sheets. In addition to evaluating whether the tasking complied with the targeting procedures, the NSD and ODNI review the targeting for

\begin{itemize}
\item\textsuperscript{310} 50 U.S.C. § 1881a(1)(3)(A)(i)–(iii).
\item\textsuperscript{311} 50 U.S.C. § 1881a(1)(3)(A), (B).
\item\textsuperscript{312} \textit{AUGUST 2013 SEMIANNUAL ASSESSMENT}, supra, at 7.
\item\textsuperscript{313} \textit{AUGUST 2013 SEMIANNUAL ASSESSMENT}, supra, at A-5; see also NSA DCLPO REPORT, supra, at 4-5.
\item\textsuperscript{314} \textit{AUGUST 2013 SEMIANNUAL ASSESSMENT}, supra, at A-5.
\item\textsuperscript{315} See PCLOB March 2014 Hearing Transcript, supra, at 61 (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ) (stating that tasking sheets “are all reviewed . . . by the Department of Justice on a regular basis”).
\end{itemize}
overall compliance with the statutory limitations, such as the prohibition against reverse targeting. If the NSD or ODNI is unable to determine whether the tasking sheet is sufficient, the NSD and ODNI will require the NSA to provide the cited documents and communications that underlie the NSA’s foreignness determination at a bimonthly onsite review.316 The NSD and ODNI also engage with the NSA compliance and legal personnel to ask follow-up questions regarding the foreignness and foreign intelligence purpose determinations.317 As needed, the NSD and ODNI also seek additional information from the CIA and FBI regarding selectors that they have nominated.318 The NSD and ODNI’s review of foreign intelligence purpose determinations is more limited than its review of foreignness determinations insofar as the NSA analysts are required to document the basis for their foreignness determination (i.e., they must show their work), whereas the analyst need only identify a foreign intelligence purpose. The results of each NSD/ODNI bimonthly review are required by statute to be provided to the Congressional Committees.319 Historically, the NSD and ODNI’s bimonthly reviews have determined that approximately 0.1% of all the NSA taskings did not meet the requirements of the NSA targeting procedures.320

Additionally but separately, the NSD and ODNI also conduct approximately monthly reviews of the FBI’s application of its own targeting procedures.321 The NSD currently reviews every instance in which the FBI’s evaluation of foreignness revealed any information regarding the target, regardless of whether the information confirms or rebuts the NSA’s foreignness determination. Follow-up questions regarding the FBI’s evaluation of this information are discussed with FBI analysts and supervisory personnel.322 Like the NSA reviews, the results of the NSD/ODNI monthly reviews regarding FBI targeting are documented in a report that must be sent to the Congressional Committees.323 The NSD and ODNI have not reported the historical percentage of tasking incidents that have been discovered as a result of these reviews. For the period of June through November 2012, the

316 AUGUST 2013 SEMIANNUAL ASSESSMENT, supra, at 7.
317 AUGUST 2013 SEMIANNUAL ASSESSMENT, supra, at 7.
318 See, e.g., AUGUST 2013 SEMIANNUAL ASSESSMENT, supra, at 8 (noting that with respect to CIA nominations “the joint oversight review team conducts onsite visits at CIA” and “the results of these visits are included in the bimonthly NSA review reports discussed above”); see also AUGUST 2013 SEMIANNUAL ASSESSMENT, at 6-7 (describing these content of the bimonthly review reports, including the NSA tasking review).
320 PCLOB March 2014 Hearing Transcript, supra, at 43 (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ).
321 AUGUST 2013 SEMIANNUAL ASSESSMENT, supra, at 9-10.
322 AUGUST 2013 SEMIANNUAL ASSESSMENT, supra, at 10.
overall FBI tasking incident error rate, which would include incidents discovered by the NSD/ODNI reviews, was 0.04%.

B. NSD/ODNI Minimization Reviews

The NSD and ODNI also conduct at least bimonthly reviews of the NSA, CIA, and FBI’s application of their respective minimization procedures. These reviews vary based on the differences in each agency’s minimization procedures and the manner in which each agency uses the Section 702–acquired data. In addition to reviewing agency activities for compliance with the minimization procedures, the NSD and ODNI also look for any other potential violations of statutory prohibitions, such as the prohibition against reverse targeting. For example, if a Section 702 tasking resulted in substantial reporting by the Intelligence Community regarding a U.S. person, but little about the Section 702 target, this would be a strong indication to the oversight team that reverse targeting may have occurred. The results of the NSD/ODNI reviews are documented in reports that are, as required by FISA, sent to the Congressional Committees.

The NSD and ODNI bimonthly minimization reviews at the NSA focus on dissemination and queries using U.S. person identifiers. With respect to dissemination, the NSA identifies to the NSD/ODNI review team all NSA-issued reports that contain U.S. person information derived from Section 702 acquisition. The NSD/ODNI team has reviewed a substantial majority of these reports. The NSD/ODNI team also reviews other disseminations of foreign intelligence information to foreign governments, which may or may not contain U.S. person information. With respect to queries of Section 702–acquired metadata using U.S. person identifiers, the NSD/ODNI team reviews all such queries and analysts’ justifications for the queries. With respect to Section 702–acquired content queries, the NSD/ODNI review team reviews the documentation for all U.S. person identifiers that are approved as query terms.

---

324 August 2013 Semiannual Assessment, supra, at 5-10 (regarding frequency of reviews and fact that they include minimization reviews).
325 August 2013 Semiannual Assessment, supra, at 5-6.
327 August 2013 Semiannual Assessment, supra, at 7, 13.
328 August 2013 Semiannual Assessment, supra, at 7.
329 The NSD/ODNI previously reviewed a substantial majority of these reports. See NSA DCLPO Report, supra, at 8. NSD has advised that it has recently revised its reviews and is now reviewing all reports provided by NSA that contain U.S. person information.
330 August 2013 Semiannual Assessment, supra, at 7.
331 See NSA October 2011 Minimization Procedures, supra, § 3(b)(6) (regarding documentation requirements for such query terms); NSA DCLPO Report, supra, at 7 (regarding fact that this documentation is made available to NSD and ODNI for review).
At the CIA, the NSD/ODNI team reviews the CIA’s querying, retention, and dissemination of Section 702–acquired data. The NSD/ODNI team evaluates all of the required written justifications for use of a U.S. person identifier (or any other query term intended to return information about a particular U.S. person) to query Section 702–acquired content. Metadata queries are not reviewed. The NSD/ODNI review team samples decisions made by CIA personnel to permanently retain data. The CIA is required to provide, and the NSD/ODNI team reviews, all disseminations of Section 702–acquired U.S. person information.

With respect to the FBI, the NSD/ODNI team also evaluates the FBI’s querying, retention, and dissemination determinations. The NSD and ODNI review a sample of communications that FBI assesses meets the retention standards, a sample of disseminations containing Section 702–derived U.S. person information, and a sample of queries conducted by FBI personnel.

The NSD and ODNI also conduct annual process reviews at the NCTC and FBI. The NCTC process review examines the processes that the NCTC has put in place to control access and train personnel with regard to its limited Section 702 minimization procedures. The FBI annual process review surveys the systems FBI uses to receive, verify, and route PRISM collection.

The NSD and ODNI also conduct ad hoc reviews related to newly developed or modified systems that the agencies plan to use to target non-U.S. persons under Section 702 or acquire, retain, or disseminate Section 702–acquired information. These ad hoc system reviews are intended to identify existing compliance issues, prevent future compliance incidents from occurring, and ensure that systems are designed in a manner that facilitates subsequent oversight of their use.

C. NSD/ODNI Incident Investigation, Reporting, and Related Activities

Whether initially discovered via an NSD/ODNI review, an internal agency compliance review, or by self-reporting, Section 702 and the FISC’s own rules of procedure require the NSD to report compliance incidents by the Intelligence Community or electronic communication service providers to the Congressional Committees and to the

332 August 2013 Semiannual Assessment, supra, at 8.
333 August 2013 Semiannual Assessment, supra, at 8.
334 August 2013 Semiannual Assessment, supra, at 8.
335 August 2013 Semiannual Assessment, supra, at 8.
336 August 2013 Semiannual Assessment, supra, at 10 & n.6.
337 August 2013 Semiannual Assessment, supra, at 11.
FISC. Specifically, the FISA Amendments Act requires the Attorney General to report every incident of noncompliance to the Congressional Committees in a semiannual report. Pursuant to FISC Rule of Procedure 13(b), all compliance incidents must be reported to the FISC in either an immediate notice or (for less significant incidents) in a quarterly report. Rule 13(b) states that such reports must include a description of the incident of noncompliance, the facts and circumstances related to the incident, any modifications that will be made in how the government is using the authority in light of the incident, and a description of how the government will handle any information obtained as a result of the incident. In addition, but separately, the Attorney General and Director of National Intelligence must semiannually jointly conduct an assessment regarding the agencies’ compliance with their targeting procedures, minimization procedures, and the Attorney General Guidelines. This semiannual assessment must be provided to the Congressional Committees and to the FISC. To date, four of the semiannual assessments have been partially declassified and are publicly available.

To meet these various reporting obligations, a team of NSD and ODNI personnel review incident reports, request additional information, and (when necessary) further investigate potential incidents of noncompliance. These inquiries and investigations entail frequent interaction with counterparts in the internal agency compliance programs discussed above. In addition to resolving individual compliance matters, the NSD and ODNI team lead weekly calls and bimonthly meetings with representatives from the NSA, CIA, and FBI to discuss, among other things, compliance trends and incidents that affect multiple agencies.

340 See May 2010 Semiannual Assessment, supra at 22 (discussing requirements under Rule 10(c), the predecessor to Rule 13(b) in the prior set of FISC Rules of Procedure); NSA DCLPO Report, supra, at 3 (discussing individual notices and quarterly reports).
341 FISC Rule of Procedure 13(b).
345 May 2010 Semiannual Assessment, supra, at 22.
346 See generally August 2013 Semiannual Report, supra, at 11 (discussing bimonthly meetings).
Some of the results of the NSD and ODNI’s compliance investigations and reports are discussed below.

D. Inspector General Reports

Section 702 also authorizes inspectors general of agencies that acquire data pursuant to Section 702 to conduct reviews of the Section 702 program.\textsuperscript{347} The inspectors general are authorized to evaluate the agencies compliance with the targeting procedures, minimization procedures, and Attorney General Guidelines.\textsuperscript{348} Any such reviews are required to contain an accounting of the number of disseminated reports containing U.S. person identities, the number of instances those identities were unmasked, and the number of targets that were subsequently determined to be located in the United States.\textsuperscript{349} The results of these reviews must be provided to the Attorney General, Director of National Intelligence, FISC, and the Congressional Committees.\textsuperscript{350} The NSA and DOJ\textsuperscript{351} Inspectors General have conducted reviews under this provision. The reports of these reviews have not been declassified.

E. FISC Oversight

The FISC’s primary role in Section 702 is to review the Section 702 certifications and corresponding targeting and minimization procedures for compliance with the statute and the Fourth Amendment. As is described in detail above, the FISC has held that this review of the Section 702 certifications and related documents cannot be made in a vacuum, but instead must be made in light of the actual manner in which the government has implemented (or plans to implement) the Section 702 authorities. In addition to filings made by the government to the FISC in support of the certifications, the FISC’s determinations are informed by the information provided in the NSD’s reports of all incidents of noncompliance with the procedures,\textsuperscript{352} the Attorney General and Director of National Intelligence’s semiannual assessment regarding compliance with the procedures,\textsuperscript{353} the annual reports of agency heads that conduct Section 702 acquisition,\textsuperscript{354}

\textsuperscript{347} 50 U.S.C. § 1881a(l)(2).
\textsuperscript{349} 50 U.S.C. § 1881a(l)(2)(B), (C).
\textsuperscript{350} 50 U.S.C. § 1881a(l)(2)(D).
\textsuperscript{352} FISC Rule of Procedure 13(b).
\textsuperscript{353} 50 U.S.C. § 1881a(l)(1).
\textsuperscript{354} 50 U.S.C. § 1881a(l)(3).
and any reports by the inspectors general.\footnote{50 U.S.C. § 1881a(l)(2).} In reviewing the certifications, the FISC also will order the government to respond in writing to questions regarding the conduct of the Section 702 collection program and holds hearings in order to take sworn testimony from government witnesses.\footnote{FISC Rules of Procedure 5(c) and 17; Bates October 2011 Opinion, supra, at 7-10, 2011 WL 10945618 at *2-4 (examples of filings and hearing described); Letter from Presiding Judge Reggie B. Walton, Foreign Intelligence Surveillance Court to Senator Patrick Leahy, Chairman, Senate Comm. on the Judiciary, at 4-6 (July 29, 2013) (“Judge Walton Letter”) (describing government submissions related to Section 702 certifications and the types of additional information sought from the government by the FISA court), available at http://www.fisc.uscourts.gov/sites/default/files/Correspondence%20Leahy-1.pdf.}

The FISC’s oversight role is not limited to the renewal of Section 702 certifications. The government’s obligation to report incidents of noncompliance under the FISC’s rules is independent of whether any Section 702 certification is currently pending before the court.\footnote{FISC Rule of Procedure 13(b).} In a letter to Senate Judiciary Committee Chairman Patrick Leahy, former FISC Presiding Judge Reggie Walton stated that with respect to all FISA compliance matters, to include incidents of noncompliance with the Section 702 program, the court may seek additional information, issue orders to the government to take specific action to address an incident of noncompliance, or (if deemed necessary) issues orders to the government to cease an action that the court assesses to be non-compliant.\footnote{Judge Walton Letter, supra, at 10-11.}

F. Congressional Oversight

The Senate Select Committee on Intelligence, Senate Committee on the Judiciary, House Permanent Select Committee on Intelligence, and House Judiciary Committee are the committees that oversee the government’s use of FISA information, including Section 702 information. In passing the FISA Amendments Act, Congress mandated that the Attorney General provide these four committees with a semiannual report describing several aspects of the Section 702 program and further provide the committees with the underlying documents that govern the program.\footnote{50 U.S.C. § 1881f.} Among other things, this semiannual report must include copies of the reports from any compliance reviews conducted by the DOJ or ODNI, a description of any and all incidents of noncompliance by the Intelligence Community or an electronic communications service provider, any certifications (including targeting and minimization procedures), and the directives sent to the electronic communication service providers.\footnote{50 U.S.C. § 1881f(b)(1).} The semiannual report must also include a description of the FISC’s review of the certifications and copies of any order by the FISC or
pleading by the government that contains a significant legal interpretation of Section 702.\textsuperscript{361}

In practice, the government provides the four committees all government filings, hearing transcripts, and FISC orders and opinions related to the court’s consideration of the Section 702 certifications. In addition, the Congressional Committees receive the classified Attorney General and Director of National Intelligence’s semiannual assessment regarding compliance with the procedures,\textsuperscript{362} the annual reports of agency heads that conduct Section 702 acquisition,\textsuperscript{363} and any reports by the inspectors general.\textsuperscript{364}

In addition to these statutory requirements, the agencies may separately (and more promptly) inform the Congressional Committees of substantial compliance incidents.\textsuperscript{365} The committees also hold hearings, and committee members and staff receive briefings, regarding the implementation of the Section 702 program.\textsuperscript{366}

\textbf{IX. Compliance Issues}

The Section 702 program is a technically complex collection program with detailed rules embodied in the targeting procedures, minimization procedures, and Attorney General Guidelines regarding targeting, acquisition, querying, retention, and dissemination. Incidents of noncompliance with these rules have been identified in the course of the oversight conducted by the agencies themselves, by the NSD, and by the ODNI. These internal and external compliance programs have not to date identified any intentional attempts to circumvent or violate the procedures or the statutory requirements,\textsuperscript{367} but both unintentional incidents of noncompliance and instances where Intelligence Community personnel did not fully understand the requirements of the statute and the procedures have been identified.

The government calculates a compliance incident rate for the Section 702 program by dividing the number of identified compliance incidents by the average number of selectors on task. This incident rate has been substantially below one percent since the

\textsuperscript{361} 50 U.S.C. § 1881f(b)(1)(D). Copies of documents related to significant legal interpretations are also produced to Congress pursuant to 50 U.S.C. § 1871.

\textsuperscript{362} 50 U.S.C. § 1881a(l)(1).

\textsuperscript{363} 50 U.S.C. § 1881a(l)(3).

\textsuperscript{364} 50 U.S.C. § 1881a(l)(2).

\textsuperscript{365} See, e.g., NSA DCLPO REPORT, supra, at 3.


\textsuperscript{367} AUGUST 2013 SEMIANNUAL ASSESSMENT, supra, at 23.
Section 702 program was initiated. The most common type of compliance incident that has occurred has involved instances in which the NSA otherwise complied with the targeting and minimization procedures in tasking and detasking a selector, but failed to make a report to the NSD and ODNI in the time frame required by the NSA targeting procedures.368 Such notification delays made up over half of the reported incidents in the most recently declassified Attorney General/Director of National Intelligence semiannual assessment.369 Two other common reasons compliance incidents occurred have been that (1) the wrong selector was tasked due to a typographical error,370 or (2) a delay in detasking resulted when an analyst detasked some, but not all, of the Section 702–tasked selectors used by a non-U.S. person target known to be traveling to the United States.371 Taken together, these three errors accounted for almost 75% of the compliance incidents that occurred during the reporting period of the most recently declassified Attorney General/Director of National Intelligence semiannual assessment.

Less common incidents, however, can have greater privacy implications. For example, the NSA has reported instances in which the NSA analysts conducted queries of Section 702–acquired data using U.S. person identifiers without receiving the proper approvals because the analyst either did not realize that the NSA knew the identifier to be used by a U.S. person or the analyst mistakenly queried Section 702–acquired data after receiving approvals to use a U.S. person identifier to query other non-Section 702–acquired data.372

In addition to such human errors, technical issues can lead to overcollection incidents. For example, the government has disclosed that technical errors have resulted in delays in detasking selectors found to be used by persons located in the United States.373 The government has also disclosed that both changes in how communications transit the telecommunications system and design flaws in the systems the government uses to acquire such communications can, and have, resulted in the acquisition of data beyond what was authorized by Section 702 program.374 Such unauthorized collection is required to be purged upon recognition.

370 August 2013 Semiannual Assessment, supra, at 33 n.21.
371 August 2013 Semiannual Assessment, supra, at 33.
373 August 2013 Semiannual Assessment, supra, at 32.
374 August 2013 Semiannual Assessment, supra, at 31-32 (stating that an undisclosed number of “incidents” involving overcollection as a result of changes in the global telecommunications environment, unforeseen consequences of software modifications, or system design issues occurred during the reporting period).
Several systemic incidents have also occurred in the government’s operation of the Section 702 program. As is described above, the government’s upstream acquisition of multi-communication transactions led to substantial modifications of the NSA minimization procedures and the purging of several years of prior collection. In an earlier incident, the NSA discovered that its practices for executing purges were substantially incomplete. Modifications to better tag, track, and purge data from the NSA’s systems when required were implemented.

More recently, questions raised by the NSD/ODNI oversight team led to the discovery that post-tasking checks used to identify indications that a target is located in the United States were incomplete or, for some selectors, non-existent for over a year. After this issue was discovered, the relevant systems were modified to correct several errors, efforts were made to identify travel to the United States that had been previously missed (and corresponding purges were conducted), and additional modifications to the agencies’ minimization procedures were made to ensure that data acquired while a Section 702 target had traveled to the United States will not be used.

Since the Section 702 program’s inception, the compliance programs have also identified two instances of reverse targeting. The first instance, which was discovered by the NSD/ODNI targeting review, involved the reverse targeting of a non-U.S. person located inside the United States in order to acquire foreign intelligence information. The second, which involved reverse targeting to acquire information about a U.S. person located outside the United States, was identified by NSA oversight personnel. The targeting in the first incident resulted in the acquisition of communications that were subsequently purged; the targeting in the second incident did not result in any communications being acquired. In both incidents, the analysts who engaged in the reverse targeting substantially misunderstood the prohibition against reverse targeting. Given the centrality of this prohibition to Section 702 targeting, these analysts were retrained not only on the reverse targeting prohibition, but on other fundamental targeting requirements.
Part 4: LEGAL ANALYSIS

I. Overview

Part Four is divided into three sections: Statutory Analysis, Constitutional Analysis, and Analysis of Treatment of Non-U.S. Persons. The Statutory Analysis section explains the statutory framework for collection under Section 702 of the Foreign Intelligence Surveillance Act ("FISA") and provides the Board's evaluation of whether PRISM and upstream collection comply with the statute. The Constitutional Analysis section details the Board's evaluation of the constitutionality of the program — examining the warrant requirement and its exceptions, and assessing the program’s reasonableness under the Fourth Amendment. Part Four concludes with a discussion of the treatment of non-U.S. persons under the program.

II. Statutory Analysis

A. Establishment of Section 702

As noted in the Board's Report on the Section 215 program, FISA was enacted in 1978 to establish a procedure under which the Attorney General could obtain a judicial order authorizing the use of electronic surveillance in the United States for foreign intelligence purposes. Its original provisions — now referred to as "traditional FISA" — authorized, among other things, individualized FISA orders for electronic surveillance relating to a specific person, place, or communications account or device.

Over time, Congress has enacted legislation bringing additional categories of foreign intelligence gathering within FISA’s ambit. One of the latest examples of this is the enactment of the FISA Amendments Act of 2008. 375 As outlined in Part 3 of this Report, the FISA Amendments Act, which includes the new Section 702 of FISA, replaced the temporary authority of the Protect America Act, which in turn, was designed to codify part of the President’s Surveillance Program. The statute was enacted in response to Congress’ conclusion that FISA should be amended to provide a separate procedure to facilitate the targeting of persons reasonably believed to be outside the United States to acquire foreign intelligence information. 376 This statute was developed during a time of public debate and

concern regarding the intelligence activities undertaken by the government, and it was an attempt to put a statutory framework around activities that were currently ongoing.\textsuperscript{377}

As discussed below, the government utilizes two collection methods under Section 702 — PRISM collection and upstream collection (which includes acquiring “about” communications). The manner in which collection is effectuated via PRISM and upstream varies; therefore, the Board has analyzed the statutory compliance of each collection method separately. After reviewing the operation of the Section 702 program as a whole, and each collection method implemented under Section 702 individually, the Board has concluded that PRISM collection is expressly authorized by the statute and that the statute, while silent on “about” upstream collection, can permissibly be interpreted as allowing such collection as currently implemented.

**B. Collection Under Section 702**

1. **Statutory Framework for Collection**

Congress created Section 702 to authorize Foreign Intelligence Surveillance Court (“FISC” or “FISA court”) approval of certifications which authorize the acquisition of broad categories of foreign intelligence information through the targeting of non-U.S. persons reasonably believed to be located outside the United States.\textsuperscript{378} A non-U.S. person is an individual who is neither a citizen nor a lawful permanent resident of the United States. As described in detail in Part 3 of this Report, the Attorney General and the Director of National Intelligence must submit a certification to and receive an order from the FISA court that permits them to authorize the targeting.\textsuperscript{379}

Under Section 702, the FISC has the authority to review the government’s certifications, targeting procedures, and minimization procedures, and the court must approve these certifications and procedures under criteria set forth in the statute. The FISC does not review specific selectors\textsuperscript{380} task for collection nor does it review the individual factual basis for expecting that the tasking of a particular selector will result in the acquisition of foreign intelligence information. In its review and approval process, however, the FISC has the authority to do more than a rote check to ensure that the government meets its statutory requirements. The FISC’s mandate to ensure compliance with the Fourth Amendment is expressly enumerated in the statute, and the court has required the government to make changes to its collection under Section 702 in the past on

\begin{itemize}
\item \textsuperscript{378} See 50 U.S.C. § 1881a(a), (g).
\item \textsuperscript{379} 50 U.S.C. § 1881a(a), (g), (i).
\item \textsuperscript{380} A selector is a unique identifier associated with a particular individual or entity. See pages 32-33 of this Report.
\end{itemize}
this basis. Additionally, the FISA court has an oversight role: the FISC Rules of Procedure impose an ongoing duty on the government to immediately correct any misstatement or omission of material facts that it has provided to the court, as well as to disclose any instance in which the government’s conduct did not comply with the FISC’s authorization or with applicable law.

On the whole, Section 702 provides the public with transparency into the legal framework for collection and publicly outlines the basic structure of the program. Use of the words “target” and “targeting” allowed Congress to signal the type of collection activity undertaken by the government without detailing operational methods and tactics. In addition, it is clear from the face of the statute that the government must submit certifications to the FISC as well as implement targeting and minimization procedures that have been approved by the court.

2. PRISM Collection

The Board concludes that as currently implemented, the operation of PRISM collection falls within the framework of the statute. Section 702 expressly authorizes the “targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.” As described in Part 3 above, under PRISM collection the government acquires communications to and from approved targets using communications “selectors” that are associated with particular persons. Examples of communications selectors include email addresses, but not key words. The collection of communications to and from a target inevitably returns communications in which non-targets are on the other end, some of whom will be U.S. persons. Such “incidental” collection of communications is not accidental, nor is it inadvertent.

The incidental collection of communications between a U.S. person and a non-U.S. person located outside the United States, as well as communications of non-U.S. persons outside the United States that may contain information about U.S. persons, was clearly


384 PCLOB March 2014 Hearing Transcript, supra, at 96-97 (statement of Robert Litt, General Counsel, ODNI).

385 PCLOB March 2014 Hearing Transcript, supra, at 96-97.
contemplated by Congress at the time of drafting. The statute prohibits the targeting of U.S. persons, but not the incidental acquisition of communications involving U.S. persons. Further, the statute requires the government to adopt procedures that, among other things, are reasonably designed to minimize (not eliminate) the acquisition and retention of private information about U.S. persons, consistent with the government’s foreign intelligence needs. The statute also calls for the Department of Justice and the Intelligence Community to review and report on disseminations of U.S. person information, including cases in which the U.S. person is not referred to by name. The Senate Select Committee on Intelligence has explained the inevitability of such incidental collection and how Congress responded to that inevitability:

Congress recognized at the time the FISA Amendments Act was enacted that it is simply not possible to collect intelligence on the communications of a party of interest without also collecting information about the people with whom, and about whom, that party communicates, including in some cases non-targeted U.S. persons...

Specifically, in order to protect the privacy and civil liberties of U.S. persons, Congress mandated that, for collection conducted under Section 702, the Attorney General adopt, and the FISA Court review and approve, procedures that minimize the acquisition, retention, and dissemination of nonpublicly available information concerning unconsenting U.S. persons.

Based on the information that the Board has reviewed, the government’s PRISM collection complies with the structural requirements of the statute. As outlined above, the government has filed certifications authorizing the acquisition of certain categories of targets with the FISA court and has developed and submitted for FISA court approval targeting and minimization procedures as required by the statute. Incidentally collected U.S. person information is subject to these minimization procedures that set standards for acquisition and retention of information and permit disseminations of U.S. person information only for a foreign intelligence purpose or when the information is evidence of a crime. After a thorough review, the Board has concluded that the government generally is complying with the targeting limitations set forth in subsections (b)(1) through (b)(4) and has adopted Attorney General guidelines that, among other things, prohibit reverse

---

386 See 50 U.S.C. §§ 1801(h), 1881a(e).
389 See 50 U.S.C. §§ 1801(h), 1881a(e).
targeting. Although there have been documented compliance incidents, we conclude that overall PRISM collection falls within the framework of the statute.

3. Upstream Collection

As described above, upstream collection constitutes a small percentage of collection under Section 702. To the extent that upstream collection involves acquiring communications to and from targeted persons, it fits within the statutory framework in the same way that PRISM collection does. Targeting under PRISM and upstream collection work in the same way; the mode of collection is different.

Upstream collection under Section 702 poses an additional question for statutory analysis because, as described above in Part 3, the upstream process captures not only communications to and from targeted persons, but also other communications that contain reference to the selector of a targeted person — which are referred to as “about” communications.

The statutory language of Section 702 does not expressly permit or prohibit collection of communications “about” a target. The fact that the government engages in such collection is not readily apparent from the face of the statute, nor was collection of information “about” a target addressed in the public debate preceding the enactment of FISA or the subsequent enactment of the FISA Amendments Act. Indeed, the words “target” and “targeting” are not defined in either the original version of FISA or the FISA Amendments Act despite being used throughout the statute. Some commenters have questioned whether the collection of such “about” communications complies with the statute. We conclude that Section 702 may permissibly be interpreted to allow “about” collection as it is currently conducted.

Collection of “about” communications occurs only in upstream collection, not in PRISM. Unlike PRISM collection, upstream collection acquires “Internet transactions,” meaning packets of data that traverse the Internet, directly from the Internet “backbone.” Utilizing this method, the government is able to capture communications that contain an approved selector, no matter where it appears in the communication — whether in the “to” or “from” lines of an email, for instance, or in the body of the email.

As discussed in Part 3 above, there are technical reasons why “about” collection is needed to acquire even some communications that are “to” and “from” a target. Some other

390 See pages 77-79 of this Report.
392 PCLOB March 2014 Hearing Transcript, supra, at 63.
types of "about" communications also involve Internet activity of the actual target. For some communications, the NSA’s collection devices are not able to distinguish between communications that are actually "to" or "from" a target and those in which the selector is found in the body or a communication, nor can they distinguish among the different types of "about" communications. Thus, under current technology and program design, in order to avoid significant gaps in upstream collection coverage, “about” collection is largely a technical inevitability.394

As a result, if the selector is contained within the body of a communication, “about” collection may result in the acquisition of communications between two non-targets. In some such instances, both of the individuals who are parties to the communication could be U.S. persons or persons located within the United States. This occurs because the current state of technology renders the government unable to determine with certainty the location of all communicants at the time of acquisition.

In addition, upstream collection leads to the acquisition of multi-communication transactions ("MCTs").395 As explained in Part 3 above, MCTs that contain a communication to, from, or about a target may be embedded within communications that are between U.S. persons or persons located within the United States, and the government has not been able to design a filter that would acquire only the single discrete communications within transactions that contain a selector.

Thus, due to the inclusion of “about” collection and the collection of MCTs, there is a greater risk that the NSA will acquire purely domestic communications through upstream collection than through PRISM. This risk is mitigated to some extent by the fact that through the upstream process, Internet transactions are first filtered to help eliminate potential domestic transactions before they are screened to determine whether a transaction contains a tasked selector. Further, NSA’s minimization procedures include more stringent safeguards for upstream data than they do for PRISM data. In particular, the NSA, the only agency that conducts upstream collection and the only agency that has access to unminimized results of upstream collection, is not permitted to use U.S. person identifiers in conducting queries of the upstream data. In addition, the retention period for

---

394 As a general rule, in conducting traditional wiretaps, the government has been permitted to access a trunk line if it has no reasonable physical access to a particular line or device, subject to strict limits on retention and use of non-targeted communications.

395 The acquisition of MCTs through the upstream collection process, and the minimization procedures adopted to address the specific challenges posed by acquisition of MCTs, are described in detail in Part 3 of this Report. The constitutional and policy questions raised by the collection of MCTs are addressed in those respective sections of this Report.
Internet communications collected through upstream is two years, as opposed to the NSA’s five-year retention period for data collected in PRISM.\(^{396}\)

Given the lack of any textual prohibition, as well as the present technical necessity of capturing “about” communications in certain circumstances as part of the upstream collection process, we conclude that the inclusion of “about” collection under the current operation of the program is a permissible reading of the statute.

III. Constitutional Analysis

Evaluating the constitutionality of the Section 702 program poses unique challenges. Unlike the typical Fourth Amendment inquiry, where the legitimacy of “a particular search or seizure” is judged “in light of the particular circumstances” of that case,\(^{397}\) evaluating the government’s implementation of Section 702 requires assessing a complex surveillance program — one that entails many separate decisions to monitor large numbers of individuals, resulting in the annual collection of hundreds of millions of communications of different types, obtained through a variety of methods, pursuant to multiple foreign intelligence imperatives, and involving four intelligence agencies that each have their own rules governing how they may handle and use the communications that are acquired.\(^{398}\)

Further complicating the analysis, the constitutional interests at stake are not those of the persons targeted for surveillance under Section 702, all of whom lack Fourth Amendment rights because they are foreigners located outside of the United States.\(^{399}\)

\(^{396}\) Minimization Procedures used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, § 3(c) (Oct. 31, 2011) (“NSA 2011 Minimization Procedures”).


\(^{398}\) Most programs of searches or seizures that have been evaluated under the Fourth Amendment have involved uniform practices that advanced a single government interest through standardized means that intruded upon the privacy interests of each person affected in the same manner. See, e.g., Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995) (drug testing of student athletes); Michigan Dep’t of State Police v. Sitz, 496 U.S. 444 (1990) (highway sobriety checkpoints). Courts also sometimes undertake programmatic assessments in response to statutory facial challenges, where they evaluate “the constitutionality of a statute without factual development centered around a particular application.” In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1009 (FISA Ct. Rev. 2008) (citing Wash. State Grange v. Wash. State Repub. Party, 128 S. Ct. 1184, 1190 (2008)). Here, however, the Board has not asked whether Section 702 “is valid on its face — a question that would be answered by deciding whether any application of the statute passed constitutional muster.” Id. at 1009-10. Instead, it has asked whether “this specific application” of the statute — the program as it is conducted today — is consistent with the Constitution. Id. at 1010.

\(^{399}\) See United States v. Verdugo-Urquidez, 494 U.S. 259, 274-75 (1990) (holding that the Fourth Amendment has no application to a physical search in a foreign country of the residence of a citizen of that country who has no voluntary attachment to the United States).
Instead, the relevant Fourth Amendment interests are those of the U.S. persons whose communications may be acquired despite not themselves having been targeted for surveillance.\textsuperscript{400}

Although U.S. persons and other persons in the United States may not be targeted under Section 702, operation of the program nevertheless results in the government acquiring some telephone and Internet communications involving U.S. persons, potentially in large numbers. As explained above, this acquisition can occur in four main situations:

1. A U.S. person communicates by telephone or Internet with a foreigner located abroad who has been targeted. The government refers to this as “incidental” collection.

2. A U.S. person sends or receives an Internet communication that is routed internationally and that includes a reference to a selector such as an email address used by a foreigner who has been targeted. The government refers to this as “about” collection.\textsuperscript{401}

3. A U.S. person sends or receives an Internet communication that is embedded within the same “transaction” as a different communication that meets the requirements for acquisition (because it is to or from a targeted foreigner or includes a reference to the communications identifier of a targeted foreigner). The government refers to these transactions containing more than one separate communication as “multiple-communication transactions” or “MCTs.”\textsuperscript{402}

4. A U.S. person’s communications are acquired by mistake due to a targeting error, an implementation error, or a technological malfunction. The government refers to this as “inadvertent” collection.

Any Fourth Amendment assessment of the Section 702 program must take into account the cumulative privacy intrusions and risks of all four categories above, together with the limits and protections built into the program that mitigate them.\textsuperscript{403}

\textsuperscript{400} In addition to U.S. persons, foreign citizens temporarily and voluntarily present within the United States likely possess Fourth Amendment rights. \textit{See Verdugo-Urquidez}, 494 U.S. at 278 (Kennedy, J., concurring).

\textsuperscript{401} See pages 37-39 of this Report for an explanation of “about” collection.

\textsuperscript{402} See pages 39-41 of this Report for a discussion of “MCTs.”

\textsuperscript{403} Apart from these four categories, there is of course a risk that government personnel could deliberately misuse the Section 702 program to target a U.S. person for surveillance. Doing so would be grounds for professional sanction and possibly criminal prosecution, however, and auditing procedures are in place to deter such wrongdoing. Every targeting decision made by an analyst is recorded and reviewed both by supervisors within the NSA and also by a joint oversight team from the Department of Justice and Office of
After analyzing these factors, the Board finds that the core of this program — acquiring the communications of specifically targeted foreign persons who are located outside the United States, upon a belief that those persons are likely to communicate foreign intelligence, using specific communications identifiers, subject to FISA court-approved targeting rules that have proven to be accurate in targeting persons outside the United States, and subject to multiple layers of rigorous oversight — fits within the totality of the circumstances test for reasonableness as it has been defined by the courts to date. Outside of this fundamental core, certain aspects of the Section 702 program push the entire program close to the line of constitutional reasonableness. Such aspects include the scope of the incidental collection of U.S. persons’ communications, the use of “about” collection to acquire Internet communications that are neither to nor from the target of surveillance, and the use of queries to search the information collected under the program for the communications of specific U.S. persons. With these concerns in mind, this Report offers a set of policy proposals designed to push the program more comfortably into the sphere of reasonableness, ensuring that the program remains tied to its constitutionally legitimate core.

A. Privacy in Telephone and Internet Communications

The Fourth Amendment protects the right of the people “to be secure in their persons, houses, papers, and effects.” It thus prohibits “unreasonable searches and seizures” by the government, and it specifies that a warrant authorizing a search or seizure may issue only “upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”404 A search occurs not only where the government intrudes on a person’s tangible private property to obtain information, but also where “the government violates a subjective expectation of privacy that society recognizes as reasonable.”405

Because individuals who are protected by the Constitution have a reasonable expectation of privacy in their telephone conversations, it has long been the rule that wiretapping conducted within the United States for criminal or other domestic purposes is presumptively unreasonable under the Fourth Amendment unless the government has obtained a warrant based on probable cause.406 While the Supreme Court has not expressly

---

404 U.S. Const. amend. IV.


ruled on the extent of Fourth Amendment protection for Internet communications, lower
courts have concluded that emails are functionally analogous to mailed letters and that
therefore their contents cannot be examined by the government without a warrant. The
same may be true for other, similarly private forms of Internet communication, although
this question awaits further development by the courts.

B. Foreign Intelligence Exception to the Warrant Requirement

Under the authority of Section 702, the government collects telephone and Internet
communications without obtaining individual judicial warrants for the specific people it
targets. Decisions about which telephone and Internet communications to collect are made
by executive branch personnel without court review. While the FISC plays a role in
overseeing the categories of foreign intelligence the government seeks, the procedures it
employs, and its adherence to statutory and constitutional limits, the court has no part in
approving individual targeting decisions.

“Although as a general matter, warrantless searches are per se unreasonable under
the Fourth Amendment, there are a few specifically established and well-delineated
exceptions to that general rule.” And while wiretapping and other forms of domestic
electronic surveillance generally require a warrant, the Supreme Court has left open the
question of whether “safeguards other than prior authorization by a magistrate would
satisfy the Fourth Amendment in a situation involving the national security” and “the
activities of foreign powers.”

In other words, there may be a “foreign intelligence exception” to the warrant
requirement permitting the executive branch to conduct wiretapping and other forms of
electronic surveillance without judicial approval. The Supreme Court has not decided
whether such an exception exists, in part because the 1978 enactment of the Foreign
Intelligence Surveillance Act ("FISA") forestalled the question: the Act established a
framework for foreign intelligence surveillance under which the executive branch obtains

---

407 See United States v. Warshak, 631 F.3d 266, 285-86 (6th Cir. 2010) (stating that “[g]iven the
fundamental similarities between email and traditional forms of communication, it would defy common sense
to afford emails lesser Fourth Amendment protection,” and holding that government agents must obtain a
warrant based on probable cause before compelling an Internet service provider to turn over the contents of
a subscriber’s emails); United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996) (holding that “the transmitter
of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission
without probable cause and a search warrant.”); Bates October 2011 Opinion, supra, at 73-74, 2011 WL
10945618, at *26 (“A person’s ‘papers’ are among the four items that are specifically listed in the Fourth
Amendment as subject to protection against unreasonable search and seizure. Whether they are transmitted
by letter, telephone or e-mail, a person’s private communications are akin to personal papers.”).

quotation marks omitted).

(1972) ("Keith").
warrant-like orders from the FISA court before engaging in surveillance that falls within the ambit of the statute.\footnote{See 50 U.S.C. §§ 1801-1812; In re Terrorist Bombings of U.S. Embassies in E. Africa, 552 F.3d 157, 161 (2d Cir. 2008).}

While the Supreme Court has not spoken, lower courts evaluating surveillance conducted before the enactment of FISA addressed the existence of a foreign intelligence exception, and every court to decide the question recognized such an exception.\footnote{See United States v. Truong Dinh Hung, 629 F.2d 908, 913 (4th Cir. 1980); United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977); United States v. Butenko, 494 F.2d 593, 605 (3d Cir. 1974); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973); but see Zweibon v. Mitchell, 516 F.2d 594, 618-20 (D.C. Cir. 1975).} More recently the Foreign Intelligence Surveillance Court of Review concluded that a foreign intelligence exception permitted warrantless surveillance “directed at a foreign power or an agent of a foreign power” — which could include U.S. citizens — under the Protect America Act, a predecessor to Section 702.\footnote{See In re Directives, 551 F.3d at 1010-12.}

This precedent does not neatly resolve all questions about the existence and scope of a foreign intelligence exception to the warrant requirement.\footnote{Apart from the distinctions noted above, nearly all of the relevant decisions predated the implementation of FISA’s surveillance framework beginning in 1978, and experience with FISA and the FISA court since then arguably undermines some of the rationales underlying the foreign intelligence exception, such as the fear that a warrant requirement will unduly “reduce the flexibility of executive foreign intelligence initiatives” and that the judiciary is ill-suited to address “the delicate and complex decisions that lie behind foreign intelligence surveillance.” Truong Dinh Hung, 629 F.2d at 913.} The Board takes no position here on the existence or scope of that exception. We note that the program’s intrusion on U.S. persons’ privacy is reduced by its focus on targeting individually selected foreigners located outside the United States from whom the government reasonably

\begin{itemize}
\item It is not necessarily clear that the Section 702 program would fall within the scope of the foreign intelligence exception recognized by these decisions, which were limited to surveillance directly authorized by the Attorney General, targeting foreign powers or their agents, and/or pursuing foreign intelligence as the primary or sole purpose of the surveillance. See \textit{Truong Dinh Hung}, 629 F.2d at 912-16 (approving surveillance authorized by Attorney General “only if [the executive] is attempting primarily to obtain foreign intelligence from foreign powers or their assistants”); \textit{Buck}, 548 F.2d at 875 (approving surveillance “expressly authorized by the Attorney General”); \textit{Butenko}, 494 F.2d at 596, 606 (approving surveillance “concerning activities within the United States of foreign powers” where “the primary purpose of these searches is to secure foreign intelligence information”); \textit{Brown}, 484 F.2d at 421 (approving “electronic surveillance authorized by the Attorney General and made solely for the purpose of gathering foreign intelligence”). Under Section 702, targets are selected by NSA personnel without Attorney General approval, and they need not be foreign powers or their agents; foreign intelligence need only be “a significant purpose” of the surveillance. See 50 U.S.C. § 1881a(a)(g)(2)(A)(v).
\item Critically, however, Section 702 targets cannot be U.S. persons or anyone located in the United States. Moreover, limits expressed in pre-FISA opinions addressing the president’s inherent and unilateral constitutional power to conduct foreign intelligence surveillance do not necessarily apply to executive implementation of a congressionally enacted statute that involves oversight by all three branches of government. See \textit{United States v. Abu-Jihaad}, 630 F.3d 102, 121 (2d Cir. 2010).
\end{itemize}
expects to obtain foreign intelligence — and by the government’s employment of oversight mechanisms to help ensure adherence to those limitations. Unlike the warrantless surveillance of the pre-FISA era, U.S. persons and others in the United States cannot be targeted under this program, and therefore the government never will be permitted to collect and retain their entire communications history.\footnote{If a U.S. person or someone located in the United States is inadvertently targeted based on an erroneous belief about that person’s nationality or location, all of the communications acquired through that targeting must be destroyed, unless, for example, the Director or Acting Director of the NSA specifically determines in writing that an individual communication should be retained because it satisfies one of four criteria. See pages 49-50 of this Report.} Instead, the government will have access only to those scattered communications that occur between a U.S. person and a targeted overseas foreigner, or that are acquired through “about” collection or as part of an MCT (which are subject to special limitations on retention and use). Moreover, the fact that the people targeted under Section 702 are situated in foreign countries may often make it difficult and time-consuming for the government to assemble documentation about them sufficient to obtain independent judicial approval for surveillance — while those targets’ lack of Fourth Amendment rights militates against any legal obligation to obtain such approval or to strictly limit targeting to foreign powers and their agents.

C. The “Reasonableness” Framework

“Even if a warrant is not required, a search is not beyond Fourth Amendment scrutiny; for it must be reasonable in its scope and manner of execution.”\footnote{Maryland v. King, 133 S. Ct. 1958, 1970 (2013).} Thus, “even though the foreign intelligence exception applies in a given case, governmental action intruding on individual privacy interests must comport with the Fourth Amendment’s reasonableness requirement.”\footnote{In re Directives, 551 F.3d at 1012 (citing United States v. Place, 462 U.S. 696, 703 (1983)).} The absence of a warrant requirement simply means that, “rather than employing a per se rule of unreasonableness,” privacy concerns and governmental interests must be balanced to determine if the intrusion is reasonable.\footnote{King, 133 S. Ct. at 1970 (quoting Illinois v. McArthur, 531 U.S. 326, 331 (2001)).}

“Whether a search is reasonable,” therefore, “is determined by assessing, on the one hand, the degree to which it intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.”\footnote{Samson v. California, 547 U.S. 843, 848 (2006) (internal quotation marks omitted).} Making this determination requires considering the “totality of the circumstances.”\footnote{Samson, 547 U.S. at 848.}

Applying this test to a program of intelligence gathering demands “sensitivity both to the government’s right to protect itself from unlawful subversion and attack and to the
citizen’s right to be secure in his privacy against unreasonable government intrusion.”

When considering surveillance directed at national security threats, particularly those of a foreign nature, it is appropriate to “begin the inquiry by noting that the President of the United States has the fundamental duty, under Art. II, § 1, of the Constitution, to ‘preserve, protect and defend the Constitution of the United States,’” and that “[i]mplicit in that duty is the power to protect our government against those who would subvert or overthrow it by unlawful means.” More broadly, the government’s interest in protecting national security “is of the highest order of magnitude.”

Additional consideration is due to the fact that the executive branch, acting under Section 702, is not exercising its Article II power unilaterally, but rather is implementing a statutory scheme enacted by Congress after public deliberation regarding the proper balance between the imperatives of privacy and national security. By establishing a statutory framework for surveillance conducted within the United States but exclusively targeting overseas foreigners, subject to certain limits and oversight mechanisms, “Congress sought to accommodate and advance both the government’s interest in pursuing legitimate intelligence activity and the individual’s interest in freedom from improper government intrusion.”

The framework of Section 702, moreover, includes a role for the judiciary in ensuring compliance with statutory and constitutional limits, albeit a more circumscribed role than the approval of individual surveillance requests. Where, as here, “the powers of all three branches of government — in short, the whole of federal authority” — are involved in establishing and monitoring the parameters of an intelligence-gathering activity, the Fourth Amendment calls for a different calculus than when the executive branch acts alone.

Furthermore, the hostile activities of terrorist organizations and other foreign entities are prone to being geographically dispersed, long-term in their planning, conducted in foreign languages or in code, and coordinated in large part from locations outside the reach of the United States. Accordingly, “complex, wide-ranging, and

---

420 Keith, 407 U.S. at 299 (addressing intelligence gathering aimed at domestic national security threats).

421 Keith, 407 U.S. at 310.

422 In re Directives, 551 F.3d at 1012 (citing Haig v. Agee, 453 U.S. 280, 307 (1981)); see Keith, 407 U.S. at 312 (“It has been said that ‘[t]he most basic function of any government is to provide for the security of the individual and of his property.’” (citation omitted)).

423 United States v. Cavanagh, 807 F.2d 787, 789 (9th Cir. 1987) (addressing traditional FISA).

424 Abu-Jihaad, 630 F.3d at 121 (addressing traditional FISA); cf. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635-38 (1952) (Jackson, J., concurring).
decentralized organizations, such as al Qaeda, warrant sustained and intense monitoring in order to understand their features and identify their members.\footnote{In re Terrorist Bombings, 552 F.3d at 175 (citing In re Sealed Case, 310 F.3d 717, 740-41 (FISA Ct. Rev. 2002)).}

On the other side of the coin, the acquisition of private communications intrudes on Fourth Amendment interests. Even though U.S. persons and persons located in the United States are subject to having their telephone conversations collected only when they communicate with a targeted foreigner located abroad, the program nevertheless gains access to numerous personal conversations of U.S. persons that were carried on under an expectation of privacy. Email communications to and from U.S. persons, which the FISA court has said are akin to “papers” protected under the Fourth Amendment,\footnote{See Bates October 2011 Opinion, supra, at 74, 2011 WL 10945618, at *26 (“[T]he Supreme Court has held that the parties to telephone communications and the senders and recipients of written communications generally have a reasonable expectation of privacy in the contents of those communications . . . . The intrusion resulting from the interception of the contents of electronic communications is, generally speaking, no less substantial.”). Since the nineteenth century, in order to protect the security of personal papers and effects, the Supreme Court has held that the government cannot engage in a warrantless search of the contents of sealed mail. Ex parte Jackson, 96 U.S. 727, 733 (1877) (“Letters . . . in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles.”). The Sixth Circuit Court of Appeals has held that email enjoys constitutional protection no less than physical letters. Warshak, 631 F.3d at 284-86.\footnote{See Samson, 547 U.S. at 848.}} are also subject to collection in a variety of circumstances. Digital tools enable the government to query the repository of collected communications to locate communications involving a given person in search of foreign intelligence or evidence of a crime.\footnote{See pages 55-60 of this Report for a description of the rules and procedures governing queries.}

**D. Holistic Assessment of Reasonableness**

As discussed elsewhere in this Report, the Board believes that the Section 702 program significantly aids the government’s efforts to prevent terrorism, as well as to combat weapons proliferation and gather foreign intelligence for other purposes. The question, then, is how the program’s intrusion on the privacy of U.S. persons weighs against its substantial contribution to these governmental interests.\footnote{See Samson, 547 U.S. at 848.}

This evaluation must consider the program as a whole — taking into account how and why the communications of U.S. persons are acquired and what is done with them afterward. Thus, the privacy risks posed by the comparatively broad scope of targeting under this program and the absence of individual warrants must be offset by the applicable rules restricting the acquisition, use, dissemination, and retention of the communications that are acquired. In this regard, we must consider whether practices that permit use of U.S.
persons’ communications after their collection are appropriate given the less rigorous rules on targeting that permitted their acquisition.

This holistic approach is consistent with available precedent. When evaluating governmental policies authorizing warrantless searches or seizures, the Supreme Court has indicated that limits on the uses to which the collected information may be put, and on access to that information, bear on the policy’s reasonableness under the Fourth Amendment.\textsuperscript{429} Lower courts addressing the traditional FISA process have similarly noted that, despite its somewhat more lenient requirements compared with traditional criminal wiretaps, it safeguards privacy rights through “an expanded conception of minimization that differs from that which governs law-enforcement surveillance.”\textsuperscript{430} The Foreign Intelligence Surveillance Court of Review, addressing a surveillance program with similarities to Section 702, emphasized the “matrix of safeguards” governing the program, including “effective minimization procedures” that “serve[d] as an additional backstop against identification errors as well as a means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons.”\textsuperscript{431} The FISA court has applied this approach to Section 702, having “recognized that the procedures governing retention, use, and dissemination bear on the reasonableness under the Fourth Amendment of a program for collecting foreign intelligence information.”\textsuperscript{432}

The government has acknowledged that the Fourth Amendment rights of U.S. persons are affected when their communications are acquired under Section 702 incidentally or otherwise, and it has echoed the FISA court’s observation that the implementation of adequate minimization procedures is part of what makes the collection reasonable.\textsuperscript{433}

\textsuperscript{429} See, e.g., \textit{King}, 133 S. Ct. at 1967 (in approving collection of DNA information from arrestees, ascribing significance to restrictions on the information that may be added to databases and for what purposes it may be used); \textit{Vernonia}, 515 U.S. at 658 (emphasizing that “the results of the [drug] tests [for student athletes] are disclosed only to a limited class of school personnel who have a need to know; and they are not turned over to law enforcement authorities or used for any internal disciplinary function”).

\textsuperscript{430} \textit{United States v. Belfield}, 692 F.2d 141, 148 (D.C. Cir. 1982) (citation omitted).

\textsuperscript{431} \textit{In re Directives}, 551 F.3d at 1013, 1015.

\textsuperscript{432} See Bates October 2011 Opinion, \textit{supra}, at 77, 2011 WL 10945618, at *27. Exemplifying this approach, when the FISA court concluded that the upstream portion of the program was unreasonably acquiring too many domestic and irrelevant communications through the collection of MCTs, it declared that portion of the program to violate the Fourth Amendment, but it later concluded that the program had returned within constitutional bounds after new procedures were adopted to specially handle those communications. \textit{See id.} at 68-79, 2011 WL 10945618, at *24-28; \textit{see also Memorandum Opinion, [Caption Redacted], [Docket No. Redacted]}, 2011 WL 10947772 (FISA Ct. Nov. 30, 2011), available at http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents.

\textsuperscript{433} See PCLOB March 2014 Hearing Transcript, \textit{supra}, at 15 (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ) (“That’s not to say that U.S. persons whose communications are collected incidentally doesn’t trigger a Fourth Amendment review. It does. Those people
An important ramification of this holistic approach is that concerns about post-collection practices such as the use of queries to search for the communications of specific U.S. persons cannot be dismissed on the basis that the communications were “lawfully collected.” Rather, whether Section 702 collection is constitutionally reasonable in the first place, and hence “lawful,” depends on the reasonableness of the surveillance regime as a whole, including whether its rules affecting the acquisition, use, dissemination, and retention of the communications of U.S. persons appropriately balance the government’s valid interests with the privacy of U.S. persons.

This totality of the circumstances test is applicable when examining the implications of “incidental” collection. Where a wiretap is conducted in a criminal investigation pursuant to a warrant, satisfaction of the three requirements of the warrant clause (probable cause, particularity, and prior judicial review)\(^ {434}\) renders the wiretap constitutionally reasonable — both as to the intended subjects of the surveillance and as to any persons who end up being incidentally overheard, the full range of whom the government can never predict.\(^ {435}\) Likewise, under Title I of FISA, the government obtains warrant-like orders from the FISA court that require a modified form of particularity and probable cause.\(^ {436}\) Just as the requirements of judicial review, probable cause, and particularity render a wiretap constitutionally reasonable in the criminal context, even as to individuals about whom the government had no prior evidence, so the corresponding protections of Title I of FISA render it reasonable under the Fourth Amendment, courts have held.\(^ {437}\)

However, where surveillance is undertaken without individual warrants or judicial orders, as under Section 702, and where the warrant requirements therefore are not satisfied, the legitimacy of the surveillance must be assessed under the reasonableness standard of the Fourth Amendment as described above, weighing the competing privacy

---


435 See United States v. Donovan, 429 U.S. 413, 427 n.15 (1977); United States v. Kahn, 415 U.S. 143, 155 n.15 (1974); United States v. Gaines, 639 F.3d 423, 429-33 (8th Cir. 2011); United States v. Urban, 404 F.3d 754, 773-74 (3d Cir. 2005); United States v. Tehfe, 722 F.2d 1114, 1118 (3d Cir. 1983); United States v. Ramsey, 503 F.2d 524, 526 n.7 (7th Cir. 1974). Of course, even a validly authorized wiretap or other search can be executed in a constitutionally unreasonable manner.

436 See In re Sealed Case, 310 F.3d at 739-40.

437 See, e.g., United States v. Stewart, 590 F.3d 93, 129 (2d Cir. 2009); In re Sealed Case, 310 F.3d at 741; United States v. Pelton, 835 F.2d 1067, 1075 (4th Cir. 1987); Cavanagh, 807 F.2d at 789-91; United States v. Duggan, 743 F.2d 59, 79-80 & n.7 (2d Cir. 1984).
and governmental interests while taking into account the totality of circumstances. Thus, even where only foreigners outside the United States are targeted, the nature of the collection and use of some communications involving a U.S. person bears on the constitutional reasonableness of the program. Simply put, the “totality of the circumstances” that must be considered under the Fourth Amendment in this context may include factors such as why U.S. persons’ communications are acquired, the frequency with which they are acquired, how long they may be retained, who is given access to them, whether and how the government may query them for information about specific U.S. persons, under what circumstances they may be disseminated, and what degree of oversight attends to these matters. For instance, given the comparatively low standards for collection of information under Section 702, standards for querying the collected data to find the communications of specific U.S. persons may need to be more rigorous than where higher standards are required at the collection stage.

Applying this holistic inquiry to the Section 702 program therefore requires examining a web of factors bearing on the collection, use, dissemination, and retention of the communications of U.S. persons under the program. Pulling one of the threads of this web, in a more or less privacy-protective direction, alters the total picture. The ultimate Fourth Amendment assessment rests on an appraisal of the point at which any particular feature of the program, or any particular combination of features, goes too far and pushes the program across the threshold of unreasonableness.

In the Board’s view, the core of this program — acquiring the communications of specifically targeted foreign persons who are located outside the United States, upon a belief that those persons are likely to communicate foreign intelligence, using specific communications identifiers, subject to FISA court–approved targeting rules that have proven to be accurate in targeting persons outside the United States, and subject to multiple layers of rigorous oversight — fits within the totality of the circumstances test for reasonableness as it has been defined by the courts to date.

Outside of this fundamental core, certain aspects of the Section 702 program raise questions about whether its impact on U.S. persons pushes the program over the edge into constitutional unreasonableness. Such aspects include the scope of the incidental collection of U.S. persons’ communications, the use of “about” collection to acquire Internet communications that are neither to nor from the target of surveillance, the collection of MCTs that predictably will include U.S. persons’ Internet communications unrelated to the purpose of the surveillance, the use of database queries to search the information collected under the program for the communications of specific U.S. persons, and the possible use of
communications acquired under the program for criminal assessments, investigations, or proceedings that have no relationship to foreign intelligence.\textsuperscript{438}

These features of the Section 702 program, and their cumulative potential effects on the privacy of U.S. persons, push the entire program close to the line of constitutional reasonableness. At the very least, too much expansion in the collection of U.S. persons’ communications or the uses to which those communications are put may push the program over the line. The response if any feature tips the program over the line is not to discard the entire program; instead, it is to address that specific feature.

With these concerns in mind, the next section of this Report offers a set of proposals designed to push the program more comfortably into the sphere of reasonableness, ensuring that the program remains tied to its constitutionally legitimate core. Because the same factors that bear on Fourth Amendment reasonableness under a “totality of the circumstances” test are equally relevant to an assessment based purely on policy, the Board opts to present its proposals for changes to the Section 702 program as policy recommendations, without rendering a judgment about which, if any, of those proposals might be necessary from a constitutional perspective. This approach is fitting because some of the facts that may bear on the reasonableness of the Section 702 program under the Fourth Amendment, such as how many U.S. persons’ communications and domestic communications are acquired, simply are not known. It also permits us to offer the recommendations that we believe are merited on privacy grounds without making fine-tuned determinations about whether any aspect of the status quo is constitutionally fatal, and without limiting our recommendations to changes that we may deem constitutionally required.

In sum, the Board has carefully considered the totality of the circumstances surrounding the Section 702 program that must be considered in assessing the program’s reasonableness under the Fourth Amendment, but rather than render a judgment about the constitutionality of the program as a whole, the Board instead has addressed the areas of concern it has identified by formulating recommendations for changes to those aspects of the program.

\textsuperscript{438} Anecdotally, the FBI has advised the Board that it is extremely unlikely that an agent or analyst who is conducting an assessment of a non–national security crime would get a responsive result from the query against the Section 702–acquired data.
IV. Analysis of Treatment of Non-U.S. Persons

The treatment of non-U.S. persons under U.S. surveillance programs raises important but difficult legal and policy questions. Privacy is a human right that has been recognized most prominently in the International Covenant on Civil and Political Rights ("ICCPR"), an international treaty ratified by the U.S. Senate. Many of the generally applicable protections that already exist under U.S. surveillance laws apply to U.S. and non-U.S. persons alike. The President’s recent initiative under Presidential Policy Directive 28 on Signals Intelligence ("PPD-28") will further address the extent to which non-U.S. persons should be afforded the same protections as U.S. persons under U.S. surveillance laws. Because PPD-28 invites the PCLOB to be involved in its implementation, the Board has concluded that it can make its most productive contribution in assessing these issues in the context of the PPD-28 review process.

A. Existing Legal Protections for Non-U.S. Persons’ Privacy

A number of provisions of Section 702, as well as provisions in other U.S. surveillance laws, protect the privacy of U.S. and non-U.S. persons alike. These protections can be found, for example, in (1) limitations on the scope of authorized surveillance under Section 702; (2) damages and other civil remedies that are available to subjects of unauthorized surveillance as well as sanctions that can be imposed on government employees who engage in such conduct; and (3) prohibitions on unauthorized secondary use and disclosure of information acquired pursuant to the Section 702 program. These sources of statutory privacy protections are discussed briefly.

The first important privacy protection provided to non-U.S. persons is the statutory limitation on the scope of Section 702 surveillance, which requires that targeting be conducted only for purposes of collecting foreign intelligence information. The definition of foreign intelligence information purposes is limited to protecting against actual or potential attacks; protecting against international terrorism, and proliferation of weapons of mass destruction; conducting counter-intelligence; and collecting information with respect to a foreign power or foreign territory that concerns U.S. national defense or foreign affairs. Further limitations are imposed by the required certifications identifying the specific categories of foreign intelligence information, which are reviewed and


441 50 U.S.C. § 1801(e).
approved by the FISC. These limitations do not permit unrestricted collection of information about foreigners.

The second group of statutory privacy protections for non-U.S. persons are the penalties that apply to government employees who engage in improper information collection practices — penalties that apply whether the victim is a U.S. person or a non-U.S. person. Thus, if an intelligence analyst were to use the Section 702 program improperly to acquire information about a non-U.S. person (for example, someone with whom he or she may have had a personal relationship), he or she could be subject not only to the loss of his or her employment, but to criminal prosecution. Finally, a non-U.S. person who was a victim of a criminal violation of either FISA or the Wiretap Act could be entitled to civil damages and other remedies. In sum, if a U.S. intelligence analyst were to use the Section 702 program to collect information about a non-U.S. person where it did not both meet the definition of foreign intelligence and relate to one of the certifications approved by the FISA court, he or she could face not only the loss of a job, but the prospect of a term of imprisonment and civil damage suits.

The third privacy protection covering non-U.S. persons is the statutory restriction on improper secondary use found at 50 U.S.C. § 1806, under which information acquired from FISA-related electronic surveillance may not “be used or disclosed by Federal officers or employees except for lawful purposes.” Congress included this language “to insure that information concerning foreign visitors and other non-U.S. persons . . . is not used for illegal purposes.” Thus, use of Section 702 collection for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion, would violate Section 1806.

Further, FISA provides special protections in connection with legal proceedings, under which an aggrieved person — a term that includes non-U.S. persons — is required to be notified prior to the disclosure or use of any Section 702–related information in any

\[\text{442} \quad 50 \text{ U.S.C. § 1881a(g)(2)(A)(v).}\]
\[\text{443} \quad \text{See Bates October 2011 Opinion, supra, at 17 n.15, 2011 WL 10945618, at *6 n.15 (criminal penalties of 50 U.S.C. § 1809 of the FISA are implicated by Section 702 surveillance that strays beyond the scope of the court’s order approving such activities). In addition, to the extent that Section 702 program surveillance strayed from the certifications approved by the FISA court, it would potentially implicate the criminal provisions of the Wiretap Act, 18 U.S.C. § 2511(1), because the Section 702 surveillance would then lose its safe harbor for authorized FISA activities under Section 2511(2)(e) of the Wiretap Act.}\]
\[\text{444} \quad \text{See 50 U.S.C. § 1810 ("aggrieved person" not limited to U.S. persons); 18 U.S.C. § 2520 ("any person" not limited to U.S. persons); see also Suzlon Energy Ltd. v. Microsoft Corp., 671 F.3d 726, 728-29 (9th Cir. 2011) (construing the statutory term "any person" to include non-U.S. persons).}\]
\[\text{445} \quad 50 \text{ U.S.C. § 1806(a) (incorporated into Section 702 by 50 U.S.C. § 1881e(a)).}\]
\[\text{446} \quad \text{H.R. Rep. No. 95-1283(I), at 88-90 (1978) (discussing Section 106 of H.R. 7308, which became Section 106 of the FISA).}\]
federal or state court. The aggrieved person may then move to suppress the evidence on
the grounds that it was unlawfully acquired and/or was not in conformity with the
authorizing Section 702 certification. Determinations regarding whether the Section 702
acquisition was lawful and authorized are made by a United States District Court, which has
the authority to suppress any evidence that was unlawfully obtained or derived.

Finally, as a practical matter, non-U.S. persons also benefit from the access and
retention restrictions required by the different agencies’ minimization and/or targeting
procedures. While these procedures are legally required only for U.S. persons, the cost and
difficulty of identifying and removing U.S. person information from a large body of data
means that typically the entire dataset is handled in compliance with the higher U.S. person
standards.

B. President’s Initiative to Protect the Privacy of Non-U.S. Persons

As a matter of international law, privacy is a human right that has been recognized
most prominently in the ICCPR, an international treaty ratified by the U.S. Senate. The
question of how to apply the ICCPR right of privacy to national security surveillance,
however, especially surveillance conducted in one country that may affect residents of
another country, has to this point not been settled among the signatories to the treaty and
is the subject of ongoing spirited debate.

The executive branch is currently engaged in an extensive review of the extent to
which, as a policy matter, the United States should afford all persons, regardless of
nationality, a common baseline level of privacy protections in connection with foreign
intelligence surveillance. This review began on January 17 of this year, when President
Obama issued PPD-28, in which he directed the review of the treatment of information
regarding non-U.S. persons in connection with its surveillance programs.

Issues relating to the treatment of non-U.S. persons in government surveillance
programs are by no means limited to the Section 702 program. Questions arise in

---

447 See 50 U.S.C. § 1806(c), (d).
448 50 U.S.C. § 1806(e).
449 50 U.S.C. § 1806(f), (g).
450 The United States currently interprets the ICCPR as not applying extra-territorially. Nonetheless the
Board has received thoughtful comments and testimony arguing to the contrary. The Board also notes that in
November 2013, the United Nations adopted, with United States support, a Resolution on “The right to
privacy in the digital age.” This resolution includes a provision requesting that the United Nations High
Commissioner for Human Rights develop and present a report examining “the protection and promotion of
the right to privacy in the context of domestic and extraterritorial surveillance and/or interception of digital
communications and collection of personal data, including on a mass scale.” This report is expected to be
presented in August 2014.
451 PPD-28, supra.
connection with signals intelligence conducted under other statutes and programs, including Executive Order 12333. Under PPD-28, the government has begun to address, as a matter of policy, the privacy and civil liberties of non-U.S. persons in connection with the full spectrum of signals intelligence programs conducted by the United States. The introduction to that directive notes that “signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information.”\textsuperscript{452} The government is presently in the process of implementing the principles set forth in that directive, including the requirement that “signals intelligence activities shall be as tailored as feasible.”\textsuperscript{453} PPD-28 sets forth a number of principles that have historically been, or will be, implemented, among them:

Privacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities. The United States shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion. Signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions and not for any other purposes.\textsuperscript{454}

Further, PPD-28 provides that:

U.S. signals intelligence activities must, therefore, include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where that individual resides.\textsuperscript{455}

The Intelligence Community has already begun reviewing various options for implementing PPD-28, and the Board will engage in this process. PPD-28 specifically provides for direct PCLOB participation:

The Privacy and Civil Liberties Oversight Board is encouraged to provide [the President] with a report that assesses the implementation of any matters contained within this directive that fall within its mandate.\textsuperscript{456}

\textsuperscript{452} PPD-28, supra.
\textsuperscript{453} PPD-28, supra, § 3(d).
\textsuperscript{454} PPD-28, supra, § 3(b).
\textsuperscript{455} PPD-28, supra, § 4.
\textsuperscript{456} PPD-28, supra, § 5(b).
The Board has thus concluded that the optimal way for it to assess the treatment of information of non-U.S. persons is in the broader context of the PPD-28 review where it can evaluate other surveillance programs, along with Section 702, with a view to an integrated approach to foreign subjects of surveillance and the collection of signals intelligence. The implementation of PPD-28 may change the way Section 702 is operated and in so doing alleviate some of the concerns that have been voiced about its treatment of non-U.S. persons.
Part 5:

POLICY ANALYSIS

I. Introduction

In the Board’s assessment, the Section 702 program has proven valuable in enabling the government to prevent acts of terrorism within the United States and abroad, and to pursue other foreign intelligence goals. The program has helped the government to learn about the membership and activities of terrorist organizations, as well as to discover previously unknown terrorist operatives and disrupt specific terrorist plots. Although the program is large in scope and involves collecting a great number of communications, it consists entirely of targeting individual persons and acquiring communications associated with those persons, from whom the government has reason to expect it will obtain certain types of foreign intelligence. The program does not operate by collecting communications in bulk.

At the same time, the communications of U.S. persons or people located in the United States may be acquired by the government under Section 702 in the course of targeting non-U.S. persons located abroad. The breadth of collection under the program and its technical complexity enhance this possibility. The communications of U.S. persons can be acquired when a U.S. person is in contact with a foreign target (who need not be involved in wrongdoing in order to be targeted), when the government makes a mistake, and in certain other situations. The government’s ability to query its databases for the communications of specific U.S. persons, and to retain and disseminate such communications under certain circumstances, heightens the potential for privacy intrusions.

The Board has been impressed with the rigor of the government’s efforts to ensure that it acquires only those communications it is authorized to collect, and that it targets only those persons it is authorized to target. Moreover, the government has taken seriously its obligations to establish and adhere to a detailed set of rules regarding how it handles U.S. person communications that it acquires under the program. Available figures suggest, consistent with the Board’s own assessment, that the primary focus of the Section 702 program remains monitoring non-U.S. persons located overseas for valid foreign intelligence purposes. Nevertheless, there are some indications that the government may be gathering and utilizing a significant amount of information about U.S. persons under Section 702. While the Board has seen no evidence of abuse of this information for improper purposes, the collection and examination of personal communications can be a
privacy intrusion even in the absence of abuse, and a number of the Board’s recommendations are motivated by a desire to provide more clarity and transparency regarding the government’s activities in the Section 702 program.

II. Value of the Section 702 Program

A. Advantages and Unique Capabilities

The Section 702 program makes a substantial contribution to the government’s efforts to learn about the membership, goals, and activities of international terrorist organizations, and to prevent acts of terrorism from coming to fruition. Section 702 allows the government to acquire a greater range of foreign intelligence than it otherwise would be able to obtain, and it provides a degree of flexibility not offered by comparable surveillance authorities.

Because the oversight mandate of the Board extends only to those measures taken to protect the nation from terrorism, our focus in this section is limited to the counterterrorism value of the Section 702 program, although the program serves a broader range of foreign intelligence purposes.457

Section 702 enables the government to acquire the contents of international telephone and Internet communications in pursuit of foreign intelligence. While this ability is to some degree provided by other legal authorities, particularly “traditional” FISA and Executive Order 12333, Section 702 offers advantages over these other authorities.

In order to conduct electronic surveillance under “traditional” FISA (i.e., Title I of the Foreign Intelligence Surveillance Act of 1978), the government must persuade the Foreign Intelligence Surveillance Court (“FISC” or “FISA court”), under a standard of probable cause, that an individual it seeks to target for surveillance is an agent of a foreign power, and that the telephone number or other communications facility it seeks to monitor is used, or is about to be used, by a foreign power or one of its agents.458 In addition, a high-level executive branch official must certify (with a supporting statement of facts) that a significant purpose of the surveillance is to obtain foreign intelligence, and that the information sought cannot reasonably be obtained through normal investigative techniques.459 To meet these requirements and satisfy the probable cause standard, facts must be gathered by the Intelligence Community, a detailed FISA court application must be drafted by the DOJ, the facts in the application must be vetted for accuracy, the senior

457 See page 25 of this Report.
government official’s certification must be prepared, the Attorney General must approve the application, and the application must be submitted to the FISA court, which must review it, determine if the pertinent standards are met, and, if so, grant it. 460 These steps consume significant time and resources. 461 In practice, FISA applications are lengthy and the process not infrequently takes weeks from beginning to final approval. 462

This system is deliberately rigorous, for it was designed to provide a check on the government’s surveillance of U.S. persons and other people located in the United States. Its goal was to prevent the abusive and politically motivated surveillance of U.S. persons and domestic activists that had occurred under the guise of foreign intelligence surveillance in the mid-twentieth century. Under FISA, electronic surveillance may be directed only at individuals who are acting at the behest of a foreign power (such as a foreign government or international terrorist organization), only for legitimate foreign intelligence purposes, and only where the aims of the surveillance cannot be achieved by other means. 463 The statute’s procedural hurdles help to ensure that surveillance takes place only after detailed analysis, a strong factual showing, measured judgment by high-level executive branch officials, and approval by a neutral judge.

Although the FISA process was designed for surveillance directed at people located in the United States, the government later sought and obtained approval from the FISA court to use this process to target foreign persons located outside the United States as well. Developments in communications technology and the Internet services industry meant that such surveillance could feasibly be conducted from within the United States in some instances. 464 Utilizing the process of traditional FISA to target significant numbers of individuals overseas, however, required considerable time and resources, and government officials have argued that it slowed and sometimes prevented the acquisition of important intelligence. 465

461 These steps also must be repeated each time the government wishes to continue the surveillance beyond the time limit specified in the original order. See 50 U.S.C. § 1805(d).
462 FISA permits surveillance to begin prior to court approval in emergency situations, but in order to exercise this option the Attorney General must make a determination that an emergency exists and that the factual basis required for the surveillance exists, and an application must be submitted to the FISA court for the normal probable cause determination within seven days. See 50 U.S.C. § 1805(e).
463 Moreover, when the target of surveillance is a U.S. person, that person must be “knowingly” acting on behalf of a foreign power. See 50 U.S.C. § 1801(b)(1), (2). An exception to the requirement that the target be acting on behalf of a foreign power permits a so-called “lone wolf” with no apparent connection to a foreign power to be targeted, if there is probable cause that the person is engaged in international terrorism or proliferation of weapons of mass destruction. See 50 U.S.C. §§ 1801(b)(1)(C), (D), 1805(a)(2)(A).
464 See pages 16-18 of this Report.
465 See pages 18-19 of this Report.
Section 702 imposes significantly fewer limits on the government when it targets non-U.S. persons located abroad, permitting greater flexibility and a dramatic increase in the number of people who can realistically be targeted.\textsuperscript{466} Rather than approving or denying individual targeting requests, the FISA court authorizes the surveillance program as a whole, approving the certification in which the government identifies the types of foreign intelligence information sought and the procedures the government uses to target people and handle the information it obtains.\textsuperscript{467} Targets of surveillance need not be agents of foreign powers; instead, the government may target any non-U.S. person overseas whom it reasonably believes has or is likely to communicate designated types of foreign intelligence.\textsuperscript{468} The government need not have probable cause for this belief, or for its belief that the target uses the particular selector, such as a telephone number or email address, to be monitored. There is no requirement that the information sought cannot be acquired through normal investigative techniques. Targeting decisions are made by NSA analysts and reviewed only within the executive branch.\textsuperscript{469} Once monitoring of a particular person begins, it may continue until new information indicates that the person no longer is an appropriate target. Whether a person remains a valid target must be reviewed annually.\textsuperscript{470}

These differences allow the government to target a much wider range of foreigners than was possible under traditional FISA. For instance, people who might have knowledge about a suspected terrorist can be targeted even if those people are not themselves involved in terrorism or any illegitimate activity.

In addition to expanding the pool of potential surveillance targets, Section 702 also enables a much greater degree of flexibility, allowing the government to quickly begin monitoring new targets and communications facilities without the delay occasioned by the requirement to secure approval from the FISA court for each targeting decision.

As a result of these two factors, the number of people who can feasibly be targeted is significantly greater under Section 702 than under the traditional FISA process. And

\textsuperscript{466} Under FISA and the FISA Amendments Act, the term “United States person” includes U.S. citizens, legal permanent residents, unincorporated associations with a substantial number of U.S. citizens or legal permanent residents as members, and corporations incorporated in the United States. It does not include associations or corporations that qualify as a “foreign power.” See 50 U.S.C. § 1801(i).

\textsuperscript{467} 50 U.S.C. § 1881a(a), (i).

\textsuperscript{468} NSA DCLPO REPORT, supra, at 4-5.

\textsuperscript{469} NSA DCLPO REPORT, supra, at 4-5.

\textsuperscript{470} Analysts are required to review the communications acquired from a target at least annually, to ensure that the targeting is still expected to provide the foreign intelligence sought and that the person otherwise remains an appropriate target under Section 702. See NSA DCLPO REPORT, supra, at 6.
indeed, the number of targets under the program has been steadily increasing since the statute was enacted in 2008.

The government also conducts foreign intelligence surveillance outside of the United States against non-U.S. persons under the authority of Executive Order 12333. In some instances, this surveillance can capture the same communications that the government obtains within the United States through Section 702. And because this collection takes place outside the United States, it is not restricted by the detailed rules of FISA outlined above. Nevertheless, Section 702 offers advantages over Executive Order 12333 with respect to electronic surveillance. The fact that Section 702 collection occurs in the United States, with the compelled assistance of electronic communications service providers, contributes to the safety and security of the collection, enabling the government to protect its methods and technology. In addition, acquiring communications with the compelled assistance of U.S. companies allows service providers and the government to manage the manner in which the collection occurs. By helping to prevent incidents of overcollection and swiftly remedy problems that do occur, this arrangement can benefit the privacy of people whose communications are at risk of being acquired mistakenly.

B. Contributions to Counterterrorism

The Section 702 program has proven valuable in a number of ways to the government’s efforts to combat terrorism. It has helped the United States learn more about the membership, leadership structure, priorities, tactics, and plans of international terrorist organizations. It has enabled the discovery of previously unknown terrorist operatives as well as the locations and movements of suspects already known to the government. It has led to the discovery of previously unknown terrorist plots directed against the United States and foreign countries, enabling the disruption of those plots.

While the Section 702 program is indeed a program, operating to some degree as a cohesive whole and approved by the FISA court accordingly, its implementation consists entirely of targeting specific individuals about whom the government already knows something. Because surveillance is conducted on an individualized basis where there is reason to target a particular person, it is perhaps unsurprising that the program yields a great deal of useful information.

The value of the Section 702 program is to some extent reflected in the breadth of NSA intelligence reporting based on information derived from the program. Since 2008, the number of signals intelligence reports based in whole or in part on Section 702 has

---

471 FISA does not generally cover surveillance conducted outside the United States, except where the surveillance intentionally targets a particular, known U.S. person, or where it acquires radio communications in which the sender and all intended recipients are located in the United States and the acquisition would require a warrant for law enforcement purposes. See 50 U.S.C. §§ 1801(f), 1881c.
increased exponentially. A significant portion of those reports relate to counterterrorism, and the NSA disseminates hundreds of reports per month concerning terrorism that include information derived from Section 702. Presently, over a quarter of the NSA’s reports concerning international terrorism include information based in whole or in part on Section 702 collection, and this percentage has increased every year since the statute was enacted. These reports are used by the recipient agencies and departments for a variety of purposes, including to inform senior leaders in government and for operational planning.

More concretely, information acquired from Section 702 has helped the Intelligence Community to understand the structure and hierarchy of international terrorist networks, as well as their intentions and tactics. In even the most well-known terrorist organizations, only a small number of individuals have a public presence. Terrorist groups use a number of practices to obscure their membership and activities. Section 702 has enabled the U.S. government to monitor these terrorist networks in order to learn how they operate and to understand how their priorities, strategies, and tactics continue to evolve.

Monitoring these networks under Section 702 has led the government to identify previously unknown individuals who are involved in international terrorism. Identifying such persons allows the government to pursue new efforts focusing on those individuals and the disruption of their activities, such as taking action to prevent them from entering the United States. Finally, the flexibility of Section 702 surveillance enables the government to effectively maintain coverage on particular individuals as they add or switch their modes of communications.

As important as discovering the identities of individuals engaged in international terrorism is determining where those individuals are located. Modern communications permit the members of a terrorist group, and even a small number of people involved in a specific plot, to be spread out all over the world. Information acquired from Section 702 has been used to monitor individuals believed to be engaged in terrorism.

In one case, for example, the NSA was conducting surveillance under Section 702 of an email address used by an extremist based in Yemen. Through that surveillance, the agency discovered a connection between that extremist and an unknown person in Kansas City, Missouri. The NSA passed this information to the FBI, which identified the unknown person, Khalid Ouazzani, and subsequently discovered that he had connections to U.S.-based Al Qaeda associates, who had previously been part of an abandoned early stage plot to bomb the New York Stock Exchange. All of these individuals eventually pled guilty to providing and attempting to provide material support to Al Qaeda.

Finally, pursuit of the foregoing information under Section 702 has led to the discovery of previously unknown terrorist plots and has enabled the government to
disrupt them. By providing the sites of specific targets of attacks, the means being contemplated to carry out the attacks, and the identities and locations of the participants, the Section 702 program has directly enabled the thwarting of specific terrorist attacks, aimed at the United States and at other countries.

For instance, in September 2009, the NSA monitored under Section 702 the email address of an Al Qaeda courier based in Pakistan. Through that collection, the agency intercepted emails sent to that address from an unknown individual located in the United States. Despite using language designed to mask their true intent, the messages indicated that the sender was urgently seeking advice on the correct mixture of ingredients to use for making explosives. The NSA passed this information to the FBI, which used a national security letter to identify the unknown individual as Najibullah Zazi, located near Denver, Colorado. The FBI then began intense monitoring of Zazi, including physical surveillance and obtaining legal authority to monitor his Internet activity. The Bureau was able to track Zazi as he left Colorado a few days later to drive to New York City, where he and a group of confederates were planning to detonate explosives on subway lines in Manhattan within the week. Once Zazi became aware that law enforcement was tracking him, he returned to Colorado, where he was arrested soon after. Further investigative work identified Zazi’s co-conspirators and located bomb-making components related to the planned attack. Zazi and one of his confederates later pled guilty and cooperated with the government, while another confederate was convicted and sentenced to life imprisonment. Without the initial tip-off about Zazi and his plans, which came about by monitoring an overseas foreigner under Section 702, the subway-bombing plot might have succeeded.

In cases like the Zazi and Ouazzani investigations, one might ask whether the government could have monitored the communications of the overseas extremists without Section 702, using the traditional FISA process. In some instances, that might be the case. But the process of obtaining court approval for the surveillance under the standards of traditional FISA may, for the reasons explained above, limit the number of people the government can feasibly target and increase the delay before surveillance on a target begins, such that significant communications could be missed.

The Board has received information about other instances in which the Section 702 program has played a role in counterterrorism efforts. Most of these instances are included in a compilation of 54 “success stories” involving the Section 215 and 702 programs that was prepared by the Intelligence Community last year in the wake of Edward Snowden’s unauthorized disclosures. Other examples have been shared with the Board more recently. Information about these cases has not been declassified, but some general information about them can be shared. In approximately twenty cases that we have reviewed, surveillance conducted under Section 702 was used in support of an already existing counterterrorism investigation, while in approximately thirty cases, Section 702
information was the initial catalyst that identified previously unknown terrorist operatives and/or plots. In the vast majority of these cases, efforts undertaken with the support of Section 702 appear to have begun with narrowly focused surveillance of a specific individual whom the government had a reasonable basis to believe was involved with terrorist activities, leading to the discovery of a specific plot, after which a short, intensive period of further investigation ensued, leading to the identification of confederates and arrests of the plotters. A rough count of these cases identifies well over one hundred arrests on terrorism-related offenses. In other cases that did not lead to disruption of a plot or apprehension of conspirators, Section 702 appears to have been used to provide warnings about a continuing threat or to assist in investigations that remain ongoing. Approximately fifteen of the cases we reviewed involved some connection to the United States, such as the site of a planned attack or the location of operatives, while approximately forty cases exclusively involved operatives and plots in foreign countries.\(^{472}\)

### C. Contributions to Other Foreign Intelligence Efforts

As noted above, the oversight mandate of our Board extends only to those measures taken by the government to protect the nation from terrorism. Some governmental activities, including the Section 702 program, are not aimed exclusively at preventing terrorism but also serve other foreign intelligence and foreign policy goals. The Section 702 program, for instance, is also used for surveillance aimed at countering the efforts of proliferators of weapons of mass destruction.\(^ {473}\) Given that these other foreign intelligence purposes of the program are not strictly within the Board’s mandate, we have not scrutinized the effectiveness of Section 702 in contributing to those other purposes with the same rigor that we have applied in assessing the program’s contribution to counterterrorism. Nevertheless, we have come to learn how the program is used for these other purposes, including, for example, specific ways in which it has been used to combat weapons proliferation and the degree to which the program supports the government’s efforts to gather foreign intelligence for the benefit of policymakers. Our assessment is that the program is highly valuable for these other purposes, in addition to its usefulness in supporting efforts to prevent terrorism.

---

\(^{472}\) The examples described in this paragraph do not represent an exhaustive list of all instances in which the Section 702 program has proven useful, even in counterterrorism efforts.

\(^{473}\) See S. Rep. No. 112-229, at 32 (2012) (appendix reproducing Background Paper on Title VII of FISA Prepared by the Department of Justice and the Office of the Director or National Intelligence) (“Section 702 . . . lets us collect information about the intentions and capabilities of weapons proliferators and other foreign adversaries who threaten the United States.”).
III. Privacy and Civil Liberties Implications of the Section 702 Program

A. Nature of the Collection under Section 702

1. Programmatic Surveillance

Unlike the telephone records program conducted by the NSA under Section 215 of the USA PATRIOT Act, the Section 702 program is not based on the indiscriminate collection of information in bulk. Instead, the program consists entirely of targeting specific persons about whom an individualized determination has been made. Once the government concludes that a specific non-U.S. person located outside the United States is likely to communicate certain types of foreign intelligence information — and that this person uses a particular communications “selector,” such as an email address or telephone number — the government acquires only those communications involving that particular selector.474

Every individual decision to target a particular person and acquire the communications associated with that person must be documented and approved by senior analysts within the NSA before targeting. Each targeting decision is later reviewed by an oversight team from the DOJ and the ODNI (“the DOJ/ODNI oversight team”) in an effort to ensure that the person targeted is reasonably believed to be a non-U.S. person located abroad, and that the targeting has a legitimate foreign intelligence purpose. The FISA court does not approve individual targeting decisions or review them after they are made.

Although the “persons” who may be targeted under Section 702 include corporations, associations, and entities as well as individuals,475 the government is not exploiting any legal ambiguity by “targeting” an entity like a major international terrorist organization and then engaging in indiscriminate or bulk collection of communications in order to later identify a smaller subset of communications that pertain to the targeted entity. To put it another way, the government is not collecting wide swaths of communications and then combing through them for those that are relevant to terrorism or contain other foreign intelligence. Rather, the government first identifies a communications identifier, like an email address, that it reasonably believes is used by the target, whether that target is an individual or an entity. It then acquires only those communications that are related to this identifier.476 In other words, selectors are always

474 See pages 20-23 and 32-33 of this Report.
475 See 50 U.S.C. §§ 1801(m), 1881a(a).
476 The NSA’s “upstream collection” (described elsewhere in this Report) may require access to a larger body of international communications than those that contain a tasked selector. Nevertheless, the government has no ability to examine or otherwise make use of this larger body of communications, except to promptly determine whether any of them contain a tasked selector. Only those communications (or more precisely, “transactions”) that contain a tasked selector go into government databases. See pages 36-41 of this Report.
unique communications identifiers used by the targeted persons. So under the Section 702 program, the government cannot, for instance, acquire communications because they are associated with a particular region where the government believes it is likely to find information related to one of its targets. Collection is instead limited to the communications identifiers of the targets themselves.

Likewise, although the selectors that the government could use are not limited to telephone numbers and email addresses, the government is not creatively interpreting the meaning of “selectors” to engage in bulk collection under Section 702. Even in the complex realm of Internet communications, a selector always must be associated with a specific person or entity. Thus, acquisition is always based on selecting communications that are associated with the target.477

2. Contents of Private Telephone and Internet Communications

Under Section 702, the government acquires the contents of international communications — collecting Internet communications like emails and recording telephone calls — as well as the addressing information or “metadata” associated with those communications. The contents of such communications may be highly personal and sensitive. U.S. persons and people located in the United States may not be targeted under Section 702, but their communications nevertheless can be acquired, including when they are in contact with a foreigner located abroad who has been targeted. Thus, the chance of government intrusion into private matters may be comparatively higher for individuals who maintain frequent contact with family members, friends, acquaintances, or professional contacts outside of the United States.

After being acquired by the government, communications obtained through Section 702 are stored in databases for default periods of time.478 There, they are subject to being examined by NSA, CIA, and FBI analysts or agents in pursuit of foreign intelligence or evidence of a crime. Subject to the separate minimization procedures at each agency, communications can be identified and retrieved from these databases for examination based on their addressing information (such as the telephone numbers or email addresses involved), while Internet communications are also retrievable by scanning their contents for the presence of certain words or terms.

3. Scope of Targeting and Collection

While the Section 702 program is based entirely on individual targeting decisions, it nevertheless results in an extremely large amount of collection. In part, this is because

477 This is true even in the unique contexts of so-called “about” collection and “MCT” collection, both of which are discussed below.

478 See page 60 of this Report.
modern technology, especially the ability to store huge amounts of data, makes it logistically feasible to target large numbers of people. The breadth of collection is also possible because, as explained above, the standards under which targeting is permitted under Section 702 are less rigorous than those governing other surveillance activities conducted within the United States. The government enjoys much more latitude when targeting foreigners located outside the United States under Section 702 than it does when targeting people located in the United States under other legal authorities, even for foreign intelligence purposes. The range of people whom the government may target and the permissible reasons for that targeting are much broader, while the level of suspicion required and the legal steps the government must take before initiating surveillance are much lower. In particular, the FISA court approves the government’s targeting and minimization procedures but plays no role in reviewing individual targeting decisions.479

As a result, the number of people targeted under Section 702 is considerable and collection has steadily grown. During the year 2013, 89,138 persons were targeted for collection under Section 702.

Thus, while the Board does not regard Section 702 as a “bulk” collection program, because it is based entirely on targeting the communications identifiers of specific people, neither does the program resemble traditional domestic surveillance conducted pursuant to individualized court orders based on probable cause. The FISA court instead determines whether to approve the surveillance program as a whole and plays a role in overseeing whether it stays within statutory and constitutional limits. The Section 702 program, in short, is perhaps best characterized by the term “programmatic surveillance.”480

B. Acquisition of the Communications of U.S. Persons under Section 702

While the scope of targeting under Section 702 is broad, that targeting cannot include U.S. persons or people located in the United States. As a result, this program does not allow the government to gain comprehensive access to any U.S. person’s communications: the government will not be able to hear every telephone call a U.S. person makes, for instance, or collect every email sent or received by that person. Instead, absent mistake or abuse, Section 702 enables the government to obtain only those communications that occur where a U.S. person is in contact with a targeted overseas foreigner, as well as those that are acquired in the unique circumstances of “about” and “MCT” collection (discussed below).

479 See pages 26-31 of this Report.
480 The Section 215 program, in contrast, represents both a bulk collection program and an example of programmatic surveillance.
Because it disallows comprehensive monitoring of any U.S. person, and prohibits deliberately acquiring even a single communication that is known to be solely among people located within the United States, the program would serve as a relatively poor vehicle to repress domestic dissent, monitor American political activists, or engage in other politically motivated abuses of the sort that came to light in the 1970s and prompted the enactment of FISA.

Nevertheless, as described below, under certain circumstances the program permits the government to collect a communication where one party is a U.S. person, including communications that are sensitive and private, and where the U.S. person may have taken steps to preserve the confidentiality of the communication. There are four main ways in which the Section 702 program, notwithstanding its focus on targeting foreigners located abroad, can lead to the acquisition of U.S. persons’ communications.

1. **Incidental Collection**

A person targeted for surveillance who speaks on the phone or communicates over the Internet is communicating with someone else. That other person’s communications with the target are said to have been “incidentally” acquired. In the context of the Section 702 program, the term “incidental collection” is used to refer to situations in which U.S. persons or people located in the United States have their communications acquired because they were in contact with a targeted foreigner located overseas. While the government cannot target U.S. persons or people located in the United States, it is permitted to acquire and in some cases retain and use communications in which a U.S. person is in contact with a target.

The term “incidental” is appropriate because such collection is not accidental or inadvertent, but rather is an anticipated collateral result of monitoring an overseas target. But the term should not be understood to suggest that such collection is infrequent or that it is an inconsequential part of the Section 702 program.

The number of communications collected under Section 702 to which one party is a U.S. person or located in the United States is not known. And one of the purposes of the program is to discover communications between a target overseas and a person in the United States. Executive and legislative branch officials have repeatedly emphasized to us that, with respect to terrorism, communications involving someone in the United States are

---

some of the “most important” communications acquired under the program.\textsuperscript{482} And indeed, where the program has directly led to the discovery and disruption of terrorist plots, it has sometimes done so by helping to discover previously unknown operatives in the United States through their communications with terrorism suspects located abroad.\textsuperscript{483}

From a privacy perspective, however, incidental collection under Section 702 differs in at least two significant ways from incidental collection that occurs in the course of a criminal wiretap or the traditional FISA process.

First, in the criminal or FISA context the targets of surveillance must be believed to be criminals or agents of a foreign power.\textsuperscript{484} That means that innocent U.S. persons need not worry about the government listening to their phone conversations or reading their emails except to the extent that they are communicating with suspected criminals or agents of foreign powers. The range of people whom the government may target under Section 702, on the other hand, is much broader. It is not limited to suspected terrorists or others engaged in nefarious activities. Instead, under an approved certification, the government may target any overseas foreigner who has or is likely to communicate certain kinds of foreign intelligence — who, for instance, may possess information “with respect to a foreign power or foreign territory that relates to . . . the conduct of the foreign affairs of the United States.”\textsuperscript{485} That person need not be acting at the behest of a foreign power or be engaged in any activities that are hostile toward the United States or would violate any laws. For instance, someone who has information about a terrorist operative may be targeted under Section 702, even if that person has no involvement in terrorism.

Second, to engage in traditional FISA or criminal electronic surveillance, the government must obtain approval from a judge, who independently assesses the legitimacy of the targeting and must be persuaded that the government’s beliefs about the person

\textsuperscript{482} See Privacy and Civil Liberties Oversight Board, Transcript of Public Workshop regarding surveillance programs operated pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act, at 109 (July 9, 2013) (statement of Steven Bradbury, formerly DOJ Office of Legal Counsel) (stating that Section 702 “is particularly focused on communications in and out of the United States because . . . those are the most important communications you want to know about if you’re talking about a foreign terrorist suspect communicating to somebody you don’t know inside the United States”); see id. at 116 (statement of Kenneth Wainstein, formerly DOJ National Security Division/White House Homeland Security Advisor) (agreeing), available at http://www.pclob.gov/SiteAssets/9-july-2013/Public%20Workshop%20-%20-%20Full.pdf; see also FISA for the 21st Century: Hearing before the Senate Comm. on the Judiciary, 109th Cong. 9 (2006) (statement of General Michael V. Hayden, Director, CIA).

\textsuperscript{483} See pages 107-110 of this Report.


\textsuperscript{485} 50 U.S.C. § 1801(e)(2)(B). The range of foreign intelligence that the government may seek under Section 702 is limited by the certifications approved by the FISA court. See pages 24-31 of this Report for a description of the certification process.
and/or communications facility being targeted are supported by probable cause.\textsuperscript{486} By providing a neutral check on the government’s authority to conduct electronic surveillance, these protections help assure innocent U.S. persons that their conversations will not be incidentally acquired in the course of improper surveillance directed at another person.

These restrictions and checks are absent under Section 702. To be clear, such absence does not mean that the government has free rein: targeting rules, a system of intra- and inter-agency oversight, programmatic supervision by the FISA court, and a host of reporting requirements all work to ensure that the government’s decisions about whom to monitor stay within legal bounds. But the expansiveness of the governing rules, combined with the technological capacity to acquire and store great quantities of data, permit the government to target large numbers of people around the world and acquire a vast number of communications. By 2011, for instance, the government was annually acquiring over 250 million Internet communications, in addition to telephone conversations.\textsuperscript{487} The current number is significantly higher. Even if U.S. persons’ communications make up only a small percentage of this total, the absolute number of their communications acquired could be considerable.

Minimization requirements to some degree compensate for the possibility of broad incidental collection. Those rules are described in detail earlier in this Report,\textsuperscript{488} and their significance is discussed below. While the existence of minimization rules may temper the privacy impact of incidental collection, the scope of that collection may also bear on whether the minimization rules are adequate. The present lack of knowledge about the range of incidental collection under Section 702 therefore hampers attempts to gauge whether the program appropriately balances national security interests with the privacy of U.S. persons.

2. Inadvertent Collection

Sometimes the NSA acquires communications under Section 702 of U.S. persons or people located in the United States by mistake. This can occur when the NSA erroneously believes that a potential target is a foreigner or located outside the United States, and discovers the truth only after collection on that person begins. It can also occur as a result of human error, such as mistyping an email address in the targeting process. Additionally, mistakes can occur as a result of technological malfunctions. Finally, targets who were located outside the United States may travel into the country, making them no longer


\textsuperscript{488} See pages 50-66 of this Report.
eligible for targeting, before the NSA discovers this fact. While all of these possibilities create risks that the NSA will acquire communications that it is not authorized to collect, the Board has been impressed by the seriousness with which the government attempts to ensure that this does not occur.

In any surveillance program as large in scope as the Section 702 program, particularly where collection involves highly sophisticated technology, mistakes are inevitable. The Board believes that the Section 702 program is implemented in a manner that reasonably avoids such errors. Furthermore, experience has shown that where there have been more significant mistakes, the government discovers them and complies with the reporting requirements that demand prompt disclosure of compliance incidents to the FISA court and to the oversight committees in Congress.

There have been a few significant large-scale implementation problems in the Section 702 program, all revolving around technological matters. As described earlier, technical problems have in some instances led the government to acquire communications not authorized for collection under the program. More recently, the checks that are designed to provide indications that a target is located inside the United States were substantially non-functioning for over a year. In yet another incident, the NSA discovered that its systems for purging data were not operating completely, leading to the retention of information that should have been destroyed. In consultation with the FISA court, the government has resolved those issues appropriately and has worked to remedy the errors that were discovered.

Inadvertent collection can also occur on an individualized basis, such as where the NSA targets people whom it mistakenly believes are foreigners or located outside the United States. Commentators have questioned the rigor of the agency’s “foreignness” determinations, particularly whether they rely on certain default assumptions where information about a person is lacking. The notion also has arisen that the agency employs a “51% test” in assessing the location and nationality of a potential target — in other words, that analysts need only be slightly more than half confident that the person being targeted is a non-U.S. person located outside the United States.

These characterizations are not accurate. In keeping with representations the government has made to the FISA court, NSA analysts consult multiple sources of information in attempting to determine a proposed target’s foreignness, and they are obligated to exercise a standard of due diligence in that effort, making their determinations based on the totality of the circumstances. They also must document the information on

489 See page 79 of this Report.
which they based their assessments, which must be reviewed and approved by two senior analysts prior to targeting, and which are subject to further review later.\textsuperscript{490}

Available figures suggest that the percentage of instances in which the NSA accidentally targets a U.S. person or someone in the United States is tiny. In 2013, the DOJ reviewed one year of data to determine the percentage of cases in which the NSA’s targeting decisions resulted in the “tasking” of a communications identifier that was used by someone in the United States or was a U.S. person. The NSA’s error rate, according to this review, was 0.4 percent.\textsuperscript{491} Moreover, once a targeting decision has been made, that is not the end of the story. Soon after collection on a selector begins, analysts must review a sample of the communications that have recently been collected, to ensure that the email address or other selector actually is associated with the person whom the NSA intended to target, and that this person is a foreigner located outside the United States. Additional measures are employed to re-verify the validity of continued collection against the selector.\textsuperscript{492} In addition, the DOJ/ODNI oversight team reviews every targeting decision, including the documentation on which the “foreignness” determination was made. The oversight team conducts on-site reviews as part of this process, and when the documentation available is not sufficient to demonstrate the basis of a foreignness determination, the oversight team requests and obtains additional information.\textsuperscript{493} The NSA counts the number of instances in which it discovers that a selector is or may be being used by someone in the United States — either because the target traveled to the United States or because the original targeting decision was erroneous. The percentage of such instances is also very small, with the total annual number of instances representing less than 1.5 percent of the average number of selectors targeted at any given moment.

To date, the DOJ/ODNI oversight team has not discovered any instances in which an analyst intentionally violated the statute, targeting procedures, or minimization procedures. In the history of the program, the government has identified only two instances of “reverse targeting” — that is, the prohibited targeting of overseas foreigners for the purpose of acquiring the communications of persons in the United States with whom they are in contact.\textsuperscript{494}

\textsuperscript{490} NSA DCLPO REPORT, \textit{supra}, at 4-5.

\textsuperscript{491} See pages 71-72 of this Report.

\textsuperscript{492} See pages 48-49 of this Report; NSA DCLPO REPORT, \textit{supra}, at 6.

\textsuperscript{493} NSA DCLPO REPORT, \textit{supra}, at 10.

\textsuperscript{494} See page 79 of this Report. In one case, the targeting resulted in no collection of communications. In the other case, all of the collection was purged.
In sum, as noted above, the Board is impressed by the rigor with which the government attempts to ensure that the persons it targets under Section 702 truly are non-U.S. persons located outside the United States.\textsuperscript{495}

3. “About” Collection

One of the most controversial aspects of the Section 702 program is the practice of so-called “about” collection. This term describes the NSA’s acquisition of Internet communications that are neither to nor from an email address — but that instead merely include a reference to that selector.\textsuperscript{496} For instance, a communication between two third parties might be acquired because it contains a targeted email address in the body of the communication.\textsuperscript{497}

The fact that the NSA acquires certain communications based on what is contained within the body of the communication has apparently led some to believe that the government is scanning the contents of U.S. persons’ international communications to see if they are discussing particular subjects or using particular key words. Initial news articles describing “about” collection may have contributed to this perception, reporting that the NSA “is searching the contents of vast amounts of Americans’ email and text communications into and out of the country, hunting for people who mention information about foreigners under surveillance[.]”\textsuperscript{498} This belief represents a misunderstanding of a more complex reality. “About” collection takes place exclusively in the NSA’s acquisition of Internet communications through its upstream collection process. That is the process whereby the NSA acquires communications as they transit the Internet “backbone” within the United States. This process is distinguished from the NSA’s PRISM collection, in which U.S.-based Internet service providers transmit communications to the government

\begin{footnotesize}
\begin{itemize}
  \item \textsuperscript{495} See below for a discussion of what happens when the NSA discovers that it inadvertently acquired the communications of a U.S. person or someone in the United States.
  \item \textsuperscript{496} See PCLOB March 2014 Hearing Transcript, \textit{supra}, at 13 (statement of Rajesh De, General Counsel, NSA).
  \item \textsuperscript{497} See The Intelligence Community’s Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, at 4 (2012) (describing differences between targeting individuals under traditional FISA electronic surveillance provisions and targeting pursuant to Section 702). This document accompanied a 2012 letter sent by the Department of Justice and the Office of the Director of National Intelligence to the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence urging the reauthorization of Section 702. See Letter from Kathleen Turner, Director of Legislative Affairs, ODNI, and Ronald Weich, Assistant Attorney General, Office of Legislative Affairs, DOJ to the Hon. Dianne Feinstein, Chairman, Senate Committee on Intelligence, et. al. (May 4, 2012), \textit{available at} http://www.dni.gov/files/documents/Ltr%20to%20HPSCI%20Chairman%20Rogers%20and%20Ranking%20Member%20Ruppersberger_Scan.pdf.
  \item \textsuperscript{498} Charlie Savage, \textit{N.S.A. Said to Search Content of Messages to and From U.S.}, \textit{N.Y. TIMES} (Aug. 8, 2013).
\end{itemize}
\end{footnotesize}
directly.\(^{499}\) Whereas PRISM collection is a comparatively simple process, because the government obtains communications of a service provider’s customers directly from that provider, the upstream process is more complex, depending upon the use of collection devices with technological limitations that significantly affect the scope of collection.\(^{500}\) Because of the way that Internet communications are transmitted in the form of data packets, the NSA’s collection devices acquire what the agency and the FISA court have termed Internet “transactions.”\(^{501}\) As a result of this acquisition technique, the FISA court has explained, “the NSA’s upstream collection devices acquire any Internet transaction transiting the device if the transaction contains a targeted selector anywhere within it[].”\(^{502}\)

This means that an Internet communication between third parties, not involving the target, can be acquired by the NSA if it contains a reference, for instance, to the email address of a target.\(^{503}\) For this reason, “about” collection raises at least two serious concerns, one relatively simple, the other more complex.

First, “about” collection may be more likely than other forms of collection to acquire wholly domestic communications — something not authorized by Section 702. Because “about” communications are not to or from the email address that was tasked for acquisition,\(^{504}\) which is used by a person reasonably believed to be located outside the United States, there is no guarantee that any of the participants to the communication are located outside the United States. In part to compensate for this problem, the NSA takes additional measures with its upstream collection to ensure that no communications are acquired that are entirely between people located in the United States. These measures can include, for instance, employing Internet protocol filters to acquire only communications that appear to have at least one end outside the United States.\(^{505}\) In this process, Internet communications are first filtered to eliminate potential domestic communications, and then are screened to capture only communications containing a tasked selector.

\(^{499}\) The Intelligence Community’s Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, supra, at 3-4; NSA DCLPO REPORT, supra, at 5. See pages 33-34 of this Report.


\(^{504}\) As explained earlier, persons are targeted under Section 702 while the selectors used by those persons are tasked.

\(^{505}\) NSA DCLPO REPORT, supra, at 5-6.
While we believe that the measures taken by the NSA to exclude wholly domestic “about” communications may be reasonable in light of current technological limits, they are not perfect.\textsuperscript{506} Even where both parties to a communication are located in the United States, in a number of situations the communication might be routed internationally, in which case it could be acquired by the NSA’s upstream collection devices.\textsuperscript{507} There are reasons to suppose that this occurs rarely, but presently no one knows how many wholly domestic communications the NSA may be acquiring each year as a result of “about” collection.\textsuperscript{508}

The more fundamental concern raised by “about” collection is that it permits the government to acquire communications exclusively between people about whom the government had no prior suspicion, or even knowledge of their existence, based entirely on what is contained within the contents of their communications.\textsuperscript{509} This practice fundamentally differs from “incidental” collection, discussed above. While incidental collection also permits the government to acquire communications of people about whom it may have had no prior knowledge, that is an inevitable result of the fact that conversations generally involve at least two people: acquiring a target’s communications by definition involves acquiring his communications with other people. But no effort is made to acquire those other peoples’ communications — the government simply is acquiring the target’s communications. In “about” collection, by contrast, the NSA’s

\textsuperscript{506} December 2011 Joint Statement, \textit{supra}, at 7 (acknowledging that the NSA’s efforts “are not perfect”).


\textsuperscript{508} Although the NSA conducted a study in 2011, at the behest of the FISA court, to estimate how many wholly domestic communications it was annually acquiring as a result of collecting “MCTs” (discussed below), the study did not focus on how many domestic communications the NSA may be acquiring due to “about” collection where the communication acquired was not an MCT but rather a single, discrete communication. Bates October 2011 Opinion, \textit{supra}, at 34 n.32, 2011 WL 10945618, at *11, n.32. At the urging of the FISA court, the NSA subsequently spent some time examining this question, but ultimately did not provide an estimate, instead explaining to the court the logistical reasons that the chance of acquiring domestic communications in “about” collection “should be smaller — and certainly no greater — than potentially encountering wholly domestic communications within MCTs.” \textit{Id.} This statement prompted the FISA court to adopt the assumption that the percentage of wholly domestic communications within the agency’s “about” collection might equal the percentage of wholly domestic communications within its collection of “MCTs,” leading to an estimate of as many as 46,000 wholly domestic “about” communications acquired each year. \textit{Id.} We do not view this as a particularly valid estimate, because there is no reason to suppose that the number of wholly domestic “about” communications matches the number of wholly domestic MCTs, but the fact remains that the NSA cannot say how many domestic “about” communications it may be obtaining each year.

\textsuperscript{509} \textit{See December 2011 Joint Statement, \textit{supra}, at 7 (“[U]pstream collection allows NSA to acquire, among other things, communications about a target where the target is not itself a communicant.”); The Intelligence Community’s Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, \textit{supra}, at 4 (“Upstream collection . . . lets NSA collect electronic communications that contain the targeted e-mail address in the body of a communication between two third parties.”).
collection devices can acquire communications to which the target is not a participant, based at times on their contents.\textsuperscript{510}

Nothing comparable is permitted as a legal matter or possible as a practical matter with respect to analogous but more traditional forms of communication. From a legal standpoint, under the Fourth Amendment the government may not, without a warrant, open and read letters sent through the mail in order to acquire those that contain particular information.\textsuperscript{511} Likewise, the government cannot listen to telephone conversations, without probable cause about one of the callers or about the telephone, in order to keep recordings of those conversations that contain particular content.\textsuperscript{512} And without the ability to engage in inspection of this sort, nothing akin to “about” collection could feasibly occur with respect to such traditional forms of communication. Digital communications like email, however, enable one, as a technological matter, to examine the contents of all transmissions passing through collection devices and acquire those, for instance, that contain a tasked selector anywhere within them.

The government values “about” communications for the unique intelligence benefits that they can provide. Although we cannot discuss the details in an unclassified public report, the moniker “about” collection describes a number of distinct scenarios, which the government has in the past characterized as different “categories” of “about” collection. These categories are not predetermined limits that confine what the government acquires; rather, they are merely ways of describing the different forms of communications that are neither to nor from a tasked selector but nevertheless are collected because they contain the selector somewhere within them.\textsuperscript{513} In some instances, the targeted person actually is a participant to the communication (using a different communications selector than the one that was “tasked” for collection), and so the term “about” collection may be misleading.\textsuperscript{514} In other instances, a communication may not involve the targeted person, but for various logistical and technological reasons it will almost never involve a person located in the United States.


\textsuperscript{513} Such communications include “any Internet transaction that references a targeted selector, regardless of whether the transaction falls within one of the . . . previously identified categories of ‘about communications[.]’” Bates October 2011 Opinion, \textit{supra}, at 31, 2011 WL 10945618, at *11.

\textsuperscript{514} The term “about” communications was originally devised to describe communications that were “about” the selectors of targeted persons — meaning communications that contained such a selector within the communication. But the term has been used more loosely by officials in a way that suggests these communications are “about” the targeted persons. References to targeted persons do not themselves lead to “about” collection; only references to the communications selectors of targeted persons lead to “about” collection.
Some forms of “about” collection, however, do potentially intrude on the privacy of U.S. persons and people in the United States, as when, for instance, a U.S. person sends or receives an international communication to or from a non-target that contains a tasked email address in the body of the communication. Because selectors that are designated for collection under Section 702 need not be affiliated with any nefarious activity themselves, as explained earlier, a U.S. person’s use of a tasked selector in a communication does not necessarily indicate that the person is assisting a foreign power or engaged in any wrongdoing. Furthermore, that person’s communication will have been acquired because the government’s collection devices examined the contents of the communication, without the government having held any prior suspicion regarding that communication.

As noted above, however, all upstream collection — of which “about” collection is a subset — is “selector-based, i.e., based on . . . things like phone numbers or emails.”515 Just as in PRISM collection, a selector used as a basis for upstream collection “is not a ‘keyword’ or particular term (e.g., ‘nuclear’ or ‘bomb’) but must be a specific communications identifier (e.g., email address).”516 In other words, the government’s collection devices are not searching for references to particular topics or ideas, but only for references to specific communications selectors used by people who have been targeted under Section 702.

Moreover, the NSA’s acquisition of “about” communications is, to a large degree, an inevitable byproduct of its efforts to comprehensively acquire communications that are to or from its targets. Because of the specific manner in which the NSA conducts upstream collection, and the limits of its current technology, the NSA cannot completely eliminate “about” communications from its collection without also eliminating a significant portion of the “to/from” communications it seeks. Only to a limited degree could the agency feasibly turn off its “about” collection without incurring this result, and the outcome would not only represent an incomplete solution but would also undermine confidence that communications to and from targets are being reliably acquired. Additionally, there is no way at present for the NSA to selectively choose among the different categories of “about” communications at the collection stage. Nor does the NSA currently have any means available to automatically segregate “about” communications from “to/from” communications after collection, or to segregate among different forms of “about” communications after collection. Thus, ending all “about” collection would require ending even those forms of “about” collection that the Board regards as appropriate and valuable, and that have very little chance of impacting the privacy of people in the United States.

515 PCLOB March 2014 Hearing Transcript, supra, at 26 (statement of Rajesh De, General Counsel, NSA); see id. ("This is not collection based on key words, for example."); id. at 57 ("Abouts is a type of collection of information . . . . [A]ll collection of information is . . . focused on selectors, not key words . . . like terrorist, or like a generic name or things along those lines. . . . And it’s the same selectors that are used for the PRISM program that are also used for upstream collection. It’s just a different way to effectuate the collection.").

516 NSA DCLPO REPORT, supra, at 4.
For now, therefore, “about” collection is an inextricable part of the NSA’s upstream collection, which we agree has unique value overall that militates against eliminating it entirely. As a result, any policy debate about whether “about” collection should be eliminated in whole or in part may be, to some degree, a fruitless exercise under present conditions. From our perspective, given a choice between the status quo and crippling upstream collection as a whole, we believe the status quo is reasonable. As explained later, however, because of the serious and novel questions raised by “about” collection as a constitutional and policy matter, we recommend that the NSA develop technology that would allow it to selectively limit or segregate certain forms of “about” communications — so that a debate can be had in which the national security benefits of the different forms of “about” collection are weighed against their respective privacy implications.

We emphasize, however, that our acceptance of “about” collection rests on the considerations described above — the inextricability of the practice from a broader form of collection that has unique value, and the limited nature of what “about” collection presently consists of: the acquisition of Internet communications that include the communications identifier of a targeted person. Although those identifiers may sometimes be found in the body of a communication, the government is not making any effort to obtain communications based on the ideas expressed therein. We are not condoning expanding “about” collection to encompass names or key words, nor to its use in PRISM collection, where it is not similarly inevitable. Finally, our unwillingness to call for the end of “about” collection is also influenced by the constraints that presently govern the use of such communications after acquisition. As with all upstream collection, “about” communications have a default retention period of two years instead of five, are not routed to the CIA or FBI, and may not be queried using U.S. person identifiers.

4. Multi-Communication Transactions (“MCTs”)

The technical means used to conduct the NSA’s upstream collection result in another issue with privacy implications. Because of the manner in which the agency intercepts communications directly from the Internet “backbone,” the NSA sometimes acquires communications that are not themselves authorized for collection (because they are not to, from, or “about” a tasked selector) in the process of acquiring a communication that is authorized for collection (because it is to, from, or “about” a tasked selector). In 2011, the FISA court held that the NSA’s procedures for addressing this problem were inadequate, and that without adequate procedures this aspect of the NSA’s collection practices violated the Fourth Amendment. The government subsequently altered its procedures to the satisfaction of the FISA court. Based on the Board’s assessment of how those procedures are being implemented today, the Board agrees that existing practices strike a reasonable balance between national security and privacy.
Unlike in PRISM collection, where the government receives communications from the Internet service providers who facilitate them, in upstream collection the NSA obtains what it calls “transactions” that are sent across the backbone of the Internet. Communications travel across the Internet in the form of data packets: a single email, for instance, can be broken up into a number of data packets that take different routes to their common destination, where they are reassembled to reconstruct the email. A complement of data packets, in NSA parlance, is a "transaction." 517 These transactions will sometimes contain only a single, discrete communication, like a single email. At times, however, these transactions will contain a number of different individual communications. The NSA refers to the latter as an MCT.

An MCT is acquired by the NSA only if at least one individual communication within it meets the criteria for collection. That is, at least one of these individual communications must be to or from a tasked selector or contain reference to a tasked selector. But the MCT might also contain other individual communications that do not meet these criteria and that have no direct relationship to the tasked selector. 518 The NSA’s collection devices are unable to distinguish, before the point of acquisition, whether or not a transaction is an MCT. Thus, in the process of intercepting a communication that is “to/from” or “about” a tasked selector, the NSA might simultaneously obtain communications that are neither, because they are embedded within an MCT that contains a different communication meeting the standards for collection. 519 These other communications might be to or from U.S. persons or people located in the United States. They also might be domestic communications, exclusively between people located in the United States.

When the FISA court first began approving the Section 702 program in 2008, it did not understand that the NSA’s upstream process acquired “transactions” or that the agency was acquiring MCTs that included communications, including wholly domestic communications, that were not themselves authorized for collection. Only in 2011, after the government submitted a clarifying letter to the FISA court, did these aspects of upstream collection become clear to the court. 520 After extensive briefing, a hearing, and the

517 “The government describes an Internet ‘transaction’ as ‘a complement of “packets” traversing the Internet that together may be understood by a device on the Internet and, where applicable, rendered in an intelligible form to the user of that device.’” Bates October 2011 Opinion, supra, at 28 n.23, 2011 WL 10945618, at *9 n.23.


519 “About” collection and “MCT” collection are separate but overlapping categories. An MCT can be acquired if one of the communications within it is “about” a tasked selector (i.e., contains reference to a tasked selector), but an MCT also can be acquired if one of the communications within it is to or from a tasked selector. Thus, while “about” collection and “MCT” collection are both unique results of the upstream collection process, there is no inherent relationship between the two.

implementation of a study to estimate how many purely domestic communications were
being acquired, the FISA court concluded that the NSA’s practices were inconsistent
with the Fourth Amendment and with the statutory requirement to minimize the retention of
information about U.S. persons consistent with foreign intelligence needs. The FISA court
accepted that the continued acquisition of MCTs was legitimate, but that the procedures in
place to handle them after collection did not adequately protect the privacy interests of
U.S. persons whose communications were acquired solely because they were contained
within an MCT that also included a communication involving a tasked selector.

The government later resolved this issue to the FISA court’s satisfaction by
implementing new procedures for handling MCTs. Most notably, the NSA implemented
procedures to segregate and restrict access to certain MCTs after collection, and
established that any MCT found to contain a wholly domestic communication must be
destroyed upon recognition. It also shortened the default retention period for
communications acquired through upstream collection to two years.521 These rules are
now embodied in the NSA’s minimization procedures. To address concerns about collection
that occurred before these new procedures were implemented, the NSA later decided to
purge all data in its repositories that it could identify as having been acquired through
upstream before the date of these new procedures.522

The Board has inquired into how the NSA’s new procedures for handling MCTs are
being implemented, and it has learned — at a level of operational detail greater than what
is reflected in the agency’s minimization procedures — about the precise manner in which
the segregation of MCTs occurs and the steps through which any use of a communication
found in an MCT is permitted to occur. Based on this information, the Board believes that
current practices adequately guard against the government’s use of wholly domestic
communications as well as other communications of U.S. persons that are not to, from, or
about a tasked selector. Given the present impossibility of identifying, before collection,
those MCTs that contain domestic communications or other U.S. persons’ communications
that are not themselves authorized for acquisition, we believe that the existing procedures
strike a reasonable balance between national security and privacy. But we echo the FISA
court’s observation that it is incumbent upon the NSA to continue working to enhance its
capability to limit its acquisitions to only targeted communications.523

521 See Memorandum Opinion at 7-11, [Caption Redacted], [Docket No. Redacted], 2011 WL 10947772, at
declassifies-intelligence-community-documents.

522 See Memorandum Opinion at 30, [Caption Redacted], [Docket No. Redacted], 2012 WL 9189263, at *3

523 See Bates October 2011 Opinion, supra, at 58 n.54, 2011 WL 10945618, at *20 n.54.

126
C. Retention, Use, and Dissemination of U.S. Persons’ Communications under Section 702

Examining the privacy implications of the Section 702 program cannot end with a discussion of what is collected, but also must consider how information about U.S. persons is treated after collection: how long it is kept, who has access to it, in what ways it may be analyzed, under what circumstances it may be disseminated, and what procedures and oversight mechanisms are in place to ensure compliance with applicable rules.\footnote{524}{Everything that is collected under Section 702 is treated as a “communication” and therefore is protected by the applicable minimization procedures.}

Once communications are acquired under Section 702, they go into one or more databases at the NSA, CIA, and FBI.\footnote{525}{The CIA and FBI each receive only a select portion of the communications acquired under Section 702, and they receive only Internet communications acquired through PRISM collection, not telephone calls or Internet communications acquired through upstream collection. The National Counterterrorism Center (“NCTC”) is not authorized to receive any unminimized Section 702 data, but instead has access to certain FBI systems containing minimized Section 702 data. The CIA holds all unminimized communications acquired through Section 702 in a standalone network that is separate from the CIA’s other information processing systems.}

At each agency, access to this Section 702 data is limited to those analysts or agents who have received training and guidance. In reviewing information contained in these databases, government personnel may come across communications involving U.S. persons. Data is frequently reviewed through queries, which identify communications that have particular characteristics specified in the query, such as containing a particular name or having been sent to or from a particular email address.\footnote{526}{Because “about” and “MCT” collection occur only in upstream collection, which NSA alone receives, FBI and CIA personnel have no access to such communications.}

Beginning first with inadvertent collection, if it is discovered that a Section 702 target is a U.S. person or was inside the United States at the time of targeting, the government must stop the collection immediately and generally must destroy any communications already acquired.\footnote{527}{See, e.g., Minimization Procedures used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, § 3(d)(2), 5 (Oct. 31, 2011) (“NSA 2011 Minimization Procedures”), available at http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20Sect%20702.pdf. If the government learns that a target who previously was outside the United States has traveled into the United States, it also must stop collection immediately, and it must generally destroy those communications that were acquired after the target entered the United States, subject to the possibility of a waiver discussed above. Id. § 3(d).}

Beginning first with inadvertent collection, if it is discovered that a Section 702 target is a U.S. person or was inside the United States at the time of targeting, the government must stop the collection immediately and generally must destroy any communications already acquired.\footnote{527}{See, e.g., Minimization Procedures used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, § 3(d)(2), 5 (Oct. 31, 2011) (“NSA 2011 Minimization Procedures”), available at http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20Sect%20702.pdf. If the government learns that a target who previously was outside the United States has traveled into the United States, it also must stop collection immediately, and it must generally destroy those communications that were acquired after the target entered the United States, subject to the possibility of a waiver discussed above. Id. § 3(d).}
communication basis, by determining in writing that the communication satisfies one of several criteria. The destruction requirement may be waived if the communication is reasonably believed to contain “significant foreign intelligence information,” evidence of a crime, “technical data base information,” or “information necessary to understand or assess a communications security vulnerability.” Communications that indicate “a threat of serious harm to life or property” may also be preserved from destruction.\textsuperscript{528} The FBI standards are similar, as are the CIA standards, except that CIA waivers are limited to communications containing significant foreign intelligence or evidence of a crime.

Although approval for these waivers must come from the highest levels of the agencies, the breadth of the circumstances in which they can be approved raises concern that the waiver provisions might permit excessive use of communications that the agencies never should have acquired. Allowing the government to exploit the fruits of mistaken targeting decisions may risk creating an incentive for lax adherence to targeting restrictions. Presently, however, it appears that the government has been invoking these waiver provisions in a restrained manner. In 2013, for instance, the NSA Director waived the destruction of approximately forty communications (none of which was a wholly domestic communication), involving eight targets, based on a finding that each communication contained significant foreign intelligence information. Neither the CIA nor FBI utilized their waiver provisions in 2013. Along with the rigor that we believe is applied to the government’s determinations of foreignness during targeting, this sparing use of waivers helps to allay concern about their abuse. Furthermore, when an erroneous targeting was the result of a compliance incident, such as mistyping an email address, as opposed to a reasonable but mistaken belief about a target’s status, the waiver provision is unavailable.

Apart from communications acquired inadvertently, U.S. persons’ communications are not typically purged or eliminated from the government’s Section 702 databases before the end of their default retention periods, even when the communications pertain to matters unrelated to foreign intelligence or crime. This is because the agencies do not scrutinize each communication that they acquire or attempt to identify those that are to or from a U.S. person or person in the United States. The NSA’s minimization procedures, for instance, require the destruction of irrelevant communications of or concerning U.S. persons, but analysts are required to make such determinations only “at the earliest practicable point in the processing cycle,” and only where the communication can be identified as “clearly” not relevant to the purpose under which it was acquired or containing evidence of a crime.\textsuperscript{529} In practice, however, this destruction rarely happens. NSA analysts do not review all or even most communications acquired under Section 702

\textsuperscript{528} NSA 2011 Minimization Procedures, \textit{supra}, § 5.

\textsuperscript{529} NSA 2011 Minimization Procedures, \textit{supra}, § 3(b)(1).
as they arrive at the agency. Instead, those communications often remain in the agency’s databases unreviewed until they are retrieved in response to a database query, or until they are deleted upon expiration of their retention period, without ever having been reviewed. Even when an analyst focuses on a particular communication, the destruction requirement is triggered only when analysts can affirm a negative: that the communication in question does not contain foreign intelligence or evidence of a crime.\textsuperscript{530} But communications that appear innocuous at first may later take on deeper significance as more contextual information is learned, and it can be difficult for one analyst to be certain that a communication has no intelligence value to any other analyst. As a matter of course, therefore, there is no routine deletion from the NSA’s Section 702 databases of information that involves U.S. persons but is not pertinent to the agency’s foreign intelligence mission. Therefore, although a communication must be “destroyed upon recognition” when an NSA analyst recognizes that it involves a U.S. person and determines that it clearly is not relevant to foreign intelligence or evidence of a crime,\textsuperscript{531} in reality this rarely happens. Nor does such purging occur at the FBI or CIA: although their minimization procedures contain age-off requirements, those procedures do not require the purging of communications upon recognition that they involve U.S. persons but contain no foreign intelligence information.

Information that remains in the government’s Section 702 databases may be queried to find the communications of specific U.S. persons under certain circumstances.\textsuperscript{532} Queries are a key mechanism through which analysts access Section 702 information in the government’s databases.\textsuperscript{533} They may involve “telephone numbers, key words or phrases, or other discriminators” as selection terms.\textsuperscript{534} Queries can be used to search both the content of communications and the addressing information, or “metadata,” associated with the communications. At the NSA, content queries based on identifiers associated with specific U.S. persons — such as a name or email address — can be performed if they are “reasonably likely to return foreign intelligence information.”\textsuperscript{535} No showing or suspicion is required that the U.S. person is engaged in any form of wrongdoing. In recent months, NSA analysts have performed queries using U.S. person identifiers to find information

\textsuperscript{530} NSA 2011 Minimization Procedures, \textit{supra}, § 3(c). In addition, the communication must be “known” to contain information of or concerning U.S. persons. \textit{Id.}

\textsuperscript{531} NSA 2011 Minimization Procedures, \textit{supra}, § 3(b)(1), (c)(1).

\textsuperscript{532} The NSA and CIA first obtained approval to conduct queries using U.S. person identifiers in 2011. \textit{See Bates October 2011 Opinion, supra.}

\textsuperscript{533} \textit{See, e.g.}, NSA DCLPO REPORT, \textit{supra}, at 6 (“[Analysts] access the information via ‘queries,’ which may be date-bound, and include alphanumeric strings such as telephone numbers, email addresses, or terms that can be used individually or in combination with one another.”).

\textsuperscript{534} \textit{See, e.g.}, NSA 2011 Minimization Procedures, \textit{supra}, § 3(b)(6).

\textsuperscript{535} NSA 2011 Minimization Procedures, \textit{supra}, § 3(b)(6); \textit{see NSA DCLPO REPORT, supra, at 7.}
concerning, among other things, “individuals believed to be involved in international terrorism.” The CIA and FBI standards for content queries are essentially the same, except that the FBI, given its law enforcement role, is permitted to conduct queries to seek evidence of a crime as well as foreign intelligence information.

At the NSA, prior approval must be obtained to use content query terms that involve U.S. person identifiers. The agency records each term that is approved, though not the number of times any particular term is actually used to query a database. The NSA performs checks of its analysts’ queries. Prior approval is not required at the CIA; instead, the agency has developed audit capability. This system requires CIA personnel using U.S. person identifiers as query terms (or any other query term intended to return information about a particular U.S. person) write a contemporaneous foreign intelligence justification, which is documented along with a record of the query. Review of queries is also provided by the DOJ/ODNI oversight team, which reviews every U.S. person term approved for querying at the NSA as well as every U.S. person query performed at the CIA, reporting their numbers and any compliance issues to congressional oversight committees.

In 2013, the NSA approved the use of 198 terms involving U.S. person identifiers to perform content queries of its Section 702–acquired communications. During the same year, the CIA conducted approximately 1,900 queries of its unminimized Section 702–acquired communications, of which approximately forty percent were at the request of other U.S. intelligence agencies.\textsuperscript{536} Outside of those queries conducted on behalf of other intelligence agencies, CIA queries might involve, for instance, U.S. persons located overseas that intelligence indicates may be engaged in planning terrorist attacks or otherwise facilitating international terrorism.

While the FBI maintains records of content queries used to search its Section 702 data, it does not separately designate those that employ U.S. person identifiers, and so the number of U.S. person queries performed by the FBI is not known.

At the NSA, metadata queries, like content queries, must be reasonably designed to return foreign intelligence information when they involve U.S. person identifiers. Prior approval is not required, but the analyst must supply a written justification for the query, and all queries are recorded and subject to audit.\textsuperscript{537} The DOJ/ODNI oversight team reviews every NSA metadata query that involves a U.S. person identifier. In 2013, NSA analysts

\textsuperscript{536} Approximately 27 percent of these queries were duplicative of previous queries that employed the same query terms.

\textsuperscript{537} NSA DCLPO REPORT, supra, at 7.
performed approximately 9,500 queries of metadata acquired under Section 702 using U.S. person identifiers.\footnote{According to the DOJ/ODNI oversight team, the NSA’s counting of its own metadata queries typically is overinclusive, often counting queries that do not actually include a U.S. person identifier as well as other queries where it is unclear whether a U.S. person identifier is involved.}

The CIA also has the capability to conduct metadata-only queries against metadata derived from Section 702 collection. However, the CIA does not track how many metadata-only queries using U.S. person identifiers have been conducted. The CIA’s minimization procedures do not contain any specific standard with respect to metadata queries involving U.S. person identifiers, although such queries are regulated under internal CIA regulations that govern queries of FISA and non-FISA information, and FISA itself requires that information collected be used only be for lawful purposes.\footnote{See 50 U.S.C. §§ 1806(a).} The FBI requires that metadata queries, like content queries, be reasonably designed to return foreign intelligence or evidence of a crime. As noted above, however, the FBI does not separately track which of its queries involve U.S. person identifiers, and so the number of such metadata queries is not known.

As illustrated above, rules and oversight mechanisms are in place to prevent U.S. person queries from being abused for reasons other than searching for foreign intelligence or, in the FBI’s case, for evidence of a crime. In pursuit of the agencies’ legitimate missions, however, government analysts may use queries to digitally compile the entire body of communications that have been incidentally collected under Section 702 that involve a particular U.S. person’s email address, telephone number, or other identifier, with the exception that Internet communications acquired through upstream collection may not be queried using U.S. person identifiers.\footnote{See NSA 2011 Minimization Procedures, supra, § 3(b)(6).} In addition, the manner in which the FBI is employing U.S. person queries, while subject to genuine efforts at executive branch oversight, is difficult to evaluate, as is the CIA’s use of metadata queries.

If the NSA, CIA, or FBI wishes to permanently retain a communication of or concerning a U.S. person (beyond the default retention periods), personnel must make a determination that retention is justified under certain criteria established in their minimization procedures. Those criteria demand a legitimate governmental interest in the communication, but are fairly broad with respect to the types of needs and purposes that justify retention. The NSA, for instance, permits retention if the identity of the U.S. person “is necessary to understand foreign intelligence information or assess its importance,” or if
the communication contains evidence of a crime, among other reasons.\footnote{NSA 2011 Minimization Procedures, \textit{supra}, § 6(a), (b)(2).} The CIA’s and FBI’s rules are comparable.

Agencies that receive Section 702 communications may disseminate to another agency foreign intelligence information of or concerning a U.S. person, or evidence of a crime concerning a U.S. person, that was acquired from those communications. This is done most frequently by the NSA, reflecting the nature of its mission. When making such disseminations, NSA personnel typically “mask” the information about that U.S. person that could be used to identify him or her — replacing a proper name with, for instance, “a U.S. person” — but they may “unmask” such information upon request (with supervisory approval) when the requesting agency is deemed to legitimately require the information for its mission.\footnote{NSA DCLPO REPORT, \textit{supra}, at 7-8; NSA 2011 Minimization Procedures, \textit{supra}, § 6(b).} The number of disseminated reports containing references to U.S. person identifiers are reported annually to congressional oversight committees. As with U.S. person queries, these rules guard against the unjustified use of information about U.S. persons for illegitimate ends, but they do not significantly restrict the use of such information for legitimate intelligence and law enforcement aims.\footnote{Under similar rules and additional internal restrictions, the NSA may share communications involving U.S. persons with foreign governments. NSA 2011 Minimization Procedures, \textit{supra}, § 8(a). The NSA also is permitted to use and disseminate U.S. persons’ privileged attorney-client communications, subject to approval from its Office of General Counsel, as long as the person is not known to be under criminal indictment in the United States and communicating with an attorney about that matter. \textit{Id.} § 4. The CIA and FBI minimization procedures contain comparable provisions.}

In 2013, the vast majority of the intelligence reports disseminated by the NSA that were based on intelligence derived from Section 702 contained no reference to any U.S. person. A significant number of such reports, however (albeit a small percentage of the total), did include references to U.S. persons. As noted, U.S. person information in these reports typically is initially “masked” to hide personally identifying information.

In response to requests from recipients of those reports (primarily intelligence and law enforcement agencies), last year the NSA “unmasked” approximately 10,000 U.S. person identities where the information was not included in the original reporting.\footnote{According to the NSA, fewer than a quarter of these identifiers were proper names of individuals or their titles; the remainder were U.S. corporation names, U.S. educational institution names, U.S.-registered IP addresses, websites hosted in the United States, email addresses or telephone numbers potentially used by U.S. persons, and other identifiers potentially used by U.S. persons.}

Apart from this intelligence reporting, the NSA is permitted to pass on information showing possible violations of the law to the DOJ and the FBI. In 2013, the agency passed on such information only ten times.
In the Board’s view, the protections contained in the agencies’ minimization procedures are reasonably designed and implemented to ward against exploitation of information acquired under Section 702 for illegitimate purposes. The Board has seen no trace of any such illegitimate activity associated with the program, or any attempt to intentionally circumvent legal limits.

Depending on the scope of collection, however, the applicable rules may allow a substantial amount of private information about U.S. persons to be acquired by the government, examined by its personnel, and used in ways that may have a negative impact on those persons. Although it is not known how many communications involving U.S. persons or people in the United States are acquired under Section 702, the limited figures available may provide some indication of the extent to which the government presently could be using such communications. Some of these figures illustrate that the Section 702 program remains primarily focused on monitoring non-U.S. persons located outside the United States. By the same token, the overall scope of collection under the program and the quantity of intelligence reporting derived from this collection involving U.S. persons suggest that the government may be gathering and utilizing a significant amount of information about U.S. persons under Section 702.

If so, this would raise legitimate concern about whether a collection program that is premised on targeting foreigners located outside the United States without individual judicial orders now acquires substantial information about U.S. persons without the safeguards of individualized court review. Emphasizing again that we have seen no indication of abuse, nor any sign that the government has taken lightly its obligations to establish and adhere to a detailed set of rules governing the program, the collection and examination of U.S. persons’ communications represents a privacy intrusion even in the absence of misuse for improper ends. The Board’s desire to provide more clarity and transparency regarding the government’s activities under Section 702, particularly insofar as they involve the acquisition and handling of U.S. persons’ communications, underlies a number of our recommendations.
Part 6:

RECOMMENDATIONS

The Board has conducted an in-depth study of the Section 702 program. We have carefully considered whether the program as implemented complies with the statute and is consistent with constitutional requirements. The Board has also evaluated whether the program strikes the right balance between national security and privacy and civil liberties as a policy matter. The Board recognizes the considerable value that the Section 702 program provides in the government’s efforts to combat terrorism and gather foreign intelligence, and finds that at its core, the program is sound. However, some features outside of the program’s core, particularly those impacting U.S. persons, raise questions regarding the reasonableness of the program. The Board therefore offers a series of policy recommendations to ensure that the program includes adequate and appropriate safeguards for privacy and civil liberties.

The Board has identified five key areas where operations of the Section 702 program could strike a better balance between privacy, civil rights, and national security. They include the manner in which targeting and tasking is implemented, the manner in which queries using U.S. person identifiers are conducted, and the Foreign Intelligence Surveillance Court’s (“FISC” or “FISA court”) role in the certification process. Additional areas for improvement include the government’s collection of upstream Internet transactions, transparency in the operations of the Section 702 program. We also make a recommendation, not limited only to Section 702, about evaluation of the efficacy of government surveillance programs. Based on our independent review and the conclusions we have drawn, the Board offers the following recommendations.

I. Targeting and Tasking

Recommendation 1: The NSA’s targeting procedures should be revised to (a) specify criteria for determining the expected foreign intelligence value of a particular target, and (b) require a written explanation of the basis for that determination sufficient to demonstrate that the targeting of each selector is likely to return foreign intelligence information relevant to the subject of one of the certifications approved by the FISA court. The NSA should implement these revised targeting procedures through revised guidance and training for analysts, specifying the criteria for the foreign intelligence determination and the kind of written explanation needed to support it. We expect that the FISA
The court’s review of these targeting procedures in the course of the court’s periodic review of Section 702 certifications will include an assessment of whether the revised procedures provide adequate guidance to ensure that targeting decisions are reasonably designed to acquire foreign intelligence information relevant to the subject of one of the certifications approved by the FISA court. Upon revision of the NSA’s targeting procedures, internal agency reviews, as well as compliance audits performed by the ODNI and DOJ, should include an assessment of compliance with the foreign intelligence purpose requirement comparable to the review currently conducted of compliance with the requirement that targets are reasonably believed to be non-U.S. persons located outside the United States.

In order to target a person under Section 702, two basic criteria must be satisfied: the person must be a non-U.S. person located outside the United States (the “foreignness determination”) and the surveillance must be conducted to collect foreign intelligence information (the “foreign intelligence purpose determination”).

The Board’s review of the Section 702 program showed that the procedures for documenting targeting decisions within the NSA, and the procedures for reviewing those decisions within the executive branch, focus primarily on the foreignness determination — establishing that a potential target is a non-U.S. person reasonably believed to be located abroad. The process for documenting and reviewing the foreign intelligence purpose of a targeting is not as rigorous. Agency personnel have not been required to articulate or explain these determinations in any detail as a matter of course, and typically indicate what category of foreign intelligence information they expect to obtain from targeting a particular person in a single brief sentence that contains only minimal information about why the analyst believes that targeting this person will yield foreign intelligence information. As a result, the Section 702 oversight team from the DOJ and the ODNI cannot scrutinize these foreign intelligence purpose determinations with the same rigor that it scrutinizes foreignness determinations. In contrast, NSA analysts are required to articulate a rationale to a much greater degree regarding their foreignness determinations, and oversight is accordingly more in-depth.

The Board recognizes that this distinction stems from the different treatment of the foreignness and foreign intelligence purpose determinations in Section 702 itself. Section 702(d), the subsection of the statute outlining the requirements for targeting procedures, specifically requires that the procedures be reasonably designed to ensure that targeting is limited to persons reasonably believed to be located outside the United States, but there is no comparable requirement in this subsection specifying that targeting procedures must be reasonably designed to ensure that targeting has a valid foreign intelligence purpose. Likewise, when the FISA court assesses whether the government’s targeting procedures
comply with statutory requirements, the court is directed by Section 702(i), to consider the adequacy of those procedures with respect to the foreignness determination, but there is no comparable provision specifically requiring a review of the foreign intelligence purpose determination.

Despite the fact that the statute treats these two determinations differently, it also demands that all targeting be intended “to acquire foreign intelligence information.” Thus, the foreign intelligence purpose determination is a critical part of the statutory framework. From a constitutional perspective, moreover, at least insofar as Section 702 surveillance incidentally collects communications to and from U.S. persons, the foreign intelligence purpose is what provides the basis for the government to conduct Section 702 surveillance without a warrant. As a result, we conclude that there should be something closer to parity between the foreignness determination and foreign intelligence purpose determination in terms of what level of explanation is required of an analyst and how rigorous the oversight of that explanation is.

Therefore, the Board recommends that the NSA’s targeting procedures be updated to require a more detailed written explanation of the foreign intelligence purpose of each targeting decision and to specify the criteria that would be sufficient to demonstrate that this standard has been met. Changes to the targeting procedures that provide more guidance to analysts and require more explanation regarding the foreign intelligence purpose of a targeting will help analysts better articulate this element of their targeting decisions. When analysts articulate at greater length the bases for their targeting decisions, the executive branch oversight team that later reviews those decisions will be better equipped to meaningfully review them.

The Board does not believe that a statutory change is needed to implement this recommendation. The government already has the authority to amend its targeting procedures, subject to FISA court approval. We believe that it would be helpful for the FISA court, when reviewing Section 702 certifications, to assess whether the government’s targeting procedures are reasonably designed to ensure that targeting is limited to persons of foreign intelligence value, much like the court now assesses whether targeting procedures are reasonably designed to ensure that targeting is limited to persons located outside the United States. We believe that, without statutory change, the government could request that the FISA court assume this additional task, as the FISA court already must and does consider how fully the Section 702 program is geared toward acquiring foreign intelligence, in order to ensure that the program is authorized by the statute and consistent with the Fourth Amendment.

Once the revised targeting procedures are in place, analysts should be trained on their implementation, to ensure that the analysts are appropriately articulating the rationale for foreign intelligence purpose determinations. The NSA should also modify its
internal agency reviews to ensure that the new targeting procedures have been adopted by its analysts. The executive branch compliance audits should also be modified to reflect the new targeting procedures and to include more rigorous scrutiny of whether valid foreign intelligence purpose determinations are being properly articulated.

II. U.S. Person Queries

Recommendation 2: The FBI’s minimization procedures should be updated to more clearly reflect actual practice for conducting U.S. person queries, including the frequency with which Section 702 data may be searched when making routine queries as part of FBI assessments and investigations. Further, some additional limits should be placed on the FBI’s use and dissemination of Section 702 data in connection with non-foreign intelligence criminal matters.

When an FBI agent or analyst initiates a criminal assessment or begins a new criminal investigation related to any type of crime, it is routine practice, pursuant to the Attorney General Guidelines for Domestic FBI Operations, to conduct a query of FBI databases in order to determine whether they contain information on the subject of the assessment or investigation. The databases queried may include information collected under various FISA authorities, including data collected under Section 702. The FBI’s rules relating to queries do not distinguish between U.S. persons and non-U.S. persons; as a domestic law enforcement agency, most of the FBI’s work concerns U.S. persons. If a query leads to a “hit” in the FISA data (i.e., if a communication is found within a repository of Section 702 data that is responsive to the query), then the agent or analyst is alerted to the existence of the hit. If the agent or analyst has received training on how to handle FISA-acquired materials, he or she is able to view the Section 702 data that was responsive to the query; however, if the agent or analyst has not received FISA training he or she is merely alerted to the existence of the information but cannot access it. The agent or analyst would have to contact a FISA-trained agent or analyst and ask him or her to review the information.

Even though FBI analysts and agents who solely work on non-foreign intelligence crimes are not required to conduct queries of databases containing Section 702 data, they are permitted to conduct such queries and many do conduct such queries. This is not clearly expressed in the FBI’s minimization procedures, and the minimization procedures should be modified to better reflect this actual practice. The Board believes that it is important for accountability and transparency that the minimization procedures provide a clear representation of operational practices. Among other benefits, this improved clarity will better enable the FISA court to assess statutory and constitutional compliance when
the minimization procedures are presented to the court for approval with the
government’s next recertification application.

In light of the privacy and civil liberties implications of using Section 702
information, collected under lower thresholds and for a foreign intelligence purpose, in the
FBI’s pursuit of non–foreign intelligence crimes, the Board believes it is appropriate to
place some additional limits on what can be done with Section 702 information. Members
of the Board differ on the nature of the limitations that should be placed on the use of that
information. Board Members’ proposals and a brief explanation of the reasoning
supporting each are stated below, with elaboration in the two separate statements.

Additional Comment of Chairman David Medine and Board Member Patricia Wald

For acquisitions authorized under Section 702, FISA permits the FBI for law
enforcement purposes, to retain and disseminate evidence of a crime. However, there is a
difference between obtaining a U.S. person’s communications when they are in plain view
as an analyst reviews the target’s communications, and the retrieval of a U.S. person’s
communications by querying the FBI’s Section 702 holdings collected over the course of
years.\footnote{On June 25, 2014, the United States Supreme Court ruled unanimously that a search of a cell phone
seized by the police from an individual who has been arrested required a warrant. \textit{Riley v. California}, No. 13-132,
2014 WL 2864483 (U.S. June 25, 2014). The Court distinguished between reviewing one record versus
conducting an extensive records search over a long period: “The fact that someone could have tucked a paper
bank statement in a pocket does not justify a search of every bank statement from the last five years.” \textit{Id. at
*18}. Likewise, observing evidence of a crime in one email does not justify conducting a search of an
American’s emails over the prior five years to or from everyone targeted under the Section 702 program.}
Therefore, consistent with our separate statement regarding Recommendation 3,
we believe that U.S. persons’ privacy interests regarding 702 data should be protected by
requiring that each identifier should be submitted to the FISA court for approval before the
identifier may be used to query data collected under Section 702, other than in exigent
circumstances. The court should determine, based on documentation submitted by the
government, whether the use of the U.S. person identifier for Section 702 queries meets the
standard that the identifier is reasonably likely to return information relevant to an
assessment or investigation of a crime. As discussed in more detail in our separate
statement, this judicial review would not be necessary for U.S. persons who are already
suspected terrorists and subject to surveillance under other government programs.

Additional Comment of Board Members Rachel Brand and Elisebeth Collins Cook

As explained in our separate statement, we would support a requirement that an
analyst conducting a query in a non–foreign intelligence criminal matter obtain
supervisory approval before accessing any Section 702 information that was responsive to
the query. We would also support a requirement of higher-level Justice Department
approval, to the extent not already required, before Section 702 information could be used
in the investigation or prosecution of a non–foreign intelligence crime (such as in the application for a search warrant or wiretap, in the grand jury, or at trial). We would not require any additional approvals before an analyst could conduct a query of databases that include FISA data.

Additional Comment of Board Member James Dempsey

It is imperative not to re-erect the wall limiting discovery and use of information vital to the national security, and nothing in the Board’s recommendations would do so. The constitutionality of the Section 702 program is based on the premise that there are limits on the retention, use and dissemination of the communications of U.S. persons collected under the program. The proper mix of limitations that would keep the program within constitutional bounds and acceptable to the American public may vary from agency to agency and under different circumstances. The discussion of queries and uses at the FBI in this Report is based on our understanding of current practices associated with the FBI’s receipt and use of Section 702 data. The evolution of those practices may merit a different balancing. For now, the use or dissemination of Section 702 data by the FBI for non-national security matters is apparently largely, if not entirely, hypothetical. The possibility, however, should be addressed before the question arises in a moment of perceived urgency. Any number of possible structures would provide heightened protection of U.S. persons consistent with the imperative to discover and use critical national security information already in the hands of the government.546

Recommendation 3: The NSA and CIA minimization procedures should permit the agencies to query collected Section 702 data for foreign intelligence purposes using U.S. person identifiers only if the query is based upon a statement of facts showing that the query is reasonably likely to return foreign intelligence information as defined in FISA. The NSA and CIA should develop written guidance for agents and analysts as to what information and documentation is needed to meet this standard, including specific examples.

Under the NSA and CIA minimization procedures for the Section 702 program, analysts are permitted to perform queries of databases that hold communications acquired under Section 702 using query terms that involve U.S. person identifiers. Such queries are designed to identify communications in the database that involve or contain information relating to a U.S. person.

The internal processes employed by the two agencies with respect to U.S. person queries differ. Under the NSA’s minimization procedures, all queries that involve U.S. person identifiers (whether they search content or metadata) must be constructed so as to be “reasonably likely to return foreign intelligence information.” The NSA also requires analysts to provide written justifications for the use of all query terms that involve U.S. person identifiers. More specifically, with respect to querying the metadata of Section 702 communications (which includes, for instance, the email address from which a communication was sent), analysts must document the basis for queries that involve U.S. person identifiers, which are subject to audit. With respect to queries that scan the contents of Section 702 communications, analysts must obtain prior approval for any query term that involves a U.S. person identifier. (Subsequent uses of an already approved query term do not require new permission.)

Under the CIA’s minimization procedures, personnel must document the foreign intelligence basis for queries of content queries that involve U.S. person identifiers, which are subject to audit, but need not document a justification or obtain prior approval for queries of metadata.

Although the Board recognizes that NSA and CIA queries are subject to rigorous oversight by the DOJ’s National Security Division and the ODNI (with the exception of metadata queries at the CIA, which are not reviewed by the oversight team), we believe that NSA and CIA analysts, before conducting a query involving a U.S. person identifier, should provide a statement of facts illustrating why they believe the query is reasonably likely to return foreign intelligence information.\(^{547}\) To assist in this process, the government should develop written guidance for the benefit of analysts who are authorized to perform such queries to clearly explain the meaning of the standard “reasonably likely to return foreign intelligence information.” It should also provide illustrative examples of permissible and impermissible queries as well as proper and improper bases on which to conclude that a query is reasonably likely to return foreign intelligence. This guidance should reflect the fact that the statutory definition of “foreign intelligence information” under FISA is narrower when the information in question involves U.S. persons than it is when information pertains only to non-U.S. persons.

Implementing these measures will help to ensure that analysts at the NSA and CIA do not access or view communications acquired under Section 702 that involve or concern U.S. persons when there is no valid foreign intelligence reason to do so.

---

\(^{547}\) Board Member Elisebeth Collins Cook would not extend a new requirement to this effect to metadata queries.
III. FISC Role

Recommendation 4: To assist in the FISA court’s consideration of the government’s periodic Section 702 certification applications, the government should submit with those applications a random sample of tasking sheets and a random sample of the NSA’s and CIA’s U.S. person query terms, with supporting documentation. The sample size and methodology should be approved by the FISA court.

The FISA court reviews the government’s proposed targeting and minimization procedures each time the government seeks approval or re-approval of a certification, typically annually. To assist the FISA court in its review, the government should provide the court with a random sample of targeting decisions (reflected in “tasking” sheets) and a random sample of NSA and CIA query terms that involve U.S. person identifiers. The FISC should approve the methodology used to select the samples and the size of those samples.

Providing a random sample of targeting decisions would allow the FISC to take a retrospective look at the targets selected over the course of a recent period of time. The data could help inform the FISA court’s review process by providing some insight into whether the government is, in fact, satisfying the foreignness and foreign intelligence purpose requirements, and it could signal to the court that changes to the targeting procedures may be needed, or prompt inquiry into that question. The data could provide verification that the government’s representations during the previous certification approval were accurate, and it could supply the FISC with more information to use in determining whether the government’s acquisitions comply with the statute and the Fourth Amendment.

Similarly, a retrospective sample of U.S. person query terms and supporting documentation will allow the FISC to conduct a fuller review of the government’s minimization procedures. Such a sample could allow greater insight into the methods by which information gathered under Section 702 is being utilized, and whether those methods are consistent with the minimization procedures. While U.S. person queries by the NSA and CIA are already subject to rigorous executive branch oversight (with the exception of metadata queries at CIA), supplying this additional information to the FISC could help guide the court by highlighting whether the minimization procedures are being followed and whether changes to those procedures are needed.

Chairman David Medine and Board Member Patricia Wald see no reason to exclude the FBI’s query process from FISA court oversight. While it is correct that the FBI does not distinguish between queries using U.S. person identifiers and those that do not, as a domestic law enforcement agency it clearly conducts a significant number of queries using identifiers belonging to U.S. persons. Therefore, a sample of the queries performed by the FBI could inform the FISA court’s review.
Recommendation 5: As part of the periodic certification process, the government should incorporate into its submission to the FISA court the rules for operation of the Section 702 program that have not already been included in certification orders by the FISA court, and that at present are contained in separate orders and opinions, affidavits, compliance and other letters, hearing transcripts, and mandatory reports filed by the government. To the extent that the FISA court agrees that these rules govern the operation of the Section 702 program, the FISA court should expressly incorporate them into its order approving Section 702 certifications.

The government’s operation of the Section 702 program must adhere to the targeting and minimization procedures that are approved by the FISA court, as well as to the pertinent Attorney General guidelines and the statute itself. The government also makes additional representations to the FISA court through compliance notices and other filings, as well as during hearings, that together create a series of more rigorous precedents and a common understanding between the government and the court regarding the operation of the program. More than once, the government has implemented rules for the Section 702 program that are more detailed than what is reflected in the text of the targeting and minimization procedures themselves, although these rules typically are viewed as an interpretation of those procedures. These more detailed rules are not centrally located but are contained in compliance letters, affidavits, mandatory reports, hearing transcripts, and other sources that arise from the interaction between the government and the FISC. Such rules have precedential value and create real consequences, as the government considers itself bound to abide by the representations it makes to the FISA court. To the extent that the rules which have emerged from these representations and this interactive process govern the operation of the Section 702 program, they should be memorialized in a single place and incorporated into the FISC’s certification review.

This recommendation is influenced by the Board’s recognition that FISC judges and legal advisors do not serve on the court forever. As judges rotate out of FISC service, the risk that important information about the contours of the Section 702 program will be lost due to attrition, or not fully appreciated by new judges, greatly increases when the body of precedent that has developed over the course of the program’s existence is not centrally located. Adopting this recommendation would ensure that each judge who may come to render decisions about the program will have ready access to a centralized source that encapsulates this body of precedent, to help inform his or her decisions and understanding of the program. This consolidation of rules will also facilitate congressional oversight of the Section 702 program. Accordingly, the Board views this recommendation as a measure to promote good government.
Additionally, incorporating the series of precedents described above into a comprehensive source will provide a single reference point for every government lawyer, agent, officer, and analyst within the Intelligence Community who has responsibilities under the Section 702 program. These precedents and rules, given their dispersed location within a range of different FISA court filings and documents, may not be readily accessible to the lawyers tasked with helping to implement the requirements specified in those documents or to the agents and analysts operating the program. A complete, readily accessible legal framework will assist lawyers and analysts throughout the government in their efforts to comply with the requirements of the Section 702 program.

IV. Upstream and “About” Collection

Recommendation 6: To build on current efforts to filter upstream communications to avoid collection of purely domestic communications, the NSA and DOJ, in consultation with affected telecommunications service providers, and as appropriate, with independent experts, should periodically assess whether filtering techniques applied in upstream collection utilize the best technology consistent with program needs to ensure government acquisition of only communications that are authorized for collection and prevent the inadvertent collection of domestic communications.

In PRISM collection, through which the government obtains communications directly from Internet service providers, the government acquires only those communications sent to or from selectors used by targeted persons. Obtaining only communications sent to and from those selectors helps ensure that no wholly domestic communications are acquired — because the targeted person who uses the selector always must be someone reasonably believed to be located outside the United States.

In upstream collection, by contrast, the NSA obtains communications directly from the Internet “backbone,” with the compelled assistance of companies that maintain those networks, rather than Internet service providers that supply particular modes of communication. The success of this process depends on collection devices that can reliably acquire data packets associated with the proper communications. In addition, through “about” collection, the upstream process includes acquiring communications that contain reference to selectors used by targeted persons, even if the communication is not sent to or from the account of that selector. Because the targeted person may not be a party to the communication, it is possible that neither participant in the communication is located outside the United States, although the NSA takes additional measures, including the use of IP filters, to try to avoid collecting wholly domestic communications.
As a result, upstream collection involves a greater risk that the government will acquire wholly domestic communications, which it is not authorized to intentionally collect under Section 702. Ensuring that the upstream collection process comports with statutory limits and with agency targeting procedures involves an important technical process of filtering out wholly domestic communications. The government acknowledges, however, that the technical methods used to prevent the acquisition of domestic communications do not completely prevent them from being acquired. Even if domestic communications were to constitute a very small percentage of upstream collection, this could still result in a large overall number of purely domestic communications being collected. Mindful of these considerations, the Board believes that there should be an ongoing dialogue, both within the government and in cooperation with telecommunications providers or independent experts, to ensure that the means being used to filter for domestic communications use the best technology. We also believe that the determination about whether this is the case should be continually revisited.

**Recommendation 7: The NSA periodically should review the types of communications acquired through “about” collection under Section 702, and study the extent to which it would be technically feasible to limit, as appropriate, the types of “about” collection.**

In the upstream collection process, as in the PRISM collection process, the NSA acquires Internet communications sent to and from the selector, such as an email address, used by a targeted person. In upstream, however, the NSA also acquires Internet communications that are not sent to or from this email address, but instead contain reference to the selector, sometimes in the body of the communication. These are termed “about” communications, because they are not to or from, but rather “about” the communication selectors of targeted persons. In addition, for technical reasons, “about” collection is needed even to acquire some communications that actually are “to” or “from” a target.

A number of different scenarios result in a communication containing reference to a particular selector when the communication is not to or from that selector. Thus, there are a number of different categories or types of “about” communications acquired by the NSA. Some forms of “about” communications are actually the communications of targeted persons. Other types of “about” collection can result in the acquisition of communications between two non-targets, thereby implicating greater privacy concerns. For instance, when a person in the United States sends or receives an international communication that contains a targeted email address in the body of the communication, that communication may be acquired by the NSA, even if the sender and recipient are not targets themselves and were completely unknown to the government before its collection devices examined...
the contents of their communication. Moreover, the permissible scope of targeting in the Section 702 program is broad enough that targets need not themselves be suspected terrorists or other bad actors. Thus, if the email address of a target appears in the body of a communication between two non-targets, it does not necessarily mean that either of the communicants is in touch with a suspected terrorist.

All of these types of “about” communications can provide intelligence value, helping the government learn more about terrorist networks and their plans or obtain other foreign intelligence. While “about” collection is valued by the government for its unique intelligence benefits, it is, to a large degree, an inevitable byproduct of the way the NSA conducts much of its upstream collection. As discussed earlier in this Report, because of the technical manner in which this collection is performed, the NSA cannot entirely stop acquiring “about” communications without also missing a significant portion of “to/from” communications. Nor does the agency have the capability to selectively acquire certain types of “about” communications but not others.

At least some forms of “about” collection present novel and difficult issues regarding the balance between privacy and national security. But current technological limits make any debate about the proper balance somewhat academic, because it is largely unfeasible to limit “about” collection without also eliminating a substantial portion of upstream’s “to/from” collection, which would more drastically hinder the government’s counterterrorism efforts.

We therefore recommend that the NSA work to develop technology that would enable it to identify and distinguish among the types of “about” collection at the acquisition stage, and then selectively limit or modify its “about” collection, as may later be deemed appropriate. If it is not possible for collection devices to identify or differentiate among types of “about” communications at the acquisition stage, we urge the NSA to develop technology that would allow it to automatically segregate all “about” communications after collection (and, if possible, to individually segregate different types of “about” communications from one another after collection). With such mechanisms in place, it will be possible to have a policy discussion about whether or not the privacy impacts of particular types of “about” collection justify treating those types of communications in a different way or eliminating their collection entirely.

V. Accountability and Transparency

Recommendation 8: To the maximum extent consistent with national security, the government should create and release, with minimal redactions, declassified versions of the FBI’s and CIA’s Section 702 minimization procedures, as well as the NSA’s current minimization procedures.
The Board believes that the public would benefit from understanding the procedures that govern the acquisition, use, retention, and dissemination of information collected under Section 702. The Board respects the government’s need to protect its operational methods and practices, but it also recognizes that transparency enables accountability to the public that the government serves. Therefore, the Board urges the government to engage in a declassification review and, to the greatest extent possible without jeopardizing national security, release unredacted versions of the FBI, CIA, and NSA minimization procedures.

Recommendation 9: The government should implement five measures to provide insight about the extent to which the NSA acquires and utilizes the communications involving U.S. persons and people located in the United States under the Section 702 program. Specifically, the NSA should implement processes to annually count the following: (1) the number of telephone communications acquired in which one caller is located in the United States; (2) the number of Internet communications acquired through upstream collection that originate or terminate in the United States; (3) the number of communications of or concerning U.S. persons that the NSA positively identifies as such in the routine course of its work; (4) the number of queries performed that employ U.S. person identifiers, specifically distinguishing the number of such queries that include names, titles, or other identifiers potentially associated with individuals; and (5) the number of instances in which the NSA disseminates non-public information about U.S. persons, specifically distinguishing disseminations that includes names, titles, or other identifiers potentially associated with individuals. These figures should be reported to Congress in the NSA Director's annual report and should be released publicly to the extent consistent with national security.

Under Section 702, the government acquires the contents of telephone calls and Internet communications from within the United States, without individualized warrants or court orders, so long as the acquisition involves targeting non-U.S. persons reasonably believed to be located outside the United States, for foreign intelligence purposes.

Those targeted persons, of course, may communicate with U.S. persons or people located in the United States, resulting in the “incidental” collection of their communications. Since the enactment of the FISA Amendment Act in 2008, the extent to which the government acquires the communications of U.S. persons under Section 702 has been one of the biggest open questions about the program, and a continuing source of public concern. Lawmakers and civil liberties advocates have called upon the executive branch to disclose how many communications of U.S. persons are being acquired. In turn,
the executive branch has responded that it cannot provide such a number — because it is often difficult to determine from a communication the nationality of its participants, and because the large volume of collection under Section 702 would make it impossible to conduct such determinations for every communication that is acquired. The executive branch also has pointed out that any attempt to document the nationality of participants to communications acquired under Section 702 would actually be invasive of privacy, because it would require government personnel to spend time scrutinizing the contents of private messages that they otherwise might never access or closely review.

As a result of this impasse, lawmakers and the public do not have even a rough estimate of how many communications of U.S. persons are acquired under Section 702.

Based on information provided by the NSA, the Board believes that certain measures can be adopted that could provide insight into these questions without unduly burdening the NSA or disrupting the work of its analysts, and without requiring the agency to further scrutinize the contents of U.S. persons’ communications. We believe that the NSA could implement five measures, listed above, that collectively would shed some light on the extent to which communications involving U.S. persons or people located in the United States are being acquired and utilized under Section 702. While the measures we have proposed will provide only partial insight into this question (they will not, for instance, reveal the number of communication obtained under PRISM collection, which accounts for the vast majority of Internet acquisitions), they will provide a snapshot, albeit imperfect, of the degree to which the NSA under Section 702 acquires communications involving U.S. persons, queries them, retains them permanently, and disseminates information from them to other agencies.

The number of queries and disseminations involving U.S. person information are already tracked by the NSA, but we believe that these figures should be annually reported in a central document along with the new figures we have proposed counting, and that the NSA’s annual reporting of its queries and disseminations should highlight those that potentially involve individuals (as opposed to businesses or institutions), which are of special interest from a privacy perspective. It is possible that with respect to the first two measures above, the information that the NSA feasibly can document might turn out to be insufficiently comprehensive to yield dependable numbers, but this will not be known until the NSA attempts to implement the recommendation.

Adopting the measures that we have proposed will supply policymakers and the public with important information about one of the most frequently discussed aspects of the Section 702 program, enabling more informed judgments to be made about the program in the future.
VI. Efficacy

**Recommendation 10: The government should develop a comprehensive methodology for assessing the efficacy and relative value of counterterrorism programs.**

The efficacy of any particular counterterrorism program is difficult to assess. Even when focusing only on programs of surveillance, such programs can serve a variety of functions that contribute to the prevention of terrorism. Most obviously, a surveillance program may reveal the existence of a planned terrorist attack, enabling the government to disrupt the attack. But the number of “plots thwarted” in this way is only one measure of success. Counterterrorism surveillance programs can enable the government to learn about the identities and activities of the individuals who make up terrorist networks. They can help the government to understand the goals and intentions of those organizations, as well as the ways in which the organizations fund their pursuits and coordinate the activities of their members. All of this knowledge can aid the government in taking steps to frustrate the efforts of these terrorist organizations — potentially stymieing their endeavors long before they coalesce around the plotting and implementation of a specific attack. Because the nature of counterterrorism efforts can vary, measures of success may vary as well.

Moreover, individual counterterrorism programs are not typically used in isolation; rather, these programs can support and mutually reinforce one another. Therefore, the success of a particular program may not be susceptible to evaluation based on what it produces in a vacuum. Any evaluation must instead seek to understand how a particular program fits within the government’s overall counterterrorism efforts, and to what degree it aids those efforts relative to other programs.

Despite these complications, determining the efficacy and value of particular counterterrorism programs is critical. Without such determinations, policymakers and courts cannot effectively weigh the interests of the government in conducting a program against the intrusions on privacy and civil liberties that it may cause. In addition, government counterterrorism resources are not unlimited, and if a program is not working, those resources should be redirected to programs that are more effective in protecting us from terrorists. Accordingly, the Board believes that the government should develop a methodology to gauge and assign value to its counterterrorism programs, and use that methodology to determine if particular programs are meeting their stated goals. The Board is aware that the ODNI conducts studies to measure the relative efficacy of different types of intelligence activities to assist in budgetary decisions. The Board believes that this important work should be continued, as well as expanded so as to differentiate more precisely among individual programs, in order to assist policymakers in making informed, data-driven decisions about governmental activities that have the potential to invade the privacy and civil liberties of the public.
Part 7:

CONCLUSION

One of the Board’s goals in developing this Report has been to provide greater transparency and clarity to the public regarding the operation of the Section 702 program. This is a complex program, and, in the wake of the unauthorized disclosures about the program, there has been a great deal of misinformation circulated to the public. The Board is grateful to the Intelligence Community and the Department of Justice for its employees’ tireless efforts to educate Board Members and staff about the program’s operation, and to work with us to declassify information in the public interest. The Board also appreciates the work of the many government officials and employees, congressional staff, privacy and civil liberties advocates, academics, trade associations, and technology and communications companies who provided input into the Board’s study of the program.

In addition to this effort to explain the Section 702 program, the Board has set forth a series of policy recommendations designed to ensure that the program appropriately balances national security concerns with privacy and civil liberties. We note that this is only the start of the dialogue. We do not believe that any of the recommendations we offer would require legislative changes, and the Board welcomes the opportunity for further discussion of these pressing issues and how to best implement the Board’s recommendations. We hope that this Report contributes to “a way forward that secures the life of our nation while preserving the liberties that make our nation worth fighting for.”

INDEX TO ANNEXES

A. Separate Statement by Chairman David Medine and Board Member Patricia Wald
B. Separate Statement by Board Members Rachel Brand and Elisebeth Collins Cook
C. July 9, 2013 Workshop Agenda and Link to Workshop Transcript
D. November 4, 2013 Hearing Agenda and Link to Hearing Transcript
E. March 19, 2014 Hearing Agenda and Link to Hearing Transcript
F. Request for Public Comments on Board Study
G. Reopening the Public Comment Period
H. Index to Public Comments on www.regulations.gov
ANNEX A

Separate Statement of Chairman David Medine and Board Member Patricia Wald

I. Recommendation Regarding U.S. Person Queries for Foreign Intelligence Purposes

We do not believe that the Board’s Recommendation 3 goes nearly far enough to protect U.S. persons’ privacy rights when their communications are incidentally collected as a consequence of targeting a non-U.S. person located abroad under Section 702. The Section 702 program has collected hundreds of millions of Internet communications. Even if only a small percentage of those communications are to or from an American, the total number of Americans’ communications is likely significant. Furthermore, these communications, which may be maintained for many years in government databases in searchable form, may contain sensitive and confidential matters having nothing to do with the foreign intelligence purposes of the Section 702 program. Although such queries must be conducted for a foreign intelligence purpose, currently, the government can query several years of such communications without court approval, which could potentially produce a composite picture of a significant slice of an American’s private life.

This practice raises two related concerns with constitutional, statutory, and policy implications. First, are sufficient protections in place to purge Americans’ communications that have no foreign intelligence value? Second, are there sufficient restrictions on when the government can query data collected under Section 702 to seek Americans’ communications? We offer the following proposals to address each of these concerns.

Recommendation

Minimization procedures that govern the use of Americans’ communications collected under Section 702 should require the following:

(1) No later than when the results of a U.S. person query of Section 702 data are generated, Americans’ communications should be purged of information that does not meet the statutory definition of foreign intelligence information relating to Americans.\(^{550}\) This process should be subject to judicial oversight.

(2) Each U.S. person identifier should be submitted to the FISA court for approval before the identifier may be used to query data collected under Section 702 for a foreign

\(^{550}\) U.S. person communications may also be responsive to queries using non-U.S. person identifiers. The same purge procedure should apply in such cases.
intelligence purpose,\textsuperscript{551} other than in exigent circumstances or where otherwise required by law.\textsuperscript{552} The court should determine, based on documentation submitted by the government, whether the use of the U.S. person identifier for Section 702 queries meets the standard that the identifier is reasonably likely to return foreign intelligence information as defined under FISA.\textsuperscript{553}

**Discussion**

As explained in Part 3 above, under Section 702, the government may lawfully collect the communications of an American where that individual is communicating with a targeted non-U.S. person who is reasonably believed to be located outside the United States.\textsuperscript{554} The government refers to the collection of such Americans’ information as “incidental” collection, because the American will not be, and cannot be, the target of Section 702 surveillance. Although we understand that the government does not currently count the number of incidentally collected American communications, it is likely that the scope and extent of the Americans’ information collected under Section 702 is substantial: as of 2011, the NSA was acquiring approximately 250 million Internet communications annually, and even if only a small percentage of these total involved Americans the number would be large in absolute terms.\textsuperscript{555}

We recognize that a query of collected Section 702 data seeking information about a specific American\textsuperscript{556} may not provide as complete a picture of the individual’s activities as it would for an actual target of surveillance. Nonetheless, such queries are capable of

\textsuperscript{551} Queries for criminal purposes are governed by the proposal in Part II of this statement.


\textsuperscript{553} Subsequent queries using a FISA court–approved U.S. person identifier would not require court approval.

\textsuperscript{554} Through “about” collection, the NSA may also collect the communication of an American who is not in direct contact with a Section 702 target if a targeted selector appears within the communication. In addition, the NSA may collect the communications of an American who is not in direct contact with a Section 702 target through acquiring an “MCT.” However, such communications are acquired only through upstream collection and, thus, they may not be queried using U.S. person identifiers under current minimization procedures.

\textsuperscript{555} The NSA minimization procedures state that permanent retention of communications of Americans is permitted if they are of foreign intelligence value or certain other standards are met, including communications in which the identity of the American is necessary to understand foreign intelligence information or assess its importance. Minimization Procedures used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, § 6(b)(2) (Oct. 31, 2011) (“NSA 2011 Minimization Procedures”).

\textsuperscript{556} We are not proposing that the parties to every communication be investigated to determine if one or more of the parties are Americans. Such reviews themselves could raise privacy and civil liberties concerns. However, where there is a reasonable basis to conclude that a party is an American, the recommended procedures should apply.
revealing a significant slice of the American’s life. This is particularly the case for Americans who correspond frequently with foreigners, including relatives, business associates, and others. Because the scope of the legitimate foreign intelligence purposes that may justify surveillance under Section 702 is broad, going beyond counterterrorism, an American could be in contact with several targets of Section 702 surveillance and yet be innocent of any complicity in terrorist or other activity of foreign intelligence interest. Since Section 702 does not require any particularized judicial finding to support the initial collection of information from either the foreign target or the American who communicated with the target, further safeguards should be required to limit the permissible scope of U.S. person queries. Under present rules, querying of the communications to which the American was a party can be justified either on the grounds that they are likely to have foreign intelligence value or contain evidence of a crime.\textsuperscript{557} Moreover, there is currently no external check outside of the executive branch on the process of making such queries or purging of non–foreign intelligence material from query results.

We agree that legitimate foreign intelligence matters which appear in these Americans’ incidentally collected communications can be retained. However, we feel strongly that the present internal agency procedures for reviewing communications and purging those portions that are of no foreign intelligence value prior to use of the information\textsuperscript{558} are wholly inadequate to protect Americans’ acknowledged constitutional rights to protection for private information or to give effect to the statutory definition of foreign intelligence information, which, as discussed below, provides a more stringent test for information relating to Americans. Minimization guidelines approved by the FISA court were intended to afford these protections, but in their present form they do not. As a practical matter, most collected communications are not reviewed for the purging of non–foreign intelligence matters upon collection, or at any set time thereafter prior to use. The NSA guidelines require only that “upon review” the analyst should purge material that is “clearly” non–foreign intelligence information. The practice, when applying the “clearly” criteria for purging Americans’ communications, is to err on the side of insuring that any piece of private information is retained that might in the future conceivably take on value or that some other analyst in the intelligence community might find to be of value. We do not think this is the intent of the statute.

Some argue that the process of reviewing and purging of private information that has no intelligence value is more intrusive than permitting the information to remain in agency databases for years subject to viewing by intelligence personnel in multiple

\textsuperscript{557} See Section II of this Separate Statement regarding FBI queries relating to evidence of a crime.

\textsuperscript{558} NSA 2011 Minimization Procedures, supra, § 3.
agencies. In our view, there is no legitimate basis to maintain potentially personal, sensitive information that has no bearing on either foreign intelligence or criminal conduct. Nor do the restrictions on use of FISA data in criminal investigations requiring only Attorney General approval provide adequate protections to the vast majority of Americans whose communications have been incidentally collected, who will never be subjected to such proceedings, but whose information can be probed and queried and used to pursue investigations against them.

Our conclusion that more controls are required for this query process is informed by constitutional, statutory, and policy concerns. As discussed above, under the Fourth Amendment, the reasonableness of this program must be assessed based on the totality of the circumstances.\textsuperscript{559} The government recognizes that the initial collection of Americans’ communications under Section 702 constitutes a search under the Fourth Amendment. The reasonableness of this surveillance depends upon whether there are sufficient safeguards, including targeting and minimization procedures, to adequately protect the Fourth Amendment interests of persons whose communications may be collected, used, and disseminated. Since there are no prior determinations that any Americans whose communications have been collected are involved in terrorism or other activities of foreign intelligence interest (because Americans cannot be targeted), there should be compensatory safeguards governing the access, use, dissemination, and retention of the contents of their communications when those communications are acquired in the course of targeting others.

In this regard, we do not believe that the Fourth Amendment analysis justifying, in other contexts, the use of queries directed at individuals who are not themselves surveillance targets applies with equal force to querying U.S. person communications acquired in the Section 702 program. As discussed above, the incidental collection of information through a Title III wiretap meets Fourth Amendment standards based on the prior judicial review, showing of probable cause, and particularity in the wiretap order, which justifies the surveillance both with respect to known suspects and with respect to incidental interceptees.\textsuperscript{560} Under Section 702, by contrast, there is no probable cause or other individualized finding by a judge — either with regard to the non-U.S. person who is the target of the surveillance or the American who communicates with the target. Nor is there any judicial review after the fact of targeting decisions or queries. It is troubling to allow the government without some form of judicial approval to compile and review private communications by U.S. persons who have not consented to the government’s collection. To address these constitutional concerns, more robust safeguards should be

\textsuperscript{559} Samson v. California, 547 U.S. 843, 848 (2006).

required at the query stage, whenever the government seeks to conduct queries seeking information about U.S. person’s communications, in order to support the reasonableness of the program. Existing query standards, which require no outside review, are insufficient to compensate for the lack of judicial review at the front end so as to provide assurance about the legitimacy and scope of the collection. On the other hand, judicial review would not be necessary for queries seeking communications of U.S. persons who are already approved as targets for collection under Title I or Sections 703/704 of FISA and identifiers that have been approved by the FISA court under the “reasonable articulable suspicion” standard for telephony metadata under Section 215.\textsuperscript{561} As a result, this would not restrict queries regarding U.S. persons who are already suspected terrorists and are under surveillance.

The statutory framework of FISA further supports the need for enhanced safeguards for U.S. person information. The definition of foreign intelligence information under FISA, which is incorporated by reference into Section 702, sets forth several categories of information, including information regarding international terrorism or international proliferation of weapons of mass destruction. To meet the statutory definition, the information generally must “relate to” one of the listed categories, but if the information concerns a U.S. person, the definition specifically requires that the information must “be necessary to” the ability of the United States to protect against these threats.\textsuperscript{562} At the query stage, this definition is relevant because the NSA minimization procedures require that queries using U.S. person identifiers must be reasonably likely to return foreign intelligence information. We believe that foreign intelligence information in the query context must track the statutory definition, which, for U.S. persons, involves the higher “necessary” standard.

When FISA was originally enacted, Congress made clear in passing the statute that enhanced safeguards were needed for U.S. person information. As the report of the House Permanent Select Committee on Intelligence explained:

[T]he committee has adopted a definition of foreign intelligence information which includes any information relating to these broad security or foreign relations concerns, so long as the information does not concern U.S. persons. Where U.S. persons are involved, the definition is much stricter; it requires that the information be “necessary” to these security or foreign relations concerns.

\textsuperscript{561} It would also not be necessary if the query produces no results or the analyst purges all results from the given query as not containing foreign intelligence.

\textsuperscript{562} 50 U.S.C. § 1801(e) (emphasis added).
Where the term “necessary” is used, the committee intends to require more than a showing that the information would be useful or convenient. The committee intends to require a showing that the information is both important and required. The use of this standard is intended to mandate that a significant need be demonstrated by those seeking the surveillance. For example, it is often contended that a counterintelligence officer or intelligence analyst, if not the policymaker himself, must have every possible bit of information about a subject because it might provide an important piece of the larger picture. In that sense, any information relating to the specified purposes might be called “necessary” but such a reading is clearly not intended.\(^{563}\)

To give effect to this definition of foreign intelligence information under FISA, and the cautionary words from both the House and Senate reports, we believe that the approval process for U.S. person queries under Section 702 must be tightened. The more stringent “necessity” test for foreign intelligence information relating to U.S. persons requires that queries seeking to identify incidentally collected communications of an American must be reasonably designed to produce information necessary to the ability of the United States to protect against the listed threats, or to assure the defense or security of the United States or the conduct of its foreign affairs. It is imperative that a process be instituted to assure compliance with this definition.

Finally, as a policy matter, we seek to find the appropriate balance that will enable the government to pursue its legitimate foreign intelligence purposes while still safeguarding legitimate privacy interests. The government urges that once information has been lawfully collected, it may be used for any lawful purposes, and that existing minimization rules under Section 702 provide sufficient safeguards against improper use. In contrast, on June 19, 2014, the U.S. House of Representatives, by a 293-to-123 bipartisan vote, approved a ban on U.S. person queries under Section 702.\(^{564}\) The President’s Review Group on Intelligence and Communications Technologies, many advocacy organizations, certain members of Congress, and others have urged that in order to conduct a U.S. person query of Section 702 data, the government should be required to obtain a FISA warrant under Title I of the statute and demonstrate probable cause that the U.S. person is a foreign power or an agent or employee of a foreign power. Last week, a federal district court judge noted that whether the Fourth Amendment requires a warrant for queries to be conducted


of Section 702 data was “a very close question.” He ultimately ruled the Fourth Amendment did not require a warrant even though such a requirement might “better protect Americans’ privacy rights.” We believe that the middle course we propose — not banning queries or requiring a warrant but instead requiring judicial approval of queries employing a more relaxed standard — more appropriately balances the government’s legitimate foreign intelligence purposes with the privacy rights of Americans.

With regard to query results, it is important on both legal and policy grounds for the government to implement procedures under which Section 702 communications are reviewed to assess whether they meet the statutory definition of foreign intelligence information applicable to U.S. persons no later than when the results of a U.S. person query are generated, to insure that only those meeting the “necessary” standard are used, retained or disseminated and those not meeting the definition are purged. At base we believe some external oversight of the review process is essential to counteract an understandable but strong reluctance of analysts to give up any information that might conceivably have some future remote value, despite the more restrictive statutory definitions of foreign intelligence for Americans’ information.

While we conclude that a particularized judicial finding should be required before a U.S. person query has been made, to ensure that it has a proper basis, we believe the FISA Title I standard for targeting is too demanding in the query context. Rather, the

---

566 We recognize that some communications of Americans may never be returned as the result of a query or otherwise reviewed before they are “aged-off” of agency systems at the end of the data retention period.
567 One alternative in that regard would be for the FISA court to use a special master with a security clearance to regularly review representative samples of query results. The master would assess whether information that does not meet the statutory definition of foreign intelligence information had been properly purged and report to the court on the master’s findings. See In re U.S. Dep’t of Defense, 848 F.2d 232, 239 (D.C. Cir. 1988) (“[W]here a massive number of classified documents exists such that the judge and his law clerk simply cannot examine them all . . . appointment of a master to structure the judge’s review of these documents is appropriate so long as the judge retains decisional authority over the issue in question.”). If the FISA court concluded over time that the review and purging process was working properly, this review process could be relaxed or suspended. If, on the other hand, the FISA court, based on the master’s report, concluded that Americans’ communications were not being properly minimized, the court would have discretion to expand its oversight of this process to insure that the privacy interests of Americans with regard to non–foreign intelligence communications were being protected. There is some similarity between this proposal and the operation of federal wiretaps. Under federal law, “[i]mmediately upon the expiration of the [wiretap order] recordings shall be made available to the judge issuing such order and sealed under his directions.” 18 U.S.C. § 2518(8)(a). This allows the court to assure itself that the government is getting the evidence that the warrant authorized. If the judge concludes that the government was collecting information outside of the scope of the warrant, the FISA court would be able to modify or terminate the wiretap authority or impose any other appropriate restrictions.

The ultimate goal of this would be to align agency practice with statutory and constitutional requirements.
government should be permitted to conduct U.S. person queries so long as the FISA court finds that the U.S. person identifier was reasonably likely to return foreign intelligence information as defined under FISA. If the Board’s Recommendation 1 regarding targeting is adopted, the Section 702 program will provide sufficient front-end safeguards that we do not believe a probable cause standard is needed at the query stage. And, provided that the statutory definition of foreign intelligence information is strictly followed, including the requirement that the Americans’ information sought be “necessary to” the government’s ability to protect against international terrorism or other designated threats, we conclude that it is appropriate for the government to seek such information through U.S. person queries without demonstrating that the American in question is an agent of a foreign power.

At the end, the current system allows a U.S. person about whom there is no suspicion of being a terrorist or engaging in other illegal activity but who unknowingly corresponds with the target of a Section 702 proceeding — perhaps a relative or professional colleague or old friend — to have his or her correspondence with the target, over a period of several years, collected, reviewed at will by intelligence analysts, and retained in a FISA data bank. If the unknowing correspondent’s emails or other Internet material do display information of foreign intelligence value, it can be used as such and we have no objection to that. But without any such determination, the correspondence in toto, however private or confidential, can be stored for years and it can be queried using the unknowing correspondent’s name as a selector not only by a few but by many NSA foreign intelligence analysts. The unknowing correspondent’s information may also be used under restrictions, but nonetheless used and disseminated outside the agency in reports or provided to a foreign government — all this with no prior review beyond that conducted within the intelligence community. The possibility of such an occurrence, even if rare, does not seem to us to come near the Fourth Amendment reasonableness standard for a significant component of Section 702 or to comply with the letter and spirit of FISA. We feel strongly that a neutral and detached judicial officer should approve the use of U.S. person identifiers. That requirement traditionally has been considered a critical component of Fourth Amendment protections against overbroad searches.568 As the Supreme Court stated last week, noting the importance of judicial approval for government access to information, “the Founders did not fight a revolution to gain the right to government agency protocols.”569


II. Recommendation Regarding FBI Queries for Criminal Purposes

The Board’s unanimous Recommendation 2 states that additional limits should be placed on the FBI’s use and dissemination of Section 702 data in connection with non-foreign intelligence criminal matters. In our view, these limits should include the requirement that the FBI obtain prior FISA court approval before using identifiers to query Section 702 data to ensure that the identifier is reasonably likely to return information relevant to a criminal assessment or investigation of a crime. In response, Board Members Brand and Cook, in their separate statement, refer to the practice of FBI’s using the results of Section 702 data queries in the investigation and prosecution of crimes as largely theoretical. Yet the FBI has not only the capability to conduct such queries but has authorized them, and, in fact, criminal agents do conduct such queries routinely; the fact is that we do not know the precise number of times there is a subsequent use of any results from those queries.570

Privacy and civil liberties concerns regarding “incidentally” collected Section 702 information do not just arise when that information is used outside the FBI, such as to obtain a search warrant. The information can also be used inside the FBI to make determinations about Americans that adversely affect them, such as deciding to move from an assessment to a formal criminal investigation. A troubling precedent could be created by permitting a general search of Section 702 material, including incidental collections of innocent Americans’ private information, which was collected with no articulable suspicion and particularized judicial approval and target-specific oversight. It could have implications when it comes to general access throughout the government to big data repositories collected for a specific purpose and under specific restrictions by a particular agency. In the case of domestic criminal law enforcement, which currently operates under a painstaking structure with deep roots in the Fourth Amendment and a myriad of particularized statutes and case law, a general permission to search such protected data without any need to demonstrate even an articulable suspicion about the named selector is especially worrisome. Finally, FISA court judges, who are drawn from the ranks of federal district judges and who preside over grand jury proceedings and criminal trials, have extensive experience in evaluating what is or is not relevant evidence in a criminal

570 Board Members Brand and Cook are concerned that any justification for a query at an early stage in a criminal investigation will often be unworkable. The alternative, however, is to permit queries of innocent subjects’ Section 702 communications without even an articulable suspicion of wrongdoing or terrorist affiliations. We note also that there is nothing to support the assertion that these queries are less “intrusive” of privacy than the other techniques listed in the Attorney General’s Domestic Rules as permissible in early stage investigations, i.e., public information, online resources, volunteered information, consent searches and requested information. Federal Bureau of Investigation, Domestic Investigations and Operations Guide, § 5.9.1 (Oct. 15, 2011), available at http://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/fbi-domestic-investigations-and-operations-guide-diog-2011-version.
investigation and our proposal that they be required to do so would not rule out queries essential to an investigation.

We do not anticipate that requiring judicial approval for queries in ordinary crime situations will erect any serious impediment to law enforcement. On the other hand, Board Members Cook and Brand’s suggestion that FBI agents be allowed to use Section 702 data without judicial approval not only in the investigative stage but, with approval by Department of Justice officials, as the basis for a warrant or grand jury subpoena, raises the substantial statutory and constitutional questions discussed above.

Our proposal will not ban any queries regarding U.S. persons or others in investigations of either foreign intelligence or domestic crimes, but rather would interpose a time honored protection of approval by a detached judicial officer of government access to Americans’ communications. This is the minimal protection that should be afforded to U.S. persons who have done nothing to merit forfeiture of all Fourth Amendment protection to their private papers.
ANNEX B

Separate Statement by Board Members Rachel Brand and Elisebeth Collins Cook

I. The Program is Legal and Effective

We hope that the length of the Board’s report and its comprehensive discussion of the legal considerations surrounding the program will not obscure the Board’s unanimous bottom-line conclusion: The core Section 702 program is clearly authorized by Congress, reasonable under the Fourth Amendment, and an extremely valuable and effective intelligence tool.

To the extent that the Board had concerns about the program after our thorough review, they focused primarily on two particular aspects to the program’s current operation: the practice of searching the database using a U.S. person identifier, and so-called “about” collection, both of which are discussed at length in the Board’s report. The Board makes a few targeted recommendations to address concerns raised by these two aspects of the program. We stress that these are policy-based recommendations designed to tighten the program’s operation and ameliorate the extent to which these aspects of the program could affect the privacy and civil liberties of U.S. persons. We do not view them to be essential to the program’s statutory or constitutional validity.

II. Queries of Section 702 Information

The extent to which additional restrictions should apply to agencies’ ability to query information collected pursuant to Section 702 using U.S. person identifiers has divided the Board. In the case of the FBI, this issue is intertwined with questions about querying Section 702 information for non–foreign intelligence purposes, the potential use of Section 702 information in criminal proceedings, and longstanding efforts to ensure information sharing within the agency. Specifically, the Board grappled with what to do about the fact that it is theoretically possible for a database query by an FBI analyst in a non–foreign intelligence criminal matter to return Section 702 information and for this information to be further used in the investigation and prosecution of that crime. In addressing this issue, we believe it important to adopt a policy that matches the scope of the problem, can work as a practical matter, and will not unnecessarily impair the government’s ability to conduct counterterrorism and other national security–related investigations.

---

571 The FBI receives only a small portion of Section 702 information and receives no information collected upstream. See Letter from Deirdre M. Walsh, Director of Legislative Affairs, to Hon. Ron. Wyden, United States Senate (June 27, 2014) (responding to question regarding number of queries using U.S. person identifiers of communications collected under Section 702).
The concern: As discussed at length in the Board’s Report, Section 702 collection differs from traditional electronic surveillance in a few key ways, including a lower standard for collection and the absence of a particularized judicial finding for targeting decisions. Moreover, Section 702 has an explicit foreign intelligence purpose requirement for authorized collection, consistent with the longstanding distinction between foreign intelligence and criminal purposes reflected elsewhere in FISA. Given these factors, our key concerns were the querying of Section 702 collection for non–foreign intelligence purposes, and the potential subsequent use of that information to further a non–foreign intelligence criminal investigation or prosecution.\(^{572}\)

Scope: According to initial information provided by the FBI, it seems clear that FBI agents and analysts routinely conduct queries across all FBI databases in non–foreign intelligence investigations and assessments. This is unsurprising, given that the FBI has traditionally considered the querying of information already within its possession to be among the least intrusive investigative techniques available, and the agency’s overall efforts since 9/11 to foster information sharing and eliminate stovepipes. But the story is far different for the potential use of Section 702 information in the investigation or prosecution of non–foreign intelligence crimes. We are unaware of any instance in which a database query in an investigation of a non–foreign intelligence crime resulted in a “hit” on 702 information, much less a situation in which such information was used to further such an investigation or prosecution.

Our proposal: As stated in the Board’s Report, we would not place limitations on the FBI’s ability to include its FISA database among the databases queried in non–foreign intelligence criminal matters. We believe that querying information already in the FBI’s possession is a relatively non-intrusive investigative tool, and the discovery of potential links between ongoing criminal and foreign intelligence investigations is potentially critical to national security.\(^{573}\) Instead, we would require an analyst who has not had FISA training to seek supervisory approval before viewing responsive Section 702 information, to ensure that the information continues to be treated consistent with applicable statutory and court-imposed restrictions.

We believe that placing some additional limitations on the use of Section 702 information in non–foreign intelligence criminal matters may also be warranted because of the increased civil liberties concerns raised by the use of FISA information outside the foreign intelligence context. Conceptually, the appropriate point at which to potentially limit the use of that information is where it could infringe on a person’s liberty by, for

---

example, being used as the basis for obtaining a search warrant, wiretap, or other intrusive investigative tool, as the basis for a criminal indictment in a grand jury proceeding, or as evidence in a criminal prosecution. Where current policy does not already require the approval of at least the Assistant Attorney General, we would require such approval before Section 702 information could be used in these contexts.

We note that it is already very unlikely that Section 702 information would be used in this way because of the existing significant hurdles to the use of any FISA-derived information in a criminal proceeding. FISA requires the personal approval of the Attorney General, Deputy Attorney General, or Assistant Attorney General for National Security before FISA-derived information can be used as evidence at trial or in some of the more preliminary stages of the criminal process, such as before the grand jury. FISA also requires that criminal defendants be notified if FISA-derived information will be used against them in a criminal proceeding. And since any decision to use Section 702 information risks revealing the intelligence community’s sources and methods, there is always a strong disincentive to permit it. The hurdles imposed by these existing requirements result in Section 702 information being used rarely in the prosecution of even national security–related crimes, and perhaps never in the prosecution of other crimes. As such, our proposal would not create an entirely new and unknown set of rules, but would build an added level of protection for civil liberties into the existing structure.

Concerns with requiring court approval prior to querying: Chairman Medine and Member Wald would require the FBI to obtain FISC approval prior to querying FISA-obtained information, regardless of whether the query relates to a U.S. person, and even in the investigation of foreign intelligence crimes such as terrorism or espionage. For an FBI query for foreign intelligence purposes (not including investigation of foreign intelligence crimes), the FISC would have to first determine that the query was likely to return foreign intelligence information. For an FBI query in the investigation of any crime—including foreign intelligence crimes—the FISC would have to first determine that the query was likely to return evidence relevant to the investigation. We have significant concerns

574 See Memorandum from Michael B. Mukasey, Attorney General, to all Federal Prosecutors, Revised Policy on the Use or Disclosure of FISA Information, at 2-7 (January 10, 2008).
576 Id. at §1806(c). We note that the Department of Justice has recently clarified its view of when information used in a criminal proceeding may be “derived from” prior Title VII FISA collection. See, e.g., United States v. Mohamud, No. 3:10-CR-475 slip op. at 3 (D. Or. June 24, 2014) (quoting government filing). In addition, the Department’s FISA Use Policy imposes additional restrictions to the use of Section 702 information in the context of more routine criminal investigative activities.
577 Foreign intelligence investigations routinely encompass foreign intelligence crimes. How the FBI or the FISA Court would determine which of these standards applied is unclear.
about the implications of this approach, which would likely have significant detrimental consequences far greater than acknowledged (or perhaps intended) by our colleagues.

First and foremost, although the apparent motivation of this proposal is to protect U.S. persons, it could not be limited to U.S. persons in practice. The FBI (our domestic law enforcement agency) naturally does not distinguish between U.S. persons and non-U.S. persons, which means this proposed requirement would apply by default to all queries of the FISA database, by all FBI personnel, in any FBI investigation of any crime. And requiring the FBI to determine whether the subject of a query is a U.S. person could result in more intrusive investigation of that person than would otherwise occur.  

Similarly, although the motivation of the proposal is to address incidental collection of U.S. person information through the Section 702 program, the FBI currently combines all FISA-obtained information in one database, which means that as a practical matter the proposal would prohibit the FBI from searching any FISA-obtained information without first obtaining a court order.

Although Chairman Medine and Member Wald reference a requirement for “judicial approval for queries in ordinary crime situations,” the text of their proposal covers even foreign intelligence crimes, meaning that an FBI agent investigating an al Qaeda operative for terrorism would have to go to the FISA court to run a query of any FISA-obtained information. Requiring the FBI to undertake the lengthy and burdensome FISC approval process before an FBI analyst could even query the information would create practical challenges so daunting that it likely never would be pursued. Even if the FBI could obtain prior approval, this would result in significant delay of the investigation and potentially enormous burdens on the FISC. The practical effect of this proposal would be to prevent the FBI from using one of our most valuable foreign intelligence tools to investigate foreign intelligence crimes. It is hard to imagine adopting a rule that is so at odds with the recommendations of the 9/11 Commission, the Webster Commission, and others in the years following 9/11.

In addition to requiring judicial approval, the proposal would impose a standard for the court’s approval in investigations of crime that would be unworkable in many circumstances. Database queries are often used at the earliest stages of an investigation—such as during an assessment, perhaps to follow up on a tip. At this stage, an analyst knows very little and conducts a query to see if there is anything at all that creates a reason to

---

578 Although apparently grounded in Fourth Amendment principles, the proposal makes no distinctions between contents of communications and metadata—as to which there is no currently recognized Fourth Amendment interest.

further pursue the investigation. It is hard to imagine the basis on which the FISC could assess what, if anything, will be returned in a database query at this stage, which would require the FISC to deny the application.

Finally, the proposal could actually exacerbate civil liberties concerns in at least two respects. First, a query of information already in the FBI’s possession has been considered one of the least intrusive investigative means available, and is therefore one of the first steps taken in any assessment or investigation. But now in order to use this preliminary investigative tool, our colleagues would require the FBI to assemble information sufficient to facilitate meaningful judicial review, which will inevitably require the use of more intrusive means. Second, because queries at the early stages of an investigation are often used to eliminate individuals from suspicion, discouraging queries could prevent the discovery of exculpatory information that otherwise might establish an individual’s innocence.

**NSA and CIA:** Our colleagues also would require prior court approval for NSA and CIA queries of Section 702 information when they involve U.S. person identifiers. Based on our review of the current use and extensive oversight of U.S. Person queries at the NSA and CIA, which we have accurately characterized at “rigorous,”\(^{580}\) the majority has declined to recommend such a requirement.\(^{581}\)

---

\(^{580}\) Board Report at Recommendation 4.

\(^{581}\) We are also concerned about the potential implications of Chairman Medine and Member Wald’s proposal regarding minimization. To the extent that their approach requires an analyst to review U.S. Person communications that the analyst would not otherwise review, we think it far from clear that it is more protective of privacy than leaving those communications in the database unreviewed until the end of the retention period.
ANNEX C
AGENDA OF PUBLIC WORKSHOP
HELD ON JULY 9, 2013

Link to Workshop transcript:

http://www.pclob.gov/All%20Documents/July%209,%202013%20Workshop%20Transcript.pdf
AGENDA

09:00 Doors Open

09:30 – 09:45 Introductory Remarks (David Medine, PCLOB Chairman)

09:45 – 11:30 Panel I: Legal/Constitutional Perspective
Facilitators: Rachel Brand and Patricia Wald, Board Members
Panel Members:
- Steven Bradbury (Formerly DOJ Office of Legal Counsel)
- Jameel Jaffer (ACLU)
- Kate Martin (Center for National Security Studies)
- Hon. James Robertson, Ret. (formerly District Court and Foreign Intelligence Surveillance Court)
- Kenneth Wainstein (formerly DOJ National Security Division/White House Homeland Security Advisor)

12:30 – 2:00 Panel II: Role of Technology
Facilitators: James Dempsey and David Medine, Board Members
Panel Members:
- Steven Bellovin (Columbia University Computer Science Department)
- Marc Rotenberg (Electronic Privacy Information Center)
Ashkan Soltani (Independent Researcher and Consultant)
Daniel Weitzner (MIT Computer Science and Artificial Intelligence Lab)

2:00 – 2:15 Break

2:15 – 4:00 Panel III: Policy Perspective
Facilitators: Elisebeth Collins Cook and David Medine, Board Members

Panel Members:
- James Baker (formerly DOJ Office of Intelligence and Policy Review)
- Michael Davidson (formerly Senate Legal Counsel)
- Sharon Bradford Franklin (The Constitution Project)
- Elizabeth Goitein (Brennan Center for Justice)
- Greg Nojeim (Center for Democracy and Technology)
- Nathan Sales (George Mason School of Law)

4:00 – 4:10 Break

4:10 – 4:30 Open for Public Comment

4:30 Closing Comments (David Medine, PCLOB Chairman)

Affiliations are listed for identification purposes only.
ANNEX D

AGENDA OF PUBLIC HEARING

HELD ON NOVEMBER 4, 2013

Link to Hearing transcript:

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD
PUBLIC HEARING

Consideration of Recommendations for Change:
The Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act
November 4, 2013

Renaissance Mayflower Hotel – Grand Ballroom
1127 Connecticut Ave NW, Washington DC

AGENDA

08:45  Doors Open

09:15 – 09:30  Introductory Remarks (David Medine, PCLOB Chairman, with Board Members Rachel Brand, Elisebeth Collins Cook, James Dempsey, and Patricia Wald)

09:30 – 11:45  Panel I: Section 215 USA PATRIOT Act and Section 702 Foreign Intelligence Surveillance Act

  ▪ Rajesh De (General Counsel, National Security Agency)
  ▪ Patrick Kelley (Acting General Counsel, Federal Bureau of Investigation)
  ▪ Robert Litt (General Counsel, Office of the Director of National Intelligence)
  ▪ Brad Wiegmann (Deputy Assistant Attorney General, National Security Division, Department of Justice)

11:45 – 1:15  Lunch Break (on your own)

1:15 – 2:30  Panel II: Foreign Intelligence Surveillance Court
• James A. Baker (formerly DOJ Office of Intelligence and Policy Review)
• Judge James Carr (Senior Federal Judge, U.S. District Court, Northern District of Ohio and former FISA Court Judge 2002-2008)
• Marc Zwillinger (Founder, ZwillGen PLLC and former Department of Justice Attorney, Computer Crime & Intellectual Property Section)

2:30 - 2:45 Break

2:45 - 4:15 Panel III: Academics and Outside Experts

• Jane Harman (Director, President and CEO, The Woodrow Wilson Center and former Member of Congress)
• Orin Kerr (Fred C. Stevenson Research Professor, George Washington University Law School)
• Stephanie K. Pell (Principal, SKP Strategies, LLC; former House Judiciary Committee Counsel and Federal Prosecutor)
• Eugene Spafford (Professor of Computer Science and Executive Director, Center for Education and Research in Information Assurance and Security, Perdue University)
• Stephen Vladeck (Professor of Law and the Associate Dean for Scholarship at American University Washington College of Law)

4:15 Closing Comments (David Medine, PLCOB Chairman)

All Affiliations are listed for identification purposes only.
ANNEX E

AGENDA OF PUBLIC HEARING

HELD ON March 19, 2014

Link to Hearing transcript:

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD
PUBLIC HEARING

Hearing Regarding the Surveillance Program Operated Pursuant
Section 702 of the Foreign Intelligence Surveillance Act

March 19, 2014

Renaissance Mayflower Hotel – Grand Ballroom
1127 Connecticut Ave NW, Washington DC

AGENDA

08:45 Doors Open

09:00 - 09:10 Introductory Remarks (David Medine, PCLOB Chairman)
Panel I: Government Perspective on Section 702 Foreign
Intelligence Surveillance Act

Panelists:

09:15 - 10:45

• James A. Baker (General Counsel, Federal Bureau of
  Investigation)
• Rajesh De (General Counsel, National Security Agency)
• Robert Litt (General Counsel, Office of the Director of
  National Intelligence)
• Brad Wiegmann (Deputy Assistant Attorney General,
  National Security Division, Department of Justice)

10:45 - 11:00 Break
Panel II: Legal Issues with 702 Foreign Intelligence Surveillance
Act

11:00 - 12:30 Panelists:

• Laura Donohue (Professor of Law, Georgetown University
  Law School)
• Jameel Jaffer (Deputy Legal Director, American Civil Liberties Union)
• Julian Ku (Professor of Law, Hofstra University)
• Rachel Levinson-Waldman (Counsel, Liberty and National Security Program, Brennan Center for Justice)

12:30 - 1:45 Lunch Break (on your own)
Panel III: Transnational and Policy Issues

Panelists:

• John Bellinger (Partner, Arnold & Porter)
• Dean C. Garfield (President and CEO, Information Technology Industry Council)

1:45 - 3:45
• Laura Pitter (Senior National Security Researcher, Human Rights Watch)
• Eric Posner (Professor of Law, University of Chicago Law School)
• Ulrich Sieber (Director, Max Planck Institute for Foreign and International Criminal Law, Freiburg/Germany)
• Christopher Wolf (Partner, Hogan Lovells)

3:45 Closing Comments (David Medine, PCLOB Chairman)

All Affiliations are listed for identification purposes only.
The Federal Register

The Daily Journal of the United States Government

56952 Federal Register/Vol. 78, No. 179/Monday, September 16, 2013/Notices

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

[Notice–PCLOB–2013–06; Docket No. 2013–0005; Sequence No. 6]

Notice of Hearing

A Notice by the Privacy and Civil Liberties Oversight Board on 10/25/2013

Action

Notice Of A Hearing.

Summary

The Privacy and Civil Liberties Oversight Board (PCLOB) will conduct a public hearing with current and former government officials and others to address the activities and responsibilities of the executive and judicial branches of the federal government regarding the government’s counterterrorism surveillance programs. This hearing will continue the PCLOB’s study of the federal government’s surveillance programs operated pursuant to Section 215 of the USA PATRIOT Act and Section 702 of Foreign Intelligence Surveillance Act. Recommendations for changes to these programs and the operations of the Foreign Intelligence Surveillance Court will be considered at the hearing to ensure that counterterrorism efforts properly balance the need to protect privacy and civil liberties. Visit www.pclob.gov for the full agenda closer to the hearing date. This hearing was rescheduled from October 4, 2013, due to the unavailability of witnesses as a result of the federal lapse in appropriations.

DATES:

Monday, November 4, 2013; 9:00 a.m.-4:30 p.m. (Eastern Standard Time).

Comments:

You may submit comments with the docket number PCLOB-2013-0005; Sequence 7 by the following method:
• *Federal eRulemaking Portal:* Go to http://www.regulations.gov. Follow the on-line instructions for submitting comments.
• Written comments may be submitted at any time prior to the closing of the docket at 11:59 p.m. Eastern Time on November 14, 2013. This comment period has been extended from October 25, 2013, as a result of the new hearing date.

All comments will be made publicly available and posted without change. Do not include personal or confidential information.

**ADDRESSES:**


**FOR FURTHER INFORMATION CONTACT:**

Susan Reingold, Chief Administrative Officer, 202-331-1986. For email inquiries, please email info@pclob.gov.

**SUPPLEMENTARY INFORMATION:**

**Procedures for Public Participation**

The hearing will be open to the public. Individuals who plan to attend and require special assistance, such as sign language interpretation or other reasonable accommodations, should contact Susan Reingold, Chief Administrative Officer, 202-331-1986, at least 72 hours prior to the meeting date.

Dated: October 21, 2013.

Diane Janosek,
Chief Legal Officer, Privacy and Civil Liberties Oversight Board.

ANNEX G

Reopening the Public Comment Period

At the March 19, 2014 public hearing, the Privacy and Civil Liberties Oversight Board (PCLOB) Chairman announced the reopening of the public comment period to allow for additional submissions in light of the information discussed and submitted during the March 19, 2014 public hearing. All comments received were posted to the PCLOB Docket No. 2013-005 and can be viewed at http://www.regulations.gov/#!docketDetail;D=PCLOB-2013-0005.
ANNEX H

Index to Public Comments received to PCLOB Docket No. 2013-005 on www.regulations.gov.
Comments Received on PCLOB Docket No. 2013-005

Can also view all entries at: http://www.regulations.gov/#!docketDetail;D=PCLOB-2013-0005

<table>
<thead>
<tr>
<th>Entity submitting comment - listed in order as they appear on docket</th>
<th>Go to URL to see comment on Docket</th>
<th>Additional details:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Network Initiative (GNI)</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0027">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0027</a></td>
<td>GNI is a multi-stakeholder group of companies, civil society organizations (including human rights and press freedom groups), investors and academics</td>
</tr>
<tr>
<td>Private individual</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0044">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0044</a></td>
<td></td>
</tr>
<tr>
<td>Nathan Sales</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0022">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0022</a></td>
<td>Panel member at PCLOB Workshop</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Name</th>
<th>Organization/Role</th>
<th>Website</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>European Digital Rights (EDRi) and the Fundamental Rights European Experts Group (FREE)</td>
<td></td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0024">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0024</a></td>
<td>EDRi is an association of 35 digital civil rights organizations from 21 European countries. FREE is an association whose focus is on monitoring, teaching and advocating in the EU.</td>
</tr>
<tr>
<td>Name</td>
<td>URL</td>
<td>Notes</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Michael Davidson- second submission</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0028">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0028</a></td>
<td>Providing the July 30th opinion of the U.S. Court of Appeals for the Fifth Circuit in In re: Application of the United States of America for Historical Cell Site Data, No. 11-20884</td>
<td></td>
</tr>
<tr>
<td>Mr Juan Fernando López Aguilar, Chair of the European Parliament’s Civil Liberties, Justice and Home Affairs Committee</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0059">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0059</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coalition of 53 groups- letter</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a> =PCLOB-2013-0005-0038</td>
<td>This is an updated coalition letter to PCLOB</td>
<td></td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------</td>
<td>--------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>The Constitution Project</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a> =PCLOB-2013-0005-0009</td>
<td>Sharon Bradford Franklin was Panel member at PCLOB Workshop</td>
<td></td>
</tr>
<tr>
<td>Computer and Communications Industry Association</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a> =PCLOB-2013-0005-0025</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Private citizen anonymous</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a> =PCLOB-2013-0005-0017</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic Frontier Foundation</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a> =PCLOB-2013-0005-0030</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BSA /The Software Alliance Computer &amp; Communications Industry Association (CCIA)/ Information Technology Industry Council (ITI)/ SIIA (Software &amp; Information Industry Association)/ TechNet</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a> =PCLOB-2013-0005-0061</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ashkan Soltani</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0039">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0039</a></td>
<td>Revised submission, was a panel member at PCLOB Workshop</td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------------------</td>
<td>--------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Private citizen anonymous</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0005">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0005</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Daniel J. Weitzner, Massachusetts Institute of Technology</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0040">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0040</a></td>
<td>Panel member at PCLOB Workshop</td>
<td></td>
</tr>
<tr>
<td>Private citizen anonymous</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0052">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0052</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information and Privacy Commissioner of Ontario, Canada, Dr. Ann Cavoukian</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0057">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0057</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy Times</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0011">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0011</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic Privacy Information Center</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0064">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0064</a></td>
<td>Marc Rotenberg was a panel member at PCLOB Workshop</td>
<td></td>
</tr>
<tr>
<td>Organization / Initiative</td>
<td>Address</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>ACLU Statement</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0032">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0032</a></td>
<td>Jameel Jaffer was a panel member at PCLOB Workshop and Hearing</td>
<td></td>
</tr>
<tr>
<td>Private citizen anonymous</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0046">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0046</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mark Sokolow</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0018">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0018</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Private citizen anonymous</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0041">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0041</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACCESS NOW</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0047">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0047</a></td>
<td>Second posting</td>
<td></td>
</tr>
<tr>
<td>Coalition letter</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0010">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0010</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Center for Democracy &amp; Technology, Gregory T. Nojeim</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0034">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0034</a></td>
<td>Gregory Nojeim was a panel member at PCLOB Workshop</td>
<td></td>
</tr>
<tr>
<td>Organization/Members</td>
<td>Link</td>
<td>Notes</td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>------</td>
<td>-------</td>
<td></td>
</tr>
<tr>
<td>Center for National Security Studies</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0060">Link</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Private citizen anonymous</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0037">Link</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brennan Center for Justice's Liberty and National Security Program</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0049">Link</a></td>
<td>Elizabeth Goitein was a panel member at PCLOB Workshop</td>
<td></td>
</tr>
<tr>
<td>Jeffrey H. Collins</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0043">Link</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jeffrey H. Collins</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0045">Link</a></td>
<td>Amended</td>
<td></td>
</tr>
<tr>
<td>Steven G. Bradbury</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0012">Link</a></td>
<td>Panel member at PCLOB Workshop</td>
<td></td>
</tr>
<tr>
<td>Human Rights Watch</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0036">Link</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>“Human rights organizations and advocates from around the world”</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0042">Link</a></td>
<td>Dozens of countries represented</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Website</td>
<td>Role</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Steven M. Bellovin</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0021">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0021</a></td>
<td>Panel member at PCLOB Workshop</td>
<td></td>
</tr>
<tr>
<td>Board of the U.S. Public Policy Council of the Association for Computing Machinery</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0026">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0026</a></td>
<td>Eugene H. Spafford was a panel member at PCLOB Hearing</td>
<td></td>
</tr>
<tr>
<td>Private citizen</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0066">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0066</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stephanie Pell</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0069">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0069</a></td>
<td>Panel member at PCLOB hearing</td>
<td></td>
</tr>
<tr>
<td>Congressman Bennie Thompson</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0071">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0071</a></td>
<td>Ranking Member, Committee on Homeland Security</td>
<td></td>
</tr>
<tr>
<td>Government Accountability Project</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0072">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0072</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jennifer S. Granick</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0090">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0090</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Private citizen anonymous</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0007">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0007</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization/Name</td>
<td>URL</td>
<td>Role</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>-----</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>Information Technology Industry Council</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0074">Link</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stephanie Pell</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0070">Link</a></td>
<td>Panel member at PCLOB hearing</td>
<td></td>
</tr>
<tr>
<td>BSA</td>
<td>The Software Alliance, Computer &amp; Communications Industry Association (CCIA), Information Technology Industry Council (ITI), SIIA – Software &amp; Information Industry Association, TechNet</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0067">Link</a></td>
<td>Panel member at PCLOB workshop and hearing</td>
</tr>
<tr>
<td>Jameel Jaffer</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0082">Link</a></td>
<td>Panel member at PCLOB hearing</td>
<td></td>
</tr>
<tr>
<td>Government Accountability Project</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0083">Link</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Martin Scheinin</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0085">Link</a></td>
<td>Panel member at PCLOB hearing</td>
<td></td>
</tr>
<tr>
<td>Marshall Erwin</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0089">Link</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic Frontier Foundation</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0100">Link</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Document URL</td>
<td>Role</td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------------</td>
<td></td>
</tr>
<tr>
<td>Christopher Wolf</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0087">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0087</a></td>
<td>Panel member at PCLOB hearing</td>
<td></td>
</tr>
<tr>
<td>Thomas Drake</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0102">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0102</a></td>
<td>Panel member at PCLOB hearing</td>
<td></td>
</tr>
<tr>
<td>Laura Pitter</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0079">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0079</a></td>
<td>Panel member at PCLOB hearing</td>
<td></td>
</tr>
<tr>
<td>NSA Director of Civil Liberties</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0101">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0101</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>and Privacy Office Report on</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSA's Implementation of FISA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Section 702</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Laura K. Donohue</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0075">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0075</a></td>
<td>Panel member at PCLOB hearing</td>
<td></td>
</tr>
<tr>
<td>Julian G. Ku</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0086">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0086</a></td>
<td>Panel member at PCLOB hearing</td>
<td></td>
</tr>
<tr>
<td>PEN American Center</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0094">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0094</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Eric A. Posner</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0081">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0081</a></td>
<td>Panel member at PCLOB hearing</td>
<td></td>
</tr>
<tr>
<td>Hogan Lovell</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0088">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0088</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>National Association of Criminal</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0091">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0091</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Defense Lawyers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Organization</td>
<td>URL</td>
<td>Position</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Ben Davis</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a></td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a></td>
<td>Panel member at PCLOB hearing</td>
</tr>
<tr>
<td>Amnesty International USA</td>
<td>USA and the American Civil Liberties Union</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a></td>
<td></td>
</tr>
<tr>
<td>Brennan Center for Justice</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a></td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a></td>
<td></td>
</tr>
<tr>
<td>Christopher Wolf</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a></td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a></td>
<td>Panel member at PCLOB hearing</td>
</tr>
<tr>
<td>Kevin Cahill</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a></td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a></td>
<td></td>
</tr>
<tr>
<td>The Constitution Project</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a></td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a></td>
<td></td>
</tr>
<tr>
<td>Center for Democracy &amp;</td>
<td>Technology</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a></td>
<td></td>
</tr>
<tr>
<td>Dean C. Garfield</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a></td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a></td>
<td>Panel member at PCLOB hearing</td>
</tr>
<tr>
<td>Laura Donohue</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a></td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a></td>
<td>Panel member at PCLOB hearing</td>
</tr>
<tr>
<td>Center for National Security</td>
<td>Studies</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a></td>
<td></td>
</tr>
<tr>
<td>John B. Bellinger, III</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a></td>
<td><a href="http://www.regulations.gov/#!documentDetail;D">http://www.regulations.gov/#!documentDetail;D</a></td>
<td>Panel member at PCLOB hearing</td>
</tr>
<tr>
<td>Name</td>
<td>Website</td>
<td>Role</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Rachel Levinson-Waldman</td>
<td><a href="http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0080">http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0080</a></td>
<td>Panel member at PCLOB hearing</td>
<td></td>
</tr>
</tbody>
</table>
This Report is the Privacy and Civil Liberties Oversight Board’s effort to analyze and review actions the executive branch takes to protect the Nation from terrorism to ensure the proper balancing of these actions with privacy and civil liberties.
The Case for Reforming Section 702 of U.S. Foreign Intelligence Surveillance Law

To rein in the NSA’s collection, monitoring, and searching of U.S. citizens’ communications, Congress should reform section 702 of the Foreign Intelligence Surveillance Amendments Act.

June 26, 2017

On December 31, 2017, section 702 of the 2008 Foreign Intelligence Surveillance Amendments Act (FAA) will expire. Section 702 governs the domestic interception of foreigners’ communications, when the targets are believed to be outside the United States. Although externally directed, this statute is being used by agencies to monitor, collect, and search U.S. citizens’ communications for foreign intelligence and criminal activity. Congress has an opportunity to amend section 702 to safeguard U.S. national security, protect citizens, and comply with the Constitution.

Controversy marks the renewal debate. The Director of National Intelligence (DNI) states that the interception powers are vital to the intelligence community’s ability to protect the United States from foreign threats. About one quarter of the counterterrorism reports from the National Security Agency (NSA) include information derived from section 702 intercepts. Renewal is the intelligence community’s top legislative priority for 2017.

In contrast, civil liberties organizations consider the current use of section 702 to be unconstitutional. These groups, along with legal analysts and members of Congress, criticize the sheer number of Americans whose communications the NSA collects—a figure that privacy advocates estimate to be in the tens of millions. Revelations about
the interception of Donald J. Trump's campaign workers' communications with Russia have generated further concern about the potential use of surveillance for political gain.

"Section 702 violates citizens’ rights, creates a situation ripe for abuse, and undermines the balance of power."

Section 702 is an important tool in the intelligence community's arsenal. But the statute should be amended to bring it within constitutional bounds. Section 702 violates citizens’ rights, creates a situation ripe for abuse, and undermines the balance of power between the branches of government. Congress should use the renewal of section 702 to restrict the NSA's ability to obtain certain kinds of information and to retain citizens’ communications. Congress should also reinstate the “primary purpose” test (which mandates that an intercept be for foreign intelligence purposes), prevent section 702 intercepts from being used to find evidence of ordinary criminal activity, and prohibit collection of communications about (not just to or from) targets.

How Section 702 Works

Section 702 authorizes the federal government, with some statutory restrictions, to intercept electronic communications inside the United States of individuals who are not U.S. persons (that is, U.S. citizens or legal residents). According to the law, the government must reasonably believe that the targets are outside the country at the time of collection.
Section 702 differs in important ways from traditional collection under the 1978 Foreign Intelligence Surveillance Act (FISA). For the government to obtain an order to intercept domestic communications under FISA, it must demonstrate probable cause that the target of the surveillance is a foreign power or an agent of a foreign power, and that each of the facilities to be placed under surveillance is likely to be used by the target. The statute generally defines “foreign power” as a foreign government, a foreign entity or political organization, or a group engaged in terrorism. For a U.S. person to be an agent of a foreign power, some level of suspected involvement in criminal activity is necessary.

Section 702, in contrast, is not subject to the same Fourth Amendment constraints, primarily because the statute targets foreigners overseas. The law, for instance, does not require the government to obtain an order specifying the person or place that it plans to target. Instead, the decision is left to the attorney general and the DNI, so long as the target is reasonably believed to be a non–U.S. person and outside the United States and collection meets the certification requirements. Specifically, the government must certify that targeting and minimization procedures—which are designed to minimize the acquisition and retention and prohibit the dissemination of information about U.S. persons that is not publicly available—meet the statutory requirements and that “a significant purpose” of the acquisition is to gather foreign intelligence. The Foreign Intelligence Surveillance Court (FISC) then determines whether the procedures comply with the law.
Once the certification has been approved, the government identifies targets for surveillance. It obtains their communications either from equipment placed at strategic locations on the U.S. internet and telecommunications infrastructure (referred to as upstream collection), or from U.S.-based service providers such as Google, Microsoft, and Apple (called downstream or PRISM collection). Section 702 prohibits backdoor searches—that is, targeting non-U.S. persons overseas with the intent of placing U.S. persons under surveillance.

In 2013, former NSA contractor Edward Snowden leaked documents to the press revealing that the agency was using section 702 to collect massive amounts of data, including U.S. persons’ communications. The DNI and the Privacy and Civil Liberties Oversight Board (PCLOB) later confirmed the NSA’s upstream and downstream collection programs. The programs—directed at foreign countries, international organizations, groups, and individuals—implicated substantial numbers of targets. According to the DNI, the one order issued under section 702 in 2013 affected around 89,000 targets. By 2015, the number of targets had reached nearly 95,000.

The NSA obtained not only messages to or from these targets, but also, for upstream collection, data about the target (or selectors associated with the target) known as “about collection.” In addition, the agency collected every message in a multi-communication transaction (MCT)—a communication containing more than one
message—linked to a collectable communication. This included U.S. persons’ communications, even when they were not sending a message to or from the target. It also led to the collection of entirely domestic conversations between citizens, unrelated to foreign intelligence.

The extent of such incidental collection appears to be significant: In 2014 the Washington Post reported that the NSA was collecting far more data on ordinary internet users than on legally targeted foreigners. In the files examined, nine out of ten account holders in a cache of intercepted conversations were not themselves a target, but simply caught up in the agency’s net. Nearly half of the files contained names, email addresses, and other details linked to U.S. persons.

Each agency maintains its own procedures for what it does with communications collected by the NSA under section 702. The NSA, CIA, FBI, and National Counterterrorism Center query downstream information for foreign intelligence purposes—broadly defined to include anything related to “the foreign affairs of the United States”—using U.S. persons’ information.

In 2011, the NSA was forbidden from querying upstream communications using information about U.S. persons. Five years later, FISC found out that the NSA had violated the rule “with much greater frequency” than it had previously disclosed. Citing the “lack of candor” and the “serious Fourth Amendment” issues at stake, FISC focused on U.S.-person queries of MCTs obtained in the collection of communications about targets—the kind of collection that was capturing domestic communications. Unable to separate these conversations from conversations to or from targets, the NSA announced in April 2017 that it would cease “about collection.” Simultaneously, the NSA expanded its authority to query all upstream data using U.S. persons’ information, bypassing the previous restraint.
The FBI’s minimization procedures allow it to query section 702 data to look for evidence of criminal activity. It can collect, analyze, and disseminate the data, even if it relates to highly sensitive personal matters such as sexual conduct; political activities (including “discussions with Members of Congress and their staff”); consulting with clergy; and psychiatric and medical appointments. In 2014 the PCLOB reported that the FBI frequently uses this power without registering its queries, making it impossible to track how often the FBI searches Americans’ communications without a warrant—a statement the DNI later verified.

In 2015, Congress made a modest effort to identify what appeared to be de facto backdoor searches, requiring the DNI to release the number of queries involving U.S. persons. In 2016, DNI reported 4,672 search terms used to query content that had not gone through minimization procedures, and 23,800 queries of un-minimized metadata by the NSA and CIA. The number omitted FBI searches.

**Constitutional Issues Raised by Section 702**

cfr
The most trenchant criticism of section 702 acquisition is that it violates the Fourth Amendment, which establishes “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable search and seizure.” The purpose of this clause was to prohibit general warrants, even as the clause that followed specified what would be required for a particularized warrant to be valid: it must be based “upon probable cause, supported by Oath or affirmation, and particularly [describe] the place to be searched, and the persons or things to be seized.”

Although section 702 theoretically prohibits the collection of Americans’ communications, in practice it acts as a general warrant. Using section 702, the intelligence community monitors and collects Americans’ international communications, as well as entirely domestic conversations, without oath or affirmation of wrongdoing. It does not apply to a particular person or place, nor does it specify the records to be obtained. A target may be in another country, but when the person on the other side is a U.S. person, then Americans’ rights are affected. Agencies are not required to delete their records of U.S. persons’ communications. To the contrary, they can be kept and queried to look for unrelated criminal activity—even though they are being collected without the ordinary protections that accompany Fourth Amendment searches.

The NSA has aggravated the constitutional problem by adopting practices that increase access to citizens’ communications. Unless evidence exists that the target is a U.S. person or is inside the country, the agency assumes these criteria are met, meaning that potentially all communications to and from the United States can be monitored and collected. This practice raises further First Amendment concerns relating to the freedom of association and freedom of religion, as well as historic Fifth Amendment rights.

cfr
There is also the risk that the executive branch will use section 702 to monitor political opposition. Watergate aside, history is replete with examples of executive power wielded inappropriately. In the 1960s, the NSA’s Project MINARET began by focusing on individuals traveling to Cuba. By the time the program ended in 1973, it was directed at civil rights leaders and anyone suspected of criminal activity. CIA programs have intercepted the international communications of members of Congress, as well as political candidates, while the FBI’s COINTELPRO actively sought to discredit and undermine political adversaries.

The myriad noncompliance issues with section 702 demonstrate the inability of the agencies to abide by the rules set by FISC. With so much information concentrated in one place, the program is ripe for abuse.

“Congress should require the NSA to delete communications that are exclusively between U.S. persons.”

Too much power in the executive branch is especially problematic, as it threatens the separation of powers. In the past, the executive branch has used surveillance and false criminal charges to undermine the operation of the other branches in their constitutional duties.

Under section 702, moreover, the judiciary is not involved in the targeting decisions either at the time of collection or subsequently. The executive branch determines when \( c \vec{p} \) query the databases using U.S. persons’ information and what to do with the data.
The process of parallel construction, whereby law enforcement agencies recreate the evidentiary trail, means that section 702 data rarely makes it into court. The result constrains judicial power.

**Recommendations for Revising Section 702**

Intelligence collection is vital for U.S. national security. It is equally critical that the country adheres to constitutional limits to protect rights, allow for political opposition, and ensure the separation of powers. Four important steps would help to move the law in the right direction.

First, Congress should require the NSA to delete communications that are exclusively between U.S. persons, and to obtain a court order to retain conversations to which a U.S. person is party, bringing collection into conformity with traditional FISA procedures. These minimization procedures are necessary to protect citizens affected by targeting decisions. Currently, as long as the data was not acquired in a way that violates the statutory targeting conditions, the intelligence community may retain citizens’ communications. Congress should require the intelligence community to follow traditional FISA rules, which mandate that U.S. persons’ information obtained from the warrantless interception of communications generally must be destroyed.

Second, section 702 should be amended to prohibit U.S. person queries unless they are subject to a procedure akin to those outlined by FISA: an individualized order from FISC supported by probable cause that the information to be obtained is relevant to foreign intelligence. In addition, queries should be limited to foreign intelligence collection and not extended to ordinary criminal activity. This alteration is critical to ensure that section 702 does not become a way to circumvent the Fourth Amendment.
Third, Congress should reinstate the “primary purpose” test, replacing the language added in 2008 requiring that only “a significant purpose” be for foreign intelligence. If the primary purpose is criminal, then the government should go through existing procedures for collecting evidence of a crime, such as obtaining a warrant for a wiretap, and not through foreign intelligence collection authorities.

Fourth, the statute should contain a prohibition on “about collection” to prevent the NSA from collecting messages mentioning targets. Congress should similarly prohibit the NSA from collecting MCTs unless it obtains only messages to or from the target, deleting other bundled messages. This alteration creates an incentive for the NSA to find a way to protect U.S. persons’ messages.

These would be necessary first steps in bringing section 702 within constitutional bounds. Congress might also consider other proposals, such as prohibiting parallel construction (wherein the NSA passes section 702 information to law enforcement agencies, who construct alternative evidentiary trails), specifying what “derived from” in section 702 means (to facilitate judicial challenges), and preventing citizens’ metadata collection.

---

This Cyber Brief is part of the Digital and Cyberspace Policy program. The Council on Foreign Relations takes no institutional positions on policy issues and has no affiliation with the U.S. government. All views expressed in its publications and on its website are the sole responsibility of the author or authors.
The Fourth Amendment in a Digital World

Laura K. Donohue
Georgetown University Law Center, lkd27@georgetown.edu

This paper can be downloaded free of charge from:
http://scholarship.law.georgetown.edu/facpub/1791
http://ssrn.com/abstract=2836647

THE FOURTH AMENDMENT IN A DIGITAL WORLD

LAURA K. DONOHUE*

I. Introduction ............................................. 554
II. Literal Reading of the Text ............................ 560
   A. Houses ............................................. 561
   B. Papers ............................................. 568
   C. Voice Communications ............................. 573
III. Private versus Public Space ......................... 581
   A. Open Fields, Naked Eye ............................ 582
   B. Aerial Surveillance ................................. 589
   C. Radio-frequency Enabled Transmitters .......... 594
   D. Global Positioning System Technology .......... 599
   E. Enhanced Detection ................................. 609
   F. Technological Challenges to the Private/Public Distinction ................. 612
      1. Digital Tracking ................................. 613
      2. Recording and Analysis: Informants and the First Amendment ............. 631
IV. Personal Information versus Third-Party Data ...... 640
   A. Information Entrusted to Others .................. 641
   B. Digital Dependence ................................. 647
V. Content versus Non-Content ........................... 650
   A. Electronic Communications .......................... 651
   B. Pen Register/Trap and Trace Devices ............. 658
   C. Envelope Information ............................... 661
VI. Domestic versus International ....................... 664
    A. Law Enforcement .................................. 666
    B. Foreign Intelligence Collection .................. 668
    C. Technological Challenges to the Domestic/International Distinction ......... 674
VII. Confronting the Digital World ....................... 678

* Professor of Law, Georgetown Law; Director, Georgetown Center on Law and National Security; Director, Georgetown Center on Privacy & Technology. Thanks to Joel Brenner, Allegra McLeod, Matthew Waxman, and participants in the Georgetown Law Faculty Workshop for their comments on an earlier version of this Article. I also am grateful to Jeremy McCabe, who provided invaluable help in securing many of the cases, laws, texts, and papers cited in this Article.
I. INTRODUCTION

Fourth Amendment doctrine no longer reflects how the world works. Technology has propelled us into a new era. Traits unique to a digital world are breaking down the distinctions on which the Court has traditionally relied to protect individual privacy.

What are these characteristics? Digital information is ubiquitous. Individuals cannot go about their daily lives without generating a footprint of nearly everything they do. The resulting data is accessible, recordable, and analyzable. And because it is digital, it can be combined with myriad sources, yielding deeper insight into our lives. Data is also non-terrestrial and borderless. Bits and bytes populate an alternative world. They may be held on a server, but their generation, transfer, and availability are not tied to territory, undermining doctrines that rely on three-dimensional space. Technology, moreover, embodies an efficiency drive. Innovation makes it possible to do more, and to do it better, faster, and cheaper than before. So more information is being captured, even as the resource expenditures required steadily decline. Simultaneously digital interfaces are rapidly proliferating, replacing traditional modes of interaction. This means that new types of information are available, even as our ability to conduct our daily lives has become heavily dependent on technology. It has become a non-option to eschew the digital world, if one wants to live in the modern age.

These characteristics undermine the distinctions that mark Fourth Amendment doctrine. Consider, for instance, the diremption between private and public space. The Court has long relied upon this dichotomy to determine what constitutes a reasonable expectation of privacy. It draws a line at the walls of the home, citing the risk assumed by individuals when they go out into public and expressing a reluctance to disadvantage law enforcement by forcing them to turn off their natural senses or to ignore what any ordinary person could ascertain.

The amount and types of information available in the public sphere, however, have exponentially increased. WiFi and Bluetooth signals can be collected, global positioning systems and vessel monitoring systems operated, and radio frequency identification chips tracked. Automated license plate readers record the time, date, and

---

location of cars, while network data reveals where mobile devices travel day and night. International mobile-subscriber identity-catchers pinpoint the devices located in a given area. Internet protocol databases, in turn, register users’ locations. Financial transactions and credit card records place people in certain places at certain times, while cameras, enhanced with remote biometric identification, may be mounted on vehicles, poles, buildings, or unmanned aerial systems, creating the potential for 24-hour monitoring, seven days a week, *ad infinitum.*

The digitization of this information means that it can be recorded and combined with biographic information and subjected to algorithmic analyses, penetrating further into citizens’ lives. Even when data is derived from the public sphere, the government’s use of it may impact free speech, the right to assemble, and religious freedom, to say nothing of personal privacy.

Technology erodes other Fourth Amendment distinctions. A series of cases in the 1970s established the contours of what would be considered “reasonable,” based on who holds the information. Data held by the individual generating it is afforded a higher level of protection, while data held by third parties, such as companies with whom one contracts for goods or services, is granted a lower level of protection. But technology has created an imbalance. Digital dependence—i.e., the degree to which we rely on digitization to live our daily lives—has radically changed the world in which we live. School, work, social interactions, hobbies, and other pursuits are now online by nature of how society functions. This has two implications. First, new kinds of information are now generated and, therefore, accessible. Second, our reliance on industry and third-party providers to service the needs of daily life has made much more of our personal information, as well as new kinds of personal data, vulnerable to government collection.

---


Another distinction centered on the *type* of information under consideration—content versus non-content—similarly collapses in the contemporary world. For years, envelope information has been considered non-content, and thus less protected than content, on the grounds that the latter, and not the former, reveals an individual’s private communications, thoughts, and beliefs. But what happens when a search engine reveals what it is that is being examined in the uniform resource locator (URL) itself? Metadata of all sorts can reveal much about an individual6—in fact, law enforcement regularly uses search terms to bring criminal charges against individuals. The reason is simple: patterns in phone calls, text messages, instant messaging, emails, or even URL visits demonstrate beliefs, relationships, and social networks—yet the form of that data (metadata) has not historically been considered content. The same is true of consumer metadata and financial records. Sophisticated pattern analytics mean that non-content morphs into content, making any formal distinction meaningless.7

5. If I were, for instance, to search for “Molotov cocktail” on Amazon.com, the URL that comes up is https://www.amazon.com/s/ref=NB_sb_noss_1?url=search-alias%3Daps&field-keywords=Molotov_cocktail. Subject-specific sites similarly indicate the content, with Wikipedia’s URL reading https://en.wikipedia.org/wiki/Molotov_cocktail.

6. See generally Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 Harv. J. L. & Pub. Pol’y 757 (2014) [hereinafter Donohue, *Bulk Metadata*] (discussing privacy issues regarding the NSA’s bulk collection of telephony metadata); Laura K. Donohue, *The Future of Foreign Intelligence* 39–53 (2016) [hereinafter Donohue, *Future*]. A helpful definition of “metadata” offered by Anne J. Gilliland is “the sum total of what one can say about any information object at any level of aggregation.” In turn, “is a digital item or group of items, regardless of type or format, that can be addressed or manipulated as a single object by a computer.” Anne J. Gilliland, *Setting the Stage*, in *Introduction to Metadata* 1, p.2 (Murtha Baca ed., 2d ed. 2008).

7. See, e.g., Swati Agarwal et al., *Open Source Social Media Analytics for Intelligence and Security Informatics Applications*, in *Big Data Analytics: 4th International
Differentiating between domestic and international communications similarly proves inapposite to the contemporary world. Communications are now global. If I email a friend from a restaurant in Boston and she reads the email while sitting at a restaurant in New York, the message may well have gone internationally, placing it under weaker Fourth Amendment standards. It is not that the privacy interest in the communication is any different than that of a traditional letter. It is simply that digitization and the advent of worldwide communications networks have narrowed my right to privacy for the same information. Or how about cloud computing, or the use of Drop Box, or Google Docs? Is all of this information fair game, so to speak, just because Google happens to hold the document in Singapore as opposed to San Francisco? The problem, as with the distinctions between private and public space, or content and non-content, has nothing to do with the interests implicated and everything to do with new technologies.

This Article explores how digitization is challenging formal distinctions in Fourth Amendment doctrine that previously have played a role in protecting the right to privacy. The purpose, consistent with the aim of the NYU Annual Survey of American Law, is to

---

8. For further discussion of the conditions under which the e-mail could be read for foreign intelligence purposes, see generally DONOHUE, FUTURE, supra note 6.

9. There are other distinctions and aspects of Fourth Amendment doctrine that this article does not consider. For instance, searches of personal devices give rise to a range of questions about the limits of plain view doctrine and ways in which such searches can be narrowed to avoid a descent into a general warrant. For a thoughtful discussion of this point, see generally Orin S. Kerr, Searches and Seizures in a Digital World, 119 HARV. L. REV. 531 (2005). The argument recurs in Orin S. Kerr, Digital Evidence and the New Criminal Procedure, 105 COLUM. L. REV. 279, 300 (2005). Another distinction made in the statutory realm is between stored communications and communications in transit, with the latter given more protections. Some commentators have argued that law enforcement has exploited this distinction to afford the type of digital information held by ISPs (photographs, email, bank records, and medical records) a lower level of protection. See, e.g., James M. O’Neil, Note, The Impact of VoIP Technology on Fourth Amendment Protections Against Electronic Surveillance, 12 INTELL. PROP. L. BULL. 35, 42–43 (2008). I do not address this directly in the Article as it is primarily a statutory concern.
provide an overview of where the doctrine has been and where it is now, with some thoughts about what direction it could go to take account of the privacy interests implicated by the digital world.\footnote{10}

This Article postulates that four Fourth Amendment dichotomies (private vs. public space; personal vs. third party data; content vs. non-content; and domestic vs. international) are breaking down in light of new and emerging technologies. The distinctions are becoming blurred. Information previously protected is no longer guarded. The categories themselves are failing to capture important privacy interests, so fewer protections are being granted at the outset. Simultaneously, the absence of use restrictions in Fourth Amendment doctrine blinds the law to the deeper privacy interests at stake. Legal doctrines that fail to recognize any privacy interest in the collection of information at the outset prove inadequate to acknowledge interests that later arise apparently \textit{ex nihilo},\footnote{11} despite the fact that more serious inroads into privacy occur with the recording of data, extended collection, and further analysis of the information. In addition, as the collection and analysis of information requires fewer and fewer resources, constraints that previously played a key role in protecting privacy are dropping away. The way in which the digital era interacts with the doctrine is steadily constricting the right to privacy. If no steps are taken to stem the tide, privacy interests will continue to narrow with significant long-term implications.

Part II of this Article begins the survey by focusing on the territorial grounding of Fourth Amendment doctrine at the founding. It describes the Court’s literal, textual reading of “houses” as matters within the home, while explaining that “papers” meant that letters sent through the post received \textit{the same protections} as items

\footnote{10. The journal, which was founded in 1942, aims to provide a comprehensive summary of developments in American law. \textit{See Mission, NYU Annual Survey of American Law, https://annualsurveyofamericanlaw.org/aboutus/} (last visited Nov. 2, 2016).}

inside the home. The doctrine hewed to a three-dimensional worldview. But with the advent of the telephone, the question of how to protect similar interests with regard to voice communications created difficulties.

Part III begins with *Katz v. United States*, which aspired to rather more than it delivered. Even as it (ostensibly) wrested reasonableness from a territorial tie, the Court entrenched the private/public distinction. The persistence of the open fields doctrine, the establishment of aerial surveillance, and the Court’s failure to acknowledge the impact of tracking technologies on personal liberty reinforced the dichotomy. Thermal scanning underscored the reliance on line-drawing in three-dimensional space. This Article focuses on location tracking to illustrate gaps in the Court’s jurisprudence that result from new technologies.

Part IV turns to the distinction between personal information and third party data, noting that the constellation of cases from the 1970s similarly fails to acknowledge the ever-deepening privacy interests of a digital age. Increasing dependence on technology means that the amount of private information at stake is considerable.

Part V considers the content versus non-content dichotomy, noting that technology is blurring the distinction. Electronic communications that convey content are not currently protected, even as areas traditionally considered to fall on the non-content side of the line, such as data from pen register (or trap and trace devices) or envelope information, provide insight into individuals’ private affairs.

Part VI focuses on the domestic versus international distinction. It begins by recognizing that the Fourth Amendment did not initially extend beyond the United States. In 1967, the Court changed course for U.S. persons overseas, granting limited protec-

---


14. See Weaver, supra note 12, at 1222 (suggesting that the post-*Katz* cases actually digressed with regard to standing doctrine, while “the Court’s post-*Katz* technology decisions are a bit more of a mixed bag. However, in a number of those cases, the Court has restrictively construed the [reasonable expectation of privacy] test;” nevertheless, the author finds some “heartening trends for privacy in some recent decisions.”).
tions. In 1990, it determined that non-U.S. persons located abroad and lacking a substantial connection to the U.S. hold no constitutional rights under the Fourth Amendment. This section contrasts the law enforcement approach with that adopted in the foreign intelligence realm, which similarly draws a line at the border. The problem comes in the form of new technologies, which doggedly refuse to recognize terrestrial boundaries. Domestic communications may now travel outside the country, simply by nature of how the Internet works. In so doing, they lose protections that they otherwise would have had, had they stayed within the country.

Part VII concludes by highlighting the importance of re-thinking the theoretical framing for the Fourth Amendment. While some commentators have suggested that legislation is the most appropriate vehicle to address Fourth Amendment concerns, it is to the Courts we must look to for relief. The questions posed by the digital age are profound. Failure to address them in a meaningful way will lead to continually narrower constitutional protections, at great cost to liberty in the United States.

II.
LITERAL READING OF THE TEXT

Fourth Amendment doctrine has long recognized the importance of protecting individuals within their homes from governmental intrusion. Prior to the 1970s, it afforded what people did in public, or made visible to others, considerably less protection. The doctrine reflected a literal reading of the text. The right of the people to be secure in their homes meant precisely that, just as the right to be secure in one’s papers afforded special protections to correspondence. Letters inside an envelope and sent through the post obtained the same protections as papers held inside the home. Once the letters were sealed and blocked from the sight of prying eyes, the fact that they were being transmitted in the mail did not alter the underlying privacy interests. Any effort to intercept and to read such documents amounted to a search, making warrantless access presumptively unreasonable.

The rationale made sense. One knew when one entered into public space that what was said and done could be seen and heard by others. If any citizen could witness others’ behavior, why should government officials, who also happened to be present, not be allowed to do the same? Similarly, one could hardly expect postal employees sorting the mail, or a postman delivering a letter, to avert their gazes from the writing on the back of a post card situated adjacent to the address. If they could see it, why shouldn’t law
enforcement? A different rule applied to correspondence hidden from public view. Taking the step to open the letter altered the behavior in question and the privacy rights entailed.

The concepts on which the distinction rested (the risk assumed by individuals doing things in public, in front of other people, and the absurdity of directing people to close their eyes, avert their gazes, or otherwise ignore their senses) became intertwined. What was visible in public to others did not fall within the protections of the Fourth Amendment. In contrast, where the government wanted to intrude on the sanctity of the home, outside of exigent circumstances, it was forced to approach a judge, to present evidence, under oath, of criminal activity, and to obtain a warrant that detailed precisely what was to be searched, or who or what would be seized, from where. Similarly, if officers wanted to read a letter located in a sealed envelope, they had to first obtain a warrant.

The line was drawn in the physical world, at the border of the home, or the parchment that made up the envelope. What was inside a home or an envelope, was de facto private, while what occurred outside the physical bounds of the home or the envelope was, with some exceptions, generally public.

A. Houses

For centuries prior to the founding of the United States, English common law afforded individuals’ homes special protections. Legal treatises detailed limits that prevented officers of the Crown from entering domiciles absent sufficient cause and/or application to a magistrate, demonstrating, under oath, probable cause of criminal activity. English jurists, lawyers, and Parliamen-

15. For discussion on the origins of the Fourth Amendment and its ties to English legal treatises and cases, see generally Laura K. Donohue, The Original Fourth Amendment, 83 U. Chi. L. Rev. 1181 (2016) [hereinafter Donohue, Original]. Chapter Four of Laura K. Donohue, The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age (2016) provides a broad overview of the founding generation’s aim in enacting the Fourth Amendment, while Chapter Five focuses on general warrants. For purposes of this Article, citations related to the original meaning of the Fourth Amendment are to the Chicago Law Review article, which goes into greater detail than the book. For individuals interested in a broader overview, see generally Donohue, Future, chs. 4, 5.

16. Id. at 1235. In 1604, Sir Edward Coke famously proclaimed in Semayne’s Case “[t]hat the house of everyone is to him as his castle and fortress, as well for his defence against injury and violence, as for his repose.” Semayne’s Case, (1604) 77 Eng. Rep. 194, 195 (K.B.), 5 Co. Rep. 91 a, 93 b. In 1628 Coke reiterated this view in his Institutes of the Laws of England: “[F]or a mans [sic] house is his castle, et domus sua casque est tutissimum refugium [and each man’s home is his safest refuge].” Sir Edward Coke, The Third Part of the Institutes on the Laws of
tarians similarly extolled the importance of protecting the home from undue government interference.\(^{17}\)

---

**England: Concerning High Treason, and Other Pleas of the Crown, and Criminal Cases** 162 (London, M. Flesher 1648). In 1736, Sir Matthew Hale underscored the protections afforded under common law, detailing the conditions under which justices of the peace, sheriffs, constables, or watchmen could breach one’s walls. See 2 Matthew Hale, The History of the Pleas of the Crown 85–95 (1736); see also Donohue, Original, supra note 15, at 1235–36 (detailing the conditions under which the home could be breached). William Blackstone in his Commentaries on the Laws of England, expounded on Coke, tying the right to be secure in one’s abode back to Ancient Rome:

> [T]he law of England has so particular and tender a regard to the immunity of a man’s house, that it stiles it his castle, and will never suffer it to be violated with impunity: agreeing herein with the sentiments of ancient Rome, as expressed in the words of Tully; ‘quid enim sanctius, quid omni religione munitius, quam domus uniuscujusque civium?’ [*For what is more sacred, what more inviolable, than the house of every citizen*] 4 William Blackstone, Commentaries on the Laws of England (Clarendon 1769) 223 (footnote omitted). William Hawkins’ Pleas of the Crown reinforced the point, citing to Hale’s conditions of entry to emphasize the special place accorded to dwellings. 2 William Hawkins, Pleas of the Crown 139 (London, Whieldon 6th ed. 1787), https://play.google.com/store/books/details?id=2qYDAAAAQAAJ&rdid=book-2qYDAAAAQAAJ&rdot=1; see also Donohue, Original, supra note 15, at 1215–17 (discussing the writings of Hale and Hawkins).

17. In Wilkes v. Wood, an action in trespass, John Glynn argued that the case “touched the liberty of every subject of this country, and if found to be legal, would shake that most precious inheritance of Englishmen.” (1763) 98 Eng. Rep. 489, 490 (C.P.); see also Donohue, Original, supra note 15, at 1199–1204 (discussing Wilkes v. Wood). Glynn protested: “In vain has our house been declared, by the law, our asylum and defence, if it is capable of being entered, upon any frivolous or no pretence at all, by a Secretary of State.” Wilkes, 98 Eng. Rep. at 490. Commenting on the award of £1000 in damages, the The London Chronicle observed, “By this important decision, every Englishman has the satisfaction of seeing that his home is his castle.” 14 The London Chronicle, 550 (Dec. 8, 1763). In Entick v. Carrington, another case brought in trespass, Charles Pratt, Chief Justice of the Common Pleas (and, from July 1765, Lord Camden), rejected the potential for a general warrant to overcome the protections otherwise afforded to dwellings. John Entick’s home had been “rifled; [and] his most valuable secrets [ ] taken out of his possession,” before he had been convicted of any crime. (1765) 19 Howell’s State Trials 1029, 1064 (C.P.). “This power so claimed by the secretary of state,” Pratt observed, “is not supported by one single citation from any law book extant. It is claimed by no other magistrate in this kingdom but himself.” Id.; see also Donohue, Original, supra note 15, at 1196–99 (discussing Entick). The reason for an absence of such authority was apparent: “The great end, for which men entered into society, was to secure their property.” Entick, 19 Howell’s State Trials, at 1066. The Chief Justice continued:

> By the laws of England, every invasion of private property, be it ever so minute, is a trespass. No man can set his foot upon my ground without my license, but he is liable to an action, though the damage be nothing; which is proved
Upon crossing the Atlantic, the American colonists expected the same protections that they held in England. When the Crown failed to respect the common law limits, the seeds of revolution were sown. In his celebrated oration in Paxton’s Case in 1761, James Otis declared, “[O]ne of the most essential branches of English liberty is the freedom of one’s house. A man’s house is his castle; and whilst he is quiet, he is as well guarded as a prince in his castle.”

The following year, John Dickinson, author of Letters from a Farmer in Pennsylvania, invoked the same ancient liberty. He attacked the Townshend Acts, which allowed the Crown to enter into “any HOUSE, warehouse, shop, cellar, or other place.” John Adams observed in 1774,

An Englishman’s dwelling House is his Castle. The Law had erected a Fortification round it—and as every Man is Party to the Law, i.e., the Law is a Covenant of every Member of society with every other Member, therefore every Member of Society has entered into a solemn Covenant with every other that he shall enjoy in his own dwelling House as compleat a security, safety and Peace and Tranquility as if it was surrounded with Walls of

by every declaration in trespass, where the defendant is called upon to answer for bruising the grass and even treading upon the soil.

Id. The sanctity of the home so permeated legal culture that the political elite spoke of it in Westminster. William Pitt (the Elder), 1st Earl of Chatham and Lord Privy Seal, declared:

The poorest man may, in his cottage, bid defiance to all the forces of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storm may enter; the rain may enter; but the King of England may not enter; all his force dares not cross the threshold of the ruined tenement.


19. John Dickinson, Letter IX, in EMPIRE AND NATION: LETTERS FROM A FARMER IN PENNSYLVANIA 51, 54 (Forrest McDonald ed., Liberty Fund Indianapolis 2d ed. 1999), http://oll.libertyfund.org/titles/690. For Dickinson, “[T]he greatest asserters of the rights of Englishmen have always strenuously contended, that such a power was dangerous to freedom, and expressly contrary to the common law, which ever regarded a man’s house as his castle, or a place of perfect security.” Id.; see also Donohue, Original, supra note 15, at 1261 (discussing Dickinson’s letter).
Brass, with Ramparts and Palisadoes and defended with a Garrison and Artillery.\textsuperscript{20}

The Fourth Amendment cemented the home as a protected sphere into the U.S. Constitution.\textsuperscript{21} It prohibited entry outside of limited circumstances absent a warrant supported by oath or affirmation relating to a named offense and particularly describing the place or persons to be searched and persons or things to be seized.\textsuperscript{22}

The common law legacy persisted in American legal thought.\textsuperscript{23} In 1833 Justice Joseph Story noted in his \textit{Commentaries on the Constitution} that the Fourth Amendment amounted to "little more than the affirmance of a great constitutional doctrine of the common law."\textsuperscript{24} Thirty-five years later Thomas Cooley wrote in his treatise: "The maxim that 'every man's house is his castle,' is made part of our constitutional law in the clauses prohibiting unreasonable searches and seizures, and has always been looked upon as of high value to the citizen."\textsuperscript{25} In 1886, Justice Bradley recalled Chief Justice Pratt’s judgment in \textit{Entick}: "The principles laid down in this opinion affect the very essence of constitutional liberty and security."\textsuperscript{26} Bradley continued:

[T]hey apply to all invasions on the part of the government and its employees of the sanctity of a man’s home and the privacies of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property.\textsuperscript{27}

\begin{thebibliography}{9}

\bibitem{22} See id. at 1193.
\bibitem{23} It also continued to be reflected in English law and legal treatises. See, e.g., Francis Lieber, \textit{On Civil Liberty and Self-Government} 60 (Theodore D. Woolsey ed., J.B. Lippincott & Co. 3d ed. 1883) ("[N]o man's house can be forcibly opened, or he or his goods be carried away after it has thus been forced, except in cases of felony, and then the sheriff must be furnished with a warrant, and take great care lest he commit a trespass. This principle is jealously insisted upon.").
\bibitem{24} Joseph Story, \textit{3 Commentaries on the Constitution of the United States} § 1895 (Boston, Hilliard, Gray & Co. 1833).
\bibitem{25} Cooley, supra note 17, at 425–26; see also Donohue, \textit{Original}, supra note 15, at 1307 (discussing Cooley's writings on the Fourth Amendment).
\bibitem{26} Boyd v. United States, 116 U.S. 616, 630 (1886); see also Donohue, \textit{Original}, supra note 15, at 1308–15 (discussing the historical and legal background of Boyd).
\bibitem{27} Boyd, 116 U.S. at 630; see also Bram v. United States, 168 U.S. 532, 544 (1897) (commenting in relation to Boyd, "[I]t was in that case demonstrated that [the Fourth and Fifth Amendments] contemplated perpetuating, in their full effi-
\end{thebibliography}
To provide a remedy for a violation of the right, in 1914 the Court adopted the exclusionary rule, prohibiting the government from using evidence obtained from an unreasonable search or seizure.\(^{28}\) The case, *Weeks v. United States*, arose from the arrest of a resident of Kansas City, Missouri.\(^{29}\) While the suspect was being held in custody, law enforcement went to his home, found a hidden key, entered the house, and conducted a search.\(^{30}\) The Court balked at the officers’ actions, as well as those of a U.S. marshal, who similarly searched the home.\(^{31}\) Neither search had been supported by a warrant.\(^{32}\) Absent a remedy, the right could not be secured. The Court explained, “[T]he Fourth Amendment . . . put the courts of the United States and Federal officials, in the exercise of their power and authority, under limitations and restraints [and] . . . forever secure[d] the people, their persons, houses, papers and effects against all unreasonable searches and seizures under the guise of law.”\(^{33}\)

Whatever position one may have on the exclusionary rule as an effective, or even a constitutional, remedy, the fact that the Court considered it necessary underscored the distinction between the


\(^{29}\) *Id.* at 387.

\(^{30}\) *Id.* at 386.

\(^{31}\) *Id.* at 386.

\(^{32}\) *Id.*

\(^{33}\) *Id.* at 391–92. A few years after *Weeks*, the Court considered a parallel fact pattern in *Silverthorne Lumber Co. v. United States*, 251 U.S. 385 (1920). Frederick Silverthorne had been indicted and arrested, and, while detained, a U.S. marshal had gone to his business and seized his books and papers. *Id.* at 390. Using the material already in its possession, the government had then drafted a new warrant to justify its actions. *Id.* at 391. The Court found that it was not permissible to allow the government to benefit from the illegal act. *Id.* at 391–92. Justice Holmes, writing for the Court, explained that allowing such actions would “reduce[,] the Fourth Amendment to a form of words. The essence of a provision forbidding the acquisition of evidence in a certain way is that not merely evidence so acquired shall not be used before the Court but that it shall not be used at all.” *Id.* at 392 (citations omitted). The Supreme Court did not apply the exclusionary rule to the states until 1961. *Mapp v. Ohio*, 367 U.S. 643, 656–57 (1961). In 1995, the Court recognized a good faith exception to the exclusionary rule. *Arizona v. Evans*, 514 U.S. 1, 14 (1995). This includes when police employees err in maintaining a database. *Herring v. United States*, 555 U.S. 135, 137 (2009). The exclusionary rule similarly does not apply where law enforcement relies on binding appellate precedent or on statutes invalidated subsequent to the search. *Davis v. United States*, 564 U.S. 229, 232, 239 (2011).
protections afforded to the private sphere, marked by the home, and public space.34

For just as the home was sacred, what happened outside the home was rather less so.35 A decade after Weeks, the Supreme Court

34. For a comprehensive article on the exclusionary rule, see generally Christopher Slobogin, The Exclusionary Rule: Is It on Its Way Out? Should It Be?, 10 Ohio St. J. Crim. L. 341 (2013). But note that over the past century, the rule has proven highly contentious both in its form and its implementation.


35. Orin Kerr, in his postulation of the equilibrium theory of the Fourth Amendment, lists as his first rule of the status quo in rule zero: “[T]he police are always free to watch suspects in public. They can walk up to suspects and monitor them at close range and ask them questions.” Orin S. Kerr, An Equilibrium-Adjustment Theory of the Fourth Amendment, 125 Harv. L. Rev. 476, 484 (2011) (footnote
declared in *Hester v. United States* that the Fourth Amendment protection of “persons, houses, papers and effects” did not extend to “open fields.”\(^ {36} \) Citing Blackstone’s *Commentaries*, Justice Holmes added, “The distinction between the latter and the house is as old as the common law.”\(^ {37} \) While the home held a special place in the law, what happened outside of it obtained fewer protections.

As the administrative state expanded, whenever the Court confronted potential exceptions, such as those that arose with regard to health inspections, the bench was closely divided.\(^ {38} \) It was only when the medical concern was sufficiently acute, and the purpose and object of the inspection sufficiently targeted, that such intrusions could be tolerated. A suspected infestation of rats would suffice; general inspection of the home’s structure would not.\(^ {39} \) Outside of any emergency situation, the unwarranted search of a

---

\(^ {36} \) Hester v. United States, 265 U.S. 57, 59 (1924). The case evolved in the shadow of the Eighteenth Amendment. U.S. Const. amend. XVIII, repealed by U.S. Const. amend. XXI. Revenue officers, hiding outside Hester’s home, saw him give a bottle of what appeared to be moonshine to another person. 265 U.S. at 58.

\(^ {37} \) *Hester*, 265 U.S. at 59 (citing 4 William Blackstone, *Commentaries* *223, 8225–826*).

\(^ {38} \) See, e.g., *Frank v. Maryland*, 359 U.S. 360 (1959) (upholding over four dissenters a Baltimore City health inspector’s search for the source of a rat infestation without a warrant). In *Ohio ex rel. Eaton v. Price*, 364 U.S. 263 (1960), the Court split evenly, leaving in place the decision of the Ohio Supreme Court upholding a housing inspector’s decision to enter a plumber’s residence without a warrant. The opinion, split four to four, is without force of precedent. But in this case, the four Justices that did not join the opinion in *Ohio* had already publicly expressed their opinion that *Frank* controlled, *id.* at 264, leading the other four Justices to write an opinion declaring *Frank* “the dubious pronouncement of a gravely divided Court” and calling for reversal, *id.* at 269.

\(^ {39} \) In the 1967 case *Camara v. Mun. Court*, the Court stated that the purpose of the Fourth Amendment, enforceable against the states through the Fourteenth Amendment, was to protect citizens against “unreasonable searches and seizures.” 387 U.S. 523, 528 (1967). Outside of carefully defined contours, an unconsented, warrantless search is *per se* unreasonable. *Id.* at 528–29. In *Camara*, the appellant had refused to allow housing inspectors access to his property in order to determine whether he was in violation of the occupancy permit. *Id.* at 525. Delivering the opinion of the Court, Justice White distinguished the case from *Frank v. Maryland*, in which the intrusion “touch[ed] at most on the periphery” of the Fourth Amendment given the importance of the municipal fire, health, and housing inspection programs designed to ensure the habitability of the structure. *Id.* at 530 (citing *Frank*, 359 U.S. at 367). In *Camara*, a general inspection was too attenuated a connection to necessity to warrant overriding the protections otherwise extended to the home. *Id.* at 533. White noted that warrantless powers of entry could be used for great mischief. Quoting *Johnson v. United States*, 333 U.S. 10, 14 (1948)
private home was per se unreasonable under the Fourth Amendment.

B. Papers

At the founding, papers in the home were subject to protections similar to those afforded to other items (and activities) within the dwelling house. Government officials could not simply cross the threshold at will to read or to seize them. Beyond this, consistent with common law, judges did not have the authority to issue search warrants to seize papers as evidence of criminal activity. This point is worth emphasizing in the contemporary environment, not least because the Director of the Federal Bureau of Investigation, in the context of the encryption debate, has taken to repeating a falsehood: that, with the appropriate process, the government has always had access to what people think, say, and write. It has not. For nearly two hundred years, the government could not obtain private papers—even with a warrant—when they were to be used as evidence of criminal activity.

(finding officers’ warrantless entry into a hotel room from which the odor of burning opium emanated unconstitutional), he wrote,

The right of officers to thrust themselves into a home is also a grave concern, not only to the individual but to a society which chooses to dwell in reasonable security and freedom from surveillance. When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or government enforcement agent. Camara, 387 U.S. at 529.

40. The history of this protection duplicates that which is detailed in Part II(A), supra. For further discussion of the special place afforded to papers, see generally Donohue, Original, supra note 15.

41. See Donohue, Original, supra note 15, at 1308–14 and infra for discussion of the mere evidence rule and its roots in common law.

In the nineteenth century, the Court extended the protection of documents to papers traveling through the post. In the 1878 case *Ex parte Jackson*, the Court considered whether a lottery circular, sent in a closed envelope, deserved Fourth Amendment protections.\(^43\) Justice Field, writing for the Court, noted that Congress’s authority “to establish post offices and post roads” extended beyond merely designating the appropriate routes, to include carriage of the mail, its safe and swift transit, and its prompt delivery.\(^44\) But while the right to carry the mail might mean that Congress could determine what could be carried *en route*, it did not give Congress the ability to *open* materials in transit.\(^45\) To read the Constitution in such a manner would give Congress the authority to override rights retained by the people.

“Letters and sealed packages . . . in the mail,” Field wrote, “are as fully guarded from examination and inspection, except as to their outward form and weight, *as if they were retained by the parties forwarding them in their own domiciles*.”\(^46\) He underscored the importance of the text: “The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be.”\(^47\) Field explained,

Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one’s own household. No law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail; and all regulations adopted as to mail matter of this kind must be in subordination to the great principle embodied in the fourth amendment of the Constitution.\(^48\)

Field recognized the close relationship between the interests protected by the Fourth Amendment and those protected by the First Amendment.\(^49\) Any restrictions on the transfer of mail also violated the freedom of the press: “[L]iberty of circulating,” Field pointed out, “is as essential to that freedom as liberty of publish-

\(^{43}\) *Ex parte Jackson*, 96 U.S. 727, 728, 733 (1877).
\(^{44}\) *Id.* at 732.
\(^{45}\) *Id.* at 733.
\(^{46}\) *Id.* (emphasis added).
\(^{47}\) *Id.*
\(^{48}\) *Id.*
\(^{49}\) *Ex parte Jackson*, 96 U.S. at 733.
ing." It meant nothing to claim that the press was free if Congress could then interfere with delivery of the newspapers, or pass laws limiting the circulation of written material.

Even as the Court allowed for private correspondence to be subject to the same protections as papers held within the home, a terrestrial test applied: documents became protected as if they still resided inside one’s domicile. Delivering the letter did not divorce it of the protections it otherwise enjoyed. In a three-dimensional world, where the government itself carried the letter, a clear line could be drawn. Absent good cause, officials could neither break into a study nor tear open an envelope en route to gain access.

*Ex parte Jackson* dealt with a lottery circular sent through the post. Other efforts to flesh out the contours of protections applied to papers followed. Just three years prior to the Court’s ruling in *Jackson*, Congress had passed a statute to prevent smuggling. The law authorized judges to direct the production of private books, invoices, and papers in revenue cases. Fourteen years later, in *Boyd v. United States*, the Supreme Court declared the provision to be unconstitutional and void. In doing so, the Court recognized the close relationship between the Fourth and Fifth amendments, noting that:

> [A] compulsory production of a man’s private papers to establish a criminal charge against him, or to forfeit his property, is within the scope of the Fourth Amendment to the Constitution in all cases in which a search and seizure would be, because it is a material ingredient, and effects the sole object and purpose of search and seizure.

The Court dismissed Congress’s effort to gain control over private papers as being almost arrogant, noting the absence of any similar effort in history, despite the egregious nature of measures implemented by the British government. “Even the act under which the obnoxious writs of assistance were issued,” the Court wrote, “did not go as far as this.” The effort to recover stolen goods, moreover, for which a warrant historically had been required, fell short of

50. Id.
51. Id. at 734.
53. Sec. 5, 18 Stat. at 187 (requiring surrender of books, invoices, and papers required in civil suits under revenue laws).
55. Id. at 622.
56. Id. at 623.
the level of intrusion now contemplated by the legislature.\footnote{57} The Court explained:

The search for and seizure of stolen or forfeited goods . . . are totally different things from a search for and seizure of a man’s private books and papers for the purpose of obtaining information therein contained, or of using them as evidence against him. The two things differ \textit{toto coelo}. In the one case, the government is entitled to the possession of the property; in the other it is not.\footnote{58}

Justice Bradley, writing for the Court in \textit{Boyd}, cited back to Coke and noted Otis’s oration in \textit{Paxton’s Case}.\footnote{59} The government could not break into an individual’s home to obtain the documents; neither could it force an individual to produce the same information, as such an action would trigger the protection against self-incrimination.\footnote{60}

\textit{Boyd} evolved into the “mere evidence” rule, which established that only criminal instrumentalities and stolen goods could be recovered by warrants consistent with the Fourth Amendment.\footnote{61} In 1917, when Congress introduced the first law giving federal law enforcement the formal authority to issue search warrants, the legislature was careful to hew to the doctrinal line.\footnote{62} It limited warrants for search and seizure to property “stolen or embezzled in violation of a law of the United States,” “used as the means of committing a felony,” or used to aid a foreign government in violating “any penal statute[.] . . . treaty or the law of nations.”\footnote{63} These reflected the rule that only the fruits or instrumentalities of crime could be obtained via warrant.

\begin{itemize}
  \item \footnote{57} Donohue, \textit{Original, supra} note 15.
  \item \footnote{58} \textit{Boyd, supra} note 54, at 623.
  \item \footnote{59} \textit{Id.} at 625, 629 (quoting \textit{Paxton’s Case}). \textit{See also supra} Part II(A).
  \item \footnote{60} \textit{See Boyd}, 116 U.S. at 630–35.
  \item \footnote{61} \textit{See Donohue, \textit{Original, supra} note 15, at 1308–14} (discussing \textit{Boyd} and the origins of the mere evidence rule, and suggesting that instead of inventing it out of whole cloth, the Court’s adherence to it reflected a long practice of rejecting the use of search and seizure to obtain evidence against individuals.).
  \item \footnote{63} § 2, 40 Stat. at 228, 230.
\end{itemize}
In 1921, the mere evidence rule reached what one commentator has referred to as its “zenith.” In *Gouled v. United States* the Court considered whether the warrantless removal of a paper from a defendant’s office violated the Fourth Amendment. Justice Clarke, on behalf of the Court, observed that making a search by stealth did not make it more reasonable than if the same were accomplished “by force or illegal coercion.” He continued,

The security and privacy of the home or office and of the papers of the owner would be as much invaded and the search and seizure would be as much against his will in the one case as in the other, and it must therefore be regarded as equally in violation of his constitutional rights.

Based on *Boyd*, the admission of the papers as evidence violated the Fifth Amendment.

The difficulty of differentiating the instrumentalities of crime from mere evidence ultimately led to the demise of the mere evidence rule. But even as it fell from use, courts agonized over the implications of giving the government access to private papers. According to one commentator, the reasons for this appear to be twofold.

First was the risk that the government would engage in searches beyond what was required. As Judge Learned Hand explained in 1926, “It is seldom that one finds a document containing evidence of crime which was not at one time used in its commission.” But to find such evidence often required “a thorough

---

65. 255 U.S. 298, 303 (1921).
66. Id. at 305.
67. Id. at 305–06.
68. Id. at 306.
70. See Rintala, *supra* note 62, at 2115.
71. Id.
72. Id.
73. United States v. Kirschenblatt, 16 F.2d 202, 204 (2d Cir. 1926); see also Rintala, *supra* note 62, at 2115 (citing and discussing *Kirschenblatt*).
search of all that the offender has.” Should the courts allow this, however, they would be endorsing “exactly what [the Fourth Amendment] was designed to prevent.”

“Therefore,” Hand continued, “we cannot agree that the power extends beyond those which are a part of the forbidden act itself.”

Second, private papers can reveal the most intimate details of an individual’s life. As William Rintala observed,

Private papers, be they diary or political tract, are felt to stand on a different footing from other kinds of personal property. This difference can be attributed at least in part to the fact that they are products of the mind; to invade this realm is to strip the individual of the last vestige of privacy.

C. Voice Communications

As new technologies extended interpersonal communications beyond dwellings and channels of written correspondence, novel questions regarding the extent of Fourth Amendment protections emerged. Initially, the Court came down on the side of the traditional distinction between private and public space, drawing the line at the walls of the home.

74. Kirschenblatt, 16 F.2d at 204.
75. Id.; see also Rintala, supra note 62, at 2115.
76. Kirschenblatt, 16 F.2d at 204.
77. Rintala, supra note 62, at 2115–16 (footnote omitted).
78. For an interesting discussion of telegraphy and why it did not give rise to similar issues, see Susan W. Brenner, The Fourth Amendment in an Era of Ubiquitous Technology, 75 Miss. L. J. 1, 12–16 (2005). For detail on the evolution of the telephone and its place in communications, see id. at 17–21.
79. I depart here from the account offered by Professor Thomas Clancy in his excellent treatise on the Fourth Amendment. In that work, he suggests that “beginning with Olmstead v. United States, the Court limited Fourth Amendment rights in two important ways. First, the only things protected were tangible objects, such as houses, papers, and physical possessions. Second, those objects were only protected against physical invasions.” Thomas K. Clancy, The Fourth Amendment: Its History and Interpretation § 3.2.2 (2d ed. 2014) (footnote omitted) (describing Olmstead v. United States, 277 U.S. 438 (1928)). Reflecting its common law origins, the Fourth Amendment had always been treated in this manner, suggesting that Fourth Amendment rights were not narrowed or newly-limited, but merely continued. Olmstead continued the traditional interpretation, until the Court eventually moved to recognize that the same privacy interests in the traditional purview of the Fourth Amendment were implicated by voice communication technologies. See generally Silverman v. United States, 365 U.S. 505 (1961) (finding eavesdropping with a listening device by means of unauthorized physical penetration a violation of the Fourth Amendment). The “property-based theories of Boyd and Olmstead,” as Clancy characterizes the concept, supra, at § 3.2.3, actually extended beyond these cases to the founding generation’s initial understanding of
privacy. Conversely, the absence of physical entry meant that no privacy interest had been disturbed.

In *Olmstead v. United States*, the first case dealing with new communications technology, the Supreme Court held that the wiretapping of an individual’s private telephone line did not fall within constitutional protections, as the government had not engaged in a physical trespass.\(^80\) Chief Justice Taft, delivering the opinion of the Court, wrote, “[U]nless there has been an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house ‘or curtilage’ for the purpose of making a seizure,” neither wiretapping nor electronic eavesdropping absent a warrant violated an individual’s Fourth Amendment rights.\(^81\)

A few observations about Taft’s language deserve note. First, this is the first time that the Supreme Court used the word “curtilage” in relation to the validity of a search under the Fourth Amendment.\(^82\) State courts, in contrast, for more than a century had considered the validity of search and seizure under state constitutional law to turn on whether the action took place within the curtilage.\(^83\)

the Fourth Amendment. *See* Donohue, *Original*, *supra* note 15, at 1192–93 (arguing that the original meaning of the Fourth Amendment limited general searches and seizures and required specific warrants, and emphasizing the importance of the common law in interpreting reasonableness). Numerous secondary sources discuss *Olmstead*, *Goldman*, and *Silverman* as precursors to *Katz*. *See*, e.g., Weaver, *supra* note 12, at 1150.

80. *Olmstead*, 277 U.S. at 466.

81. *Id.* (emphasis added).

82. Search using Westlaw’s All Federal and All State Cases database (curtilage OR curtelage OR curtailage) AND (search or warrant or warrantless) 1750 to 1921; Search using Lexis Advance in the All Federal Cases and State Cases database with exact phrase “curtilage” and any of these terms “search or seizure or warrant or warrantless” 1750 to 1921; *Id.*, using exact phrases curtilage, curtelege, and curtailage.

83. *See*, e.g., Commonwealth v. Intoxicating Liquors, 110 Mass. 182, 186 (1872) (considering whether the outbuildings contained within the curtilage were covered by a warrant); Pond v. People, 8 Mich. 150, 181 (1860) (finding in the context of the search and seizure of a person that a fence is not necessary for a net house to be considered within the curtilage if the space is no larger than that which is usually occupied for the purposes of dwelling and outbuildings); Haggerty & Nobles v. Wilber & Barnet, 16 Johns. 287, 288 (N.Y. Sup. Ct. 1819) (holding that a sheriff has the authority to break open and seize goods, but if they are located within the curtilage, the sheriff is precluded from entering unless the outer door is open); Douglass v. State, 14 Tenn. 525, 529 (1834) (the validity of seizure and arrest of rioters located in a smoke-house depends upon whether the building is considered within the curtilage); Parrish v. Commonwealth, 81 Va. 1, 4 (1884) (requiring a warrant for the search of corn in a tobacco house within the curti-
Second, Taft borrowed the term from criminal law, where it derived from the common law of burglary, which increased criminal penalties for illegal activity within the curtilage.\(^{84}\) Disagreement marked what, precisely, counted as the curtilage.\(^{85}\) In the early 19th century, for instance, *Jacob’s Law Dictionary* defined it as “[a] courtyard, back-side, or piece of ground lying near and belonging to a dwelling-house.”\(^{86}\) It incorporated buildings like out houses and store-houses occasionally used for sleeping.\(^{87}\) The way in which Taft

---

\(^{84}\) Four years prior to *Olmstead*, Justice Holmes had cited back to Blackstone’s *Commentaries* and the common law of burglary in support of establishing the open fields doctrine. Hester v. United States, 265 U.S. 57, 59 (1924) (citing 4 WILLIAM BLACKSTONE, COMMENTARIES *225*) (“For no distant barn, warehouse, or the like, are under the same privileges, nor looked upon as a man’s castle of defence: nor is a breaking open of houses wherein no man resides, and which therefore for the time being are not mansion-houses, attended with the same circumstances of midnight terror.”). Later cases attributed Taft’s reference to curtilage to stem from the common law of burglary. *E.g.* United States v. Dunn, 480 U.S. 294, 300 (1987).

\(^{85}\) State v. Langford, 12 N.C. 253, 254 (1827) (“[W]riters do not precisely agree as to what constitutes the curtilage.”); People v. Taylor, 2 Mich. 250, 252 (1851) (“The definitions of [curtilage in] Bouviere and Chitty do not strictly agree with [other law dictionaries].”)

\(^{86}\) *Curtilage*, 2 JACOB’S LAW DICTIONARY 171 (New York, Riley 1811); *see also* State v. Twitty, 2 N.C. 102, 102 (1794) (defining it as “a piece of ground either inclosed or not, that is commonly used with the dwelling house.”); State v. Shaw, 31 Me. 523, 527 (1850) (“The curtilage of a dwellinghouse is a space, necessary and convenient and habitually used, for the family purposes, the carrying on of domestic employments. It includes the garden, if there be one.”).

\(^{87}\) *See, e.g.*, State v. Brooks, 4 Conn. 446, 448–49 (1823) (“The mansion not only includes the dwelling-house, but also the out-houses, such as barns, stables, cow-houses, dairy-houses and the like, if they be parcel of the messuage, though they be not under the same roof or joining continuous to it.”) (internal quotation marks omitted) (considering a barn to be an out-house and thus protected under statutory provisions); People v. Parker, 4 Johns 424, 424 (N.Y. Sup. Ct. 1809) (placing store house specifically not used for sleeping, and not enclosed with the house, outside the curtilage); State v. Wilson, 2 N.C. 242, 242 (1795) (“All out houses standing in the same yard with the dwelling-house, and used by the owner of the dwelling-house as appurtenant thereto, whether the yard be open or enclosed, are in the eye of the law parts of the dwelling-house; and will satisfy that word used in an indictment of burglary.”) (placing storehouses used occasionally for sleeping within the curtilage); Gage v. Shelton, 3 Rich 242, 249–50 (S.C. App. L. & Eq. 1832) (noting that any out house contributory to the mansion, if placed close enough that burning it would put the dwelling in danger, was protected against arson); Douglass v. State, 14 Tenn. 525, 529–30 (1834) (finding a smokehouse to be within the curtilage of the mansion house); *see also* Twitty, 2 N.C. at 103 (considering the out house to be within the curtilage of the home); *cf.* Langford, 12 N.C.
used the term in *Olmstead*, though, allowed for a later reading that considered the curtilage coterminous with the home itself. The Court’s holding in *Hester*, the year before *Olmstead*, which distinguished between open fields and the home, reinforced this reading.\textsuperscript{88}

Third, beyond sowing the seeds for a narrower protected sphere, Taft gave the mistaken impression that the term carried weight in the Court’s Fourth Amendment jurisprudence. In support of his framing, he quoted the 1921 case of *Amos v. United States*, which dealt with a violation of revenue laws.\textsuperscript{89} In *Amos*, law enforcement had arrived at the defendant’s home and asked his wife for entry.\textsuperscript{90} Performing a warrantless search, they found a bottle of illicitly distilled whisky in a barrel of peas.\textsuperscript{91} After the jury was sworn in, but before evidence had been presented, the defendant in the criminal case presented a sworn petition to the court, requesting that his private property be returned to him.\textsuperscript{92} According to the *Amos* Court, the petition stated that the whiskey had been seized by “officers of the Government in a search of defendant’s house and store ‘within his curtilage,’ made unlawfully and without warrant of any kind, in violation of his rights under the Fourth and Fifth Amendments to the Constitution of the United States.”\textsuperscript{93} The lan-

\textsuperscript{88} *Hester*, 265 U.S. at 59.

\textsuperscript{89} *Olmstead*, 277 U.S. at 461 (citing Amos v. United States, 255 U.S. 313, 315 (1921)).

\textsuperscript{90} Amos, 255 U.S. at 315.

\textsuperscript{91} Id. at 314–15.

\textsuperscript{92} Id. at 314.

\textsuperscript{93} Id.
guage of the criminal defendant’s petition to the lower court was the only reference in *Amos* to the curtilage of the home.94

In *Olmstead*, Taft picked up on the language *in the criminal defendant’s petition*, quoting it directly and then misquoting it later in the opinion as an alternative to, or potentially a synonym for, the home (“‘or curtilage’”).95 Taft went on to rely on the absence of any *physical penetration* of the curtilage as grounds to consider wiretapping outside the contours of the Fourth Amendment.96

Justice Brandeis, joined by Justice Stone, presented a forceful dissent that objected to the emphasis on physical penetration, pointing to the interests at stake.97 He argued that the interception of the conversation constituted an “unjustifiable intrusion . . . upon the privacy of the individual,” and thus violated the Fourth Amendment.98 Brandeis underscored what the “makers of our Constitution” had tried to accomplish: “They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations.”99 He continued, “They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.”100 Brandeis warned that the Court had to look not just at the current context, but also what was coming down the pike. He cautioned,

The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.101

Brandeis was ahead of his time in identifying the privacy interests involved. The Court had yet to appreciate how technology had altered the impact of the traditional distinction between private

94. See generally id. The Court ruled for the defendant, saying that *Gouled*, and the mere evidence rule, controlled. *Id.* at 316.
96. *Id.*
97. See generally *id.* at 471 (Brandeis, J., dissenting); *Id.* at 488 (Stone, J., dissenting).
98. *Id.* at 478 (Brandeis, J., dissenting).
99. *Id.*
100. *Id.*
101. *Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting); see also *Weems v. United States*, 217 U.S. 349, 373 (1910) (“In the application of a constitution, therefore, our contemplation cannot be only what has been but of what may be. . . . Rights declared in words might be lost in reality. And this has been recognized.”).
space and the public domain. A series of cases began hammering on the door.

In 1942, the Court considered federal agents’ access to the office of an individual suspected of conspiring to violate criminal provisions of the Bankruptcy Act.\(^{102}\) Agents went into an adjoining office, where they placed a listening device in a small aperture in the wall.\(^{103}\) When the device failed, officers used a detectaphone to listen to conversations next door, which they recorded and transcribed using a stenographer.\(^{104}\) Consistent with *Olmstead*, the Court found in *Goldman v. United States* that use of the detectaphone did not run afoul of the Fourth Amendment.\(^{105}\)

In his dissent, Justice Murphy blasted the Court for not taking account of new technologies.\(^{106}\) Referencing the acclaimed 1890 *Harvard Law Review* article written by Louis Brandeis and Samuel Warren, Murphy argued for a broader reading of the Fourth Amendment to protect individuals “against unwarranted intrusions by others” into their private affairs.\(^{107}\) Although the language of the Fourth Amendment intimated protection against physical trespass, Murphy averred, “[I]t has not been the rule or practice of this Court to permit the scope and operation of broad principles ordained by the Constitution to be restricted, by a literal reading of its provisions, to those evils and phenomena that were contemporary with its framing.”\(^{108}\) Of greater importance were the privacy interests that the amendment was meant to protect.

Like Brandeis in *Olmstead*, Murphy recognized that the “conditions of modern life have greatly expanded the range and character of those activities which require protection from intrusive action by Government officials if men and women are to enjoy the full benefit of that privacy which the Fourth Amendment was intended to provide.”\(^{109}\) It was therefore the Supreme Court’s “duty to see that this historic provision receives a construction sufficiently liberal and elastic to make it serve the needs and manners of each succeeding generation.”\(^{110}\) Murphy gave little countenance to whether or not a physical entry had occurred since “science has brought forth far

---

103. *Id.* at 131.
104. *Id.* at 131–32.
105. *Id.* at 135.
106. *Id.* at 139 (Murphy, J., dissenting).
107. *Id.* at 136 (Murphy, J., dissenting) (citing Louis Brandeis & Samuel Warren, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890)).
108. *Goldman*, 316 U.S. at 138 (Murphy, J., dissenting).
109. *Id.*
110. *Id.*
more effective devices for the invasion of a person’s privacy than the direct and obvious methods of oppression which were detested by our forebears and which inspired the Fourth Amendment.”\(^{111}\) To the extent that electronic surveillance made it possible to do what had hitherto been considered within the ambit of the Fourth Amendment, so, too, ought new technologies to be considered within the reach of the Constitution.

By the time *Silverman v. United States* was decided in 1961, the intrusiveness of new technologies on interests previously guarded by the walls of the home had become apparent.\(^{112}\) The petitioner’s brief in *Silverman* underscored the impact of recent advances, drawing attention to parabolic microphones “which can pick up a conversation three hundred yards away,” experimental sound wave technology “whereby a room is flooded with a certain type of sonic wave . . . mak[ing] it possible to overhear everything said in a room without ever entering it or even going near it,” and devices that could “pick up a conversation through an open office window on the opposite side of a busy street.”\(^{113}\) But the physical characteristics of a spike mike allowed the Court to distinguish the facts from *Olmstead*: in *Silverman*, since law enforcement had made physical contact with a heating duct, “an unauthorized physical penetration into the premises occupied by the petitioners” had occurred.\(^{114}\)

In reaching its decision, the Court recognized the extent to which emerging technologies had proven contentious: “Eavesdropping accomplished by means of such a physical intrusion is beyond the pale of even those decisions in which a closely divided Court has held that eavesdropping accomplished by other electronic means did not amount to an invasion of Fourth Amendment rights.”\(^{115}\) At the same time, the Court doubled down on the importance of the home.\(^{116}\) Trespass ruled the day.\(^{117}\) The importance of

---

111. *Id.* at 139.


113. *Id.* at 508–09 (internal quotation marks omitted); *see also* *Weaver*, supra note 12, at 1148 (discussing *Silverman*).

114. *Id.* at 509.

115. *Id.* at 509–10.

116. *Id.* at 511 ("The Fourth Amendment, and the personal rights which it secures, have a long history. At the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.")

117. The parallels between *Silverman* and *United States v. Jones*, 132 S. Ct. 945, 954 (2012), also decided on grounds of trespass, are of note, as *Jones* also signaled a growing concern for how new technologies may affect rights otherwise protected
drawing a distinction between the private and public realms underlay the Court's approach. Behavior in the former realm was protected. But in public, individuals assumed the risk that what they said and did would be witnessed, and potentially recalled, by others.

Silverman proved pivotal, foreshadowing the coming confrontation between new technologies and the protections guaranteed in the Fourth Amendment. While heeding to the traditional trespass doctrine, it noted the potential for “frightening paraphernalia which the vaunted marvels of an electronic age may visit upon human society.”

In summary, the Court's initial take when confronted by technology had been to construe the Fourth Amendment “in the light of what was deemed an unreasonable search and seizure when it was adopted.” As Taft explained in Olmstead, “Congress may of course protect the secrecy of telephone messages by making them, when intercepted, inadmissible in evidence. . . . But the courts may not adopt such a policy by attributing an enlarged and unusual meaning to the Fourth Amendment.” Where the public realm ended and private life began, a higher standard applied. Accordingly, in its June 1967 Camara v. Municipal Court decision, the Court came out strongly on the side of drawing a border at the walls of the home. But the tension between new technologies and the existing doctrine had reached a boiling point. Just four months later, the Court in Katz v. United States extended the protection of the Fourth Amendment beyond physical property to include areas that individuals considered private. In doing so, the Court raised new questions as to whether the shift to protect "people," not "places,"

under the Fourth Amendment, but relied on traditional trespass theory for its holding. See discussion infra Part III(D).


119. Olmstead v. United States, 277 U.S. 438, 465 (1928) (quoting Carroll v. United States, 267 U.S. 132, 149 (1925)). In Olmstead, Chief Justice Taft wrote on behalf of the Court, “The well known historical purpose of the Fourth Amendment . . . was to prevent the use of governmental force to search a man’s house, his person, his papers and his effects; and to prevent their seizure against his will.” Id. at 463. It was the home itself that was a constitutionally protected area. “The language of the Amendment,” Taft suggested, “can not be extended and expanded to include telephone wires reaching to the whole world from the defendant’s house or office. The intervening wires are not part of his house or office any more than are the highways along which they are stretched.” Id. at 465.

120. Id. at 465–66.


created a new safeguard for activities that took place outside the curtilage of the home.

III. PRIVATE VERSUS PUBLIC SPACE

In 1967, the Supreme Court finally solidified around the arguments articulated in the dissents in *Olmstead* and *Goldman* and in dicta in *Silverman*, which recognized the impact of new technologies on privacy.\(^\text{123}\) The Court overruled *Olmstead*, rejecting the idea that the reach of the Fourth Amendment "turn[ed] upon the presence or absence of a physical intrusion into any given enclosure."\(^\text{124}\) More critical was whether individuals had a reasonable expectation of privacy.

In *Katz*, a gambler entered a public telephone booth, closed the door, and placed a call.\(^\text{125}\) The privacy interests at stake could not be ignored. Justice Stewart explained on behalf of the Court, "The Government’s activities in electronically listening to and recording the petitioner’s words violated the privacy upon which [Katz] justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."\(^\text{126}\) The central issue was not whether physical penetration of a constitutionally-protected area had occurred.\(^\text{127}\) As Stewart famously articulated, "The Fourth Amendment protects people, not places."\(^\text{128}\)

In his concurrence, Justice Harlan spelled out the two-part test that would henceforward be applied. First, whether an individual, by his or her conduct, had "exhibited an actual (subjective) expectation of privacy"\(^\text{129}\) (or, as the majority articulated, whether he had demonstrated that "he seeks to preserve [something] as private").\(^\text{130}\) And, second, whether the subjective expectation was "one

\(^{123}\) Compare id., with *Olmstead*, 277 U.S. at 438 (Brandeis, J., dissenting), and *Goldman* v. United States, 316 U.S. 129, 139 (1942) (Murphy, J., dissenting), and *Silverman* v. United States, 365 U.S. 505, 508–10 (1961).

\(^{124}\) *Katz*, 389 U.S. at 353.

\(^{125}\) Id. at 348, 352.

\(^{126}\) Id. at 353.

\(^{127}\) Id. ("The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.").

\(^{128}\) Id. at 351.

\(^{129}\) Id. at 361 (Harlan, J., concurring).

\(^{130}\) *Katz*, 389 U.S. at 351.
that society is prepared to recognize as ‘reasonable.’”  

The Court would look at the circumstances to ascertain whether an individual’s expectation of privacy was justified.

In *Katz*, the Court attempted to wrench Fourth Amendment doctrine from its tie to property rights, but it failed to deliver on its promise. The case left open myriad questions. Over the ensuing decade, the Court systematically worked its way through related areas, in the process modifying and carving out exceptions to the warrant requirement. Simultaneously, the rules that evolved in the 1970s and ’80s relied in significant measure on the physical world. It was thus not *Katz*’s reasonable expectation of privacy in his communication, per se, but his reasonable expectation of privacy when he entered the phone booth that proved central. The private/public distinction held. Current technologies, however, blur the distinction between private space and the public domain on which the court has relied as a way of understanding the interests at stake. Perhaps nowhere is this more apparent than in regard to location tracking.

A. Open Fields, Naked Eye

One of the earliest cases to reinforce the open fields doctrine came in 1974, when the Supreme Court determined that a Colorado inspector entering an individual’s yard during the daytime to test the plumes of smoke being emitted from the homeowner’s chimneys did not trigger Fourth Amendment protections.

In *Air Pollution Variance Board v. Western Alfalfa Corp.*, the Court went into great detail as to what had happened, concluding that the invasion of privacy, “if it can be said to exist, is abstract and theoretical.”

---


134. See discussion, infra, Part III(A).


136. Id. (“The EPA regulation for conducting an opacity test requires the inspector to stand at a distance equivalent to approximately two stack heights away but not more than a quarter of a mile from the base of the stack with the sun to his back from a vantage point perpendicular to the plume; and he must take at least
A decade later, the Court reaffirmed its position in *Oliver v. United States*.\(^{137}\) Hearkening back to *Hester*’s (pre-*Katz*) reliance on the text of the Fourth Amendment, the Court established that “effects” did not include “open fields.”\(^ {138}\) In *Oliver*, the Kentucky State Police had received reports that a farmer was growing marijuana.\(^ {139}\) They searched Oliver’s property, which was surrounded by a gate marked “No Trespassing,” without first obtaining a warrant.\(^ {140}\) In a 6-3 decision, Justice Powell explained that the open fields doctrine applied.\(^ {141}\) Even where police officers might be engaged in a common law trespass, the act of entering a privately owned field did not automatically trigger Fourth Amendment protections.\(^ {142}\) Justice White’s concurrence noted that fields, by definition, were neither a “house” nor an “effect.”\(^ {143}\)

The Court recognized multiple factors for determining whether a place should be free from government intrusion absent a warrant.\(^ {144}\) It noted the importance of “the intention of the Framers of the Fourth Amendment, the uses to which the individual has put a location, and our societal understanding that certain areas deserve the most scrupulous protection from government invasion.”\(^ {145}\) The factors were “equally relevant to determining whether the government’s intrusion upon open fields without a warrant or probable cause violates reasonable expectations of privacy.”\(^ {146}\)

The open fields doctrine applied even when the land in question was fenced and posted: “[A]n individual may not legitimately demand privacy for activities conducted out of doors in fields, except in the area immediately surrounding the home.”\(^ {147}\) The Court emphasized “the overriding respect for the sanctity of the home

\(^{25}\) readings, recording the data at 15- to 30-second intervals. Depending upon the layout of the plant, the inspector may operate within or without the premises but, in either case, he is well within the ‘open fields’ exception to the Fourth Amendment approved in *Hester*.”


\(^{138}\) *Id.* at 177.

\(^{139}\) *Id.* at 173.

\(^{140}\) *Id.* at 173–74.

\(^{141}\) *Id.* at 183–84.

\(^{142}\) *Id.* at 183–84.

\(^{143}\) *Oliver*, 466 U.S. at 184 (White, J., concurring).

\(^{144}\) *Id.* at 177–78.

\(^{145}\) *Id.* at 178 (citations omitted).

\(^{146}\) *Id.*

\(^{147}\) *Id.* By adopting this position, the court departed from the traditional understanding of curtilage, as the term had been used in criminal statutes and property disputes. See generally 1 CHITTY’S GENERAL PRACTICE 175 (London, Butterworth 1833).
that has been embedded in our traditions since the origins of the Republic.”

Justice Marshall, joined by Justices Brennan and Stevens, dissented. Marshall could not agree “that an individual may not legitimately demand privacy for activities conducted out of doors in fields, except in the area immediately surrounding the home.”

The plain language of the amendment protected neither telephone booths nor businesses—yet both had fallen within its contours.

The reason was clear: the Fourth Amendment was not designed to specify with “precision” which activities were permissible or not, but rather “to identify a fundamental human liberty that should be shielded forever from government intrusion.”

Unlike statutes, constitutional provisions must be understood in a way that “effectuate[s] their purposes—to lend them meanings that ensure that the liberties the Framers sought to protect are not undermined by the changing activities of government officials.”

Marshall cited to Chief Justice Marshall’s famous words in *McCulloch v. Maryland*, “[W]e must never forget, that it is a constitution we are expounding.”

Marshall argued that under a *Katz* analysis, the Court should look to positive law, the nature of the uses to which the space could be put, and whether the individual claiming the privacy interest made it clear to the public in a way that others “would understand and respect.”

While privacy interests may not be coterminous with property rights, they reflected explicit recognition of a domain over which an individual held authority.

Marshall, nevertheless, fell back upon the traditional private/public distinction: “Privately owned woods and fields that are not exposed to public view regu-

---

148. Oliver, 466 U.S. at 178 (internal quotation marks omitted).
149. Id. at 179.
150. Id. at 184 (Marshall, J., dissenting).
151. Id. at 185 (Marshall, J., dissenting) (quoting id. at 178 (majority opinion)).
152. Id. at 185–86.
153. Id. at 186.
154. Oliver, 466 U.S. at 187.
155. Id. at 187 n.4 (Marshall, J., dissenting) (quoting McCulloch v. Maryland, 17 U.S. 316, 407 (1819)).
156. Id. at 187–88.
157. Id. at 189.
158. Id. at 189–90.
larly are employed in a variety of ways that society acknowledges deserve privacy.”

Oliver made it clear that Katz had not changed the basic tenets of the open fields doctrine. For the majority, it was not that Katz did not expand what might be included within a reasonable expectation of privacy. It simply did not incorporate open fields. For Marshall, the private/public distinction similarly controlled. He merely reached a different answer for privately owned land.

Questions remained about the precise limits of the curtilage. In 1987, the Court went on to determine that the space immediately outside a barn—some half a mile from any road and only reachable after crossing a number of fences—constituted “open fields.” In United States v. Dunn, Robert Carpenter, and his co-defendant, Ronald Dunn, were convicted of conspiring to manufacture phenylacetone and amphetamine, as well as possessing amphetamine with an intent to distribute it. Drug Enforcement Administration (DEA) agents discovered that Carpenter had purchased significant amounts of chemicals and equipment used in the manufacture of the controlled substances. The agents obtained warrants from a Texas state judge, allowing them to install radio frequency-enabled transmitters in the material and equipment. They tracked Carpenter’s truck until it arrived at Dunn’s ranch. Aerial photographs captured images of the truck parked next to a barn.

The property, some 198 acres, was encircled by a fence and contained several interior fences, mostly constructed of posts and barbed wire. The nearest public road was a half-mile away. A fence surrounded the house and a nearby greenhouse, with two barns another fifty feet away. The front of one of the barns had a wooden fence around it, along with locked, waist-high gates and netting material stretched between the barn and the gates. A DEA agent and an officer from the Houston Police Department

---

159. Id. at 192.
160. Oliver, 466 U.S. at 192.
162. Id. at 296.
163. Id.
164. Id.
165. Id. at 297.
166. Id.
167. Dunn, 480 U.S. at 297.
168. Id.
169. Id.
170. Id.
crossed the outside fence and one interior fence.\footnote{Id.} Part way be-
tween the residence and the barns, the agent smelled phenylacetic
acid coming from the barns.\footnote{Id.} The officers crossed another
barbed-wire fence and a wooden fence, walked under the barn’s
overhang to the locked wooden gates, and, using a flashlight,
looked into the barn.\footnote{\textit{Dunn}, 480 U.S. at 297–98.} Seeing a laboratory, they did not enter the
barn, although the following day they returned twice to confirm
their initial sighting.\footnote{Id. at 298.} That evening, they obtained a warrant au-
thorizing them to search the ranch.\footnote{Id. at 298–99.} Two days later, they exe-
cuted the warrant, seizing chemicals, laboratory equipment, and
amphetamines.\footnote{Id.}

The Supreme Court reiterated the special place of the home in
Fourth Amendment jurisprudence. “The curtilage concept,” the
Court wrote, “originated at common law to extend to the area im-
mediately surrounding a dwelling house the same protection under
the law of burglary as was afforded the house itself.”\footnote{\textit{Dunn}, 480 U.S. at 299.}

The Court was right insofar as the curtilage had historically
been considered relevant to the penalties associated with criminal
activity. But it was not until 1928, with Taft’s decision in \textit{Olmstead},
that the term became drawn into the Supreme Court’s Fourth
Amendment jurisprudence. And prior to that time, curtilage had a
much broader meaning.

According to Cunningham’s law dictionary from 1764, for in-
stance, curtilage meant precisely what the Court rejected in \textit{Oliver}:

\begin{itemize}
\item Part way between the residence and the barns, the agent smelled phenylacetic
acid coming from the barns.
\item The officers crossed another barbed-wire fence and a wooden fence, walked under the barn’s
overhang to the locked wooden gates, and, using a flashlight,
looked into the barn. Seeing a laboratory, they did not enter the
barn, although the following day they returned twice to confirm
their initial sighting. That evening, they obtained a warrant au-
thorizing them to search the ranch. Two days later, they exe-
cuted the warrant, seizing chemicals, laboratory equipment, and
amphetamines.
\end{itemize}
“a yard, backside, or piece of ground lying near a dwelling house, where they sow hemp, beans, and such like.”  

In 1820, Sheppard’s *Touchstone of Common Assurances* described it as “a little garden, yard, field, or piece of void ground, lying near and belonging to the messuage, and houses adjoining the dwelling house, and the close upon which the dwelling-house is built.”  

In 1828, Johnson & Walker simply defined it as “a garden, yard, or field lying near to a messuage.”  

*Oliver* narrowed the meaning of the term, and the Court in *Dunn* highlighted four factors to be taken into account:

[T]he proximity of the area claimed to be curtilage to the home, whether the area is included within an enclosure surrounding the home, the nature of the uses to which the area is put, and the steps taken by the resident to protect the area from observation by people passing by.

It eschewed a rigid adherence to the categories, arguing that they were “useful analytical tools only to the degree that, in any given case, they bear upon the centrally relevant consideration—whether the area in question is so intimately tied to the home itself that it should be placed under the home’s ‘umbrella’ of Fourth Amendment protection.”  

Applied to the barn, the Court concluded that it did not.

Curtilage considerations thus dismissed, naked eye doctrine prevailed. “Under *Oliver* and *Hester,*” the Court wrote, “there is no constitutional difference between police observations conducted while in a public place and while standing in the open fields.”

---

178. *Curtilage*, 1 TIMOTHY CUNNINGHAM, A NEW AND COMPLETE LAW DICTIONARY (London, Law-Printers to the King’s Most Excellent Majesty 1764), https://archive.org/stream/newcompletelawdi01cunn#page/n613/mode/2up; see also *Curtilage*, 2 GILES JACOB & T.E. TOMLINS, THE LAW-DICTIONARY: EXPLAINING THE RISE, PROFESS, AND PRESENT STATE, OF THE ENGLISH LAW 171 (New York, I. Riley 1811) (“CURTILAGE, curtilagrium, from the Fr. cour, court and Sax. leagh, locus.] A court-yard, back-side, or piece of ground lying near and belonging to a dwelling house. And though it is said to be a yard or garden, belonging to a house, it seems to differ from a garden, for we find cum quodam gardino et curtilagio.”) (citations omitted).


181. See *Dunn*, 480 U.S. at 301 (discussing *Oliver* and deriving factors from lower courts).

182. Id.

183. Id. at 304.
Just as the observation from a plane in *California v. Ciraolo* (discussed *infra* in Section III(B)) did not violate the Fourth Amendment, neither did peering into the barn.\footnote{In *Ciraolo*, the Court had observed that the Fourth Amendment “has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares.” *California v. Ciraolo*, 476 U.S. 207, 213 (1986). Also note that in 1983 the court settled that simply using a flashlight to illuminate the interior of a car, without probable cause to search the automobile, did not transgress any rights secured by the Fourth Amendment. *Texas v. Brown*, 460 U.S. 730, 739–40 (1983); *see also* United States v. Lee, 274 U.S. 559, 563 (1927) (use of searchlight by Coast Guard on high seas is not a search).} Despite *Katz’s* move to a reasonable expectation of privacy as centered on persons, and not property, the curtilage of the home continued to serve as a proxy.

In *Dunn*, Justice Brennan, joined by Justice Marshall, dissented.\footnote{185. *Dunn*, 480 U.S. at 305 (Brennan, J., dissenting).} The reasoning paralleled their position in *Oliver*: the intrusion violated the Fourth Amendment because the barnyard “lay within the protected curtilage of Dunn’s farmhouse,” and the agents’ inspection violated Dunn’s reasonable expectation of privacy. Like the majority, the dissent’s logic reflected the private-space/public domain distinction that had long marked Fourth Amendment doctrine. Brennan did note, though, the underlying *purpose* of the constitutional text: prohibiting “police activity which, if left unrestricted, would jeopardize individuals’ sense of security or would too heavily burden those who wished to guard their privacy.”\footnote{186. *Id.* at 306.} DEA agents had gone “one-half mile off a public road over respondent’s fenced-in property, crossed over three additional wooden and barbed wire fences, stepped under the eaves of the barn, and then used a flashlight to peer through otherwise opaque fishnetting.”\footnote{187. *Id.* at 319.} He concluded, “For the police habitually to engage in such surveillance—without a warrant—is constitutionally intolerable.”\footnote{188. *Id.*}

Just a few months after *Dunn*, the Court beat the proverbial horse. In *California v. Greenwood*,\footnote{189. *California v. Greenwood*, 486 U.S. 35 (1988).} local police suspected Billy Greenwood of dealing drugs out of his home. Lacking sufficient evidence for a warrant, they searched his garbage and found incriminating material. In a 6-2 vote, the Court held that the garbage left out on the curb, “readily accessible to animals, children, scavengers,
snoops, and other members of the public," lay outside the protections of the Fourth Amendment.190

In his dissent, Justice Brennan, joined by Justice Marshall, emphasized that Greenwood had placed the garbage in opaque bags, blocking their view from casual passers-by.191 Garbage could reveal a considerable amount about Greenwood’s private life: “A single bag of trash testifies eloquently to the eating, reading, and recreational habits of the person who produced it,” he wrote.192 Search of the material could reveal “intimate details about sexual practices, health, and personal hygiene. Like rifling through desk drawers or intercepting phone calls, rummaging through trash can divulge the target’s financial and professional status, political affiliations and inclinations, private thoughts, personal relationships, and romantic interests.”193 It reflected the type of “intimate knowledge associated with the ‘sanctity of a man’s home and the privacies of life’” that the Fourth Amendment was designed to protect.194 The majority’s private space/public domain distinction, premised on lesser expectations outside the physical borders of the home, had failed to capture the privacy interests at stake.

B. Aerial Surveillance

With the line still drawn post-<i>Katz</i> at the curtilage of the home, to the extent that new means of aerial surveillance raised privacy concerns, the Court dismissed them under the private/public distinction. The underlying rationale, that government officials should not be prevented from accessing what any citizen could see or hear, persisted.

In <i>California v. Ciraolo</i>, the police received an anonymous telephone tip that a resident of Santa Clara, California, was growing marijuana in his backyard.195 A six-foot outer fence and a ten-foot inner fence blocked the view from the street, so the police hired a private plane to fly overhead.196 They spotted marijuana plants, eight to ten feet tall, growing in a fifteen by twenty-five foot plot in the back yard.197

190. Id.
191. See, e.g., id. at 45 (Brennan, J., dissenting).
192. Id. at 50.
193. Id.
194. 486 U.S. 50–51 (Brennan, J., dissenting).
196. Id.
197. Id.
Chief Justice Burger, delivering the opinion of the Court, quickly dismissed the importance of the fence, noting that even the ten-foot-high structure “might not shield these plants from the eyes of a citizen or a policeman perched on the top of a truck or a two-level bus.”\textsuperscript{198}

Burger’s statement was extraordinary, not least because it was \textit{illegal} under California law for citizens to sit atop vehicles.\textsuperscript{199} Nor were there, in 1982, \textit{any} double-decker buses to be found in the largely rural and residential community.\textsuperscript{200} Nevertheless, Burger suggested that any citizen could look over the fence from the top of a moving vehicle. It was therefore unclear whether the respondent had a subjective expectation of privacy or “merely a hope that no one would observe [the respondent’s] unlawful gardening pursuits.”\textsuperscript{201}

Turning his attention to the curtilage, the Chief Justice noted that the common-law understanding was the area within which activities associated with the “sanctity of a man’s home and the privacies of life” occurred.\textsuperscript{202} “The protection afforded the curtilage,” he wrote, “is essentially a protection of families and personal privacy in an area intimately linked to the home, both physically and psychologically, where privacy expectations are most heightened.”\textsuperscript{203} The yard, and its crops, could be understood as inside the curtilage.\textsuperscript{204} But the burden was on the homeowner to ensure that the view was blocked.\textsuperscript{205} The “naked-eye observation of the curtilage by police from an aircraft lawfully operating at an altitude of 1,000 feet” meant that the owner had not taken the requisite steps.\textsuperscript{206} Any citizen, flying over the home within navigable airspace, could have seen the same thing.\textsuperscript{207} The Fourth Amendment does not “require law enforcement officers to shield their eyes when passing by a

\textsuperscript{198.} \textit{Id.} at 211.
\textsuperscript{200.} Author Note, having grown up in Santa Clara, California in the 1980s.
\textsuperscript{201.} \textit{Ciraolo}, 476 U.S. at 212.
\textsuperscript{202.} \textit{Id.} (quoting Oliver v. United States, 466 U.S. 170, 180 (1984)).
\textsuperscript{203.} \textit{Id.} at 212–13.
\textsuperscript{204.} \textit{Id.} at 213.
\textsuperscript{205.} \textit{See id.}
\textsuperscript{206.} \textit{Id.}
\textsuperscript{207.} \textit{Ciraolo}, 476 U.S. at 213–14.
home on public thoroughfares.” What was accessible to any person, had to be accessible to law enforcement.

The decision was a 5-4 vote, with Justice Powell, joined by Justices Brennan, Marshall, and Blackmun, dissenting. Powell cited to Justice Harlan’s warning in *Katz*, that tying the Fourth Amendment only to physical intrusion “is, in the present day, bad physics as well as bad law, for reasonable expectations of privacy may be defeated by electronic as well as physical invasion.” For the dissent, the airplane was “a product of modern technology” visually intruding into the respondent’s yard. While “[c]omings and goings on public streets are public matters,” flying a plane over a home to conduct surveillance intrudes upon a reasonable expectation of privacy.

Powell underscored the importance of the Fourth Amendment adapting to new and emerging technologies. “Rapidly advancing technology now permits police to conduct surveillance in the home itself,” he explained, “an area where privacy interests are most cherished in our society, without any physical trespass.” Flexibility mattered. The Court had “repeatedly refused to freeze ‘into constitutional law those enforcement practices that existed at the time of the Fourth Amendment’s passage.’” Instead, it had “construed the Amendment ‘in light of contemporary norms and conditions,’ . . . in order to prevent ‘any stealthy encroachments’ on our citizens’ right to be free of arbitrary official intrusion.” By the time of *Ciraolo*, Powell noted, technological advances had “enabled police to see people’s activities and associations, and to hear their conversations, without being in physical proximity.” The doctrine had to evolve to protect the privacy interests at stake.

The same day that the Court handed down *Ciraolo*, it issued an opinion in *Dow Chemical v. United States*, reinforcing the idea that what was visible in public was fair game. Dow Chemical denied a

---

208. *Id.* at 213.
209. *Id.* at 213–14.
211. *Id.* at 222.
212. *Id.* at 224–25.
214. *Id.* at 217 (Powell, J., dissenting) (quoting *Steagald* v. United States, 451 U.S. 204, 217 n.10 (1981)).
215. *Id.* (quoting *Steagald*, 451 U.S. at 217; *Boyd* v. United States, 116 U.S. 616, 635 (1886)).
216. *Id.* at 218.
request by the Environmental Protection Agency (EPA) to conduct an on-site inspection of a 2000-acre facility. The EPA responded by hiring a commercial aerial photographer to take pictures of the facility from the air.

Chief Justice Burger again wrote for the Court. He began the Fourth Amendment analysis by drawing a line between private and public space. Activities undertaken potentially in the view of others did not deserve the same protections as those that transpired within the home. While Dow Chemical held a "reasonable, legitimate, and objective expectation of privacy within the interior of its covered buildings" (one that society was prepared to recognize), it did not have an equally high expectation for areas exposed to aerial view.

The Court emphasized the importance of not unduly hampering law enforcement. The photographs were "essentially like those commonly used in mapmaking. Any person with an airplane and an aerial camera could readily duplicate them." It made no sense to force the government agency to close its eyes, to prevent it from seeing what anyone else could see and from memorializing the image with a photograph—as any citizen could do.

In 1989, the Court went on to consider whether aerial surveillance from a helicopter just 400 feet above the ground similarly was exempt from Fourth Amendment protections. The concept of the naked eye—and what other citizens would be able to do in the public realm—again figured largely in the decision.

Like the Santa Clara police in Ciraolo, a Florida county sheriff’s office received an anonymous tip that Riley was growing marijuana in a greenhouse behind his home. Located on five acres of property, his mobile home was surrounded by a fence, on which a sign

---

218. Id. at 229.
219. Id.
220. Id. at 235 ("The curtilage area immediately surrounding a private house has long been given protection as a place where the occupants have a reasonable and legitimate expectation of privacy that society is prepared to accept.") (citing Ciraolo, 476 U.S. at 207). Open fields, in contrast, "do not provide the setting for those intimate activities that the [Fourth] Amendment is intended to shelter from governmental interference or surveillance." Id. (alteration in original) (quoting Oliver v. United States, 466 U.S. 170, 179 (1984)).
221. Id. at 239.
222. Id. at 236, 239.
224. See id.
226. Id. at 448.
was posted saying, “DO NOT ENTER.” Unable to see behind the house from the street, an officer flew over the property in a helicopter. The greenhouse had two sides enclosed and was covered with corrugated panels, some translucent and some opaque. Two of the panels were missing. The officer looked through the openings in the roof and the open sides of the greenhouse and saw the plants growing. He used this information to obtain a search warrant, which yielded the plants.

Justice White announced the judgment and wrote an opinion in which only three other justices joined. Because Riley had left two sides of the greenhouse open, and had failed to cover the greenhouse entirely, he “could not reasonably have expected the contents of his greenhouse to be immune from examination by an officer seated in a fixed-wing aircraft flying in navigable airspace at an altitude of 1000 feet or . . . at an altitude of 500 feet, the lower limit of the navigable airspace for such aircraft.” It made no difference that the helicopter was at a height of 400 feet, as helicopters were not bound by the lower limits of navigable airspace as required for other aircraft. “Any member of the public could legally have been flying over Riley’s property in a helicopter at the altitude of 400 feet.” Why force law enforcement to undertake a form of willful blindness?

Justice Brennan, joined by Justices Marshall and Stevens, dissented. Brennan disputed the plurality’s focus on whether any member of the public could have conducted the activity undertaken by law enforcement, without also considering the difficulty of such activity and the frequency with which it was done by members of the public. “Is the theoretical possibility that any member of the public (with sufficient means) could also have hired a helicopter and looked over Riley’s fence of any relevance at all in determining whether Riley suffered a serious loss of privacy . . . ?” Law enforcement had not been standing on a public road.

---

227. Id.
228. Id.
229. Id.
230. Id.
231. Riley, 488 U.S. at 448.
232. Id. at 448–49.
233. Id. at 451.
234. Id. at 457–58 (Brennan, J., dissenting).
235. Riley, 488 U.S. at 460 (Brennan, J., dissenting).
point he enjoyed,” Brennan pointed out, “was not one any citizen could readily share.” To see over the fence, the officer had to use “a very expensive and sophisticated piece of machinery to which few ordinary citizens have access.” It made as much sense to rely on whether the officer was legally in the air, as it would have been to ascertain whether the police officers in Katz were legally standing outside the telephone booth. “The question before us,” Brennan explained, “must be not whether the police were where they had a right to be, but whether public observation of Riley’s curtilage was so commonplace that Riley’s expectation of privacy in his backyard could not be considered reasonable.”

Brennan’s argument underscored the importance of focusing on the privacy interests implicated by new technologies. Yet largely because of the persistence of the private/public distinction, his arguments did not win the day. Warrantless searches and seizures inside a home may be presumptively unreasonable absent exigent circumstances. But visual examination, even of areas inside the curtilage of the home, when conducted from a public sphere, lies outside the protections of the Fourth Amendment.

C. Radio-frequency Enabled Transmitters

As technology progressed and questions relating to the reasonable expectation of privacy standard adopted in Katz arose, the Supreme Court held fast to its private/public distinction. Just as people had a lesser expectation of privacy in garbage placed curbside—indeed, no expectation whatsoever—so, too, did they outside of automobiles, as well as in their movements along public thoroughfares.

238. Id.
239. Id.
240. Id.
241. Id.
243. Precisely what constitutes the curtilage of the home continues to be a contentious issue in Fourth Amendment jurisprudence. See Clancy, supra note 79, at § 4.4.1.1; 1 Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment §2.3 (5th ed. 2016).
244. The seizure of a car travelling on a public highway, absent either probable cause or reasonable suspicion, did violate the Fourth Amendment. Delaware v. Prouse, 440 U.S. 648 (1979). In Prouse, a patrol officer stopped a car and smelled marijuana. Id. at 650. When the officer looked into the car, he saw the marijuana inside the vehicle. Id. Justice White, writing for the Court, stated, “An individual operating or traveling in an automobile does not lose all reasonable expectation of privacy simply because the automobile and its use are subject to government regu-
Thus it was in 1983, in *United States v. Knotts*, the Court confronted a case where Minnesota law-enforcement officers suspected Tristan Armstrong of stealing chemicals that could be used in manufacturing illicit drugs. Visual surveillance revealed that he purchased chemicals from Hawkins Chemical Co. in Minnesota. With the consent of company officials, when Armstrong next bought a container of chloroform (one of the precursor chemicals used to make drugs), the police placed a radio-frequency-enabled transmitter on the container. The police followed the container, using the tracking device and visual surveillance, to a cabin in Wisconsin. They obtained a search warrant and found a fully operable drug laboratory inside the cabin, replete with formulas for amphetamine and methamphetamine, $10,000 worth of equipment.

Professor Clancy points to this case to suggest that the case served as an early indication that, following *Katz*, "privacy might be a vital source of protection of individual interests." *Clancy*, supra note 79, at § 3.3.3. He argues, "as the composition of the Court changed," however, "those early indications gave way to a view that used privacy analysis not to expand protected individual interests but to limit the scope of the Amendment’s protections." *Id.* What emerged was a “hierarchy of privacy interests.” *Id.* Amongst the lowest level of protection is an individual’s voice, face, or handwriting, as well as travel and open fields. *Id.*

The hierarchy that Clancy identifies, though, relies on the private/public distinction as the defining feature. Lowered protections accompanied what could be seen and observed by others in public space. Clancy treats whether something is observable as only one of several potential methods adopted by the Court to distinguish between privacy interests, noting also the degree to which technological advances, empirical evidence of a subjective expectation of privacy, and degree of government regulation. *Id.* at § 3.3.4. This Article takes the stronger position, which is that the private/public distinction is a central feature of the doctrine, which remains rooted in a terrestrial understanding of a three-dimensional world, making it ill-suited to confront the challenges of a digital age.


246. *Knotts*, 460 U.S. at 278.

247. *Id.*

248. *Id.*
ment, and enough chemicals to produce 14 pounds of pure amphetamine.249

The Eighth Circuit reversed the conviction on the grounds that monitoring the radio-frequency-enabled transmitter violated the cabin owner’s reasonable expectation of privacy.250 The Supreme Court disagreed and reversed.251 In an opinion written by Chief Justice Rehnquist, the Court analyzed the question in terms of the open fields/naked eye doctrine. The transmitter was merely a battery-operated device, emitting periodic signals that could be picked up by a receiver. It allowed law enforcement to do electronically what it could do in person “on public streets and highways.”252

Rehnquist picked up on the 1974 language in Cardwell v. Lewis, which stated: “A car has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view.”253 In Knotts, Rehnquist argued, “A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.”254 The direction they took, stops they made, and their final destination could be observed.255 Just because the police relied on a radio-frequency-enabled transmitter, and not their own eyes, did not alter the situation. Rehnquist explained, “Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.”256

The respondent argued that if the Court were to adopt this rule, then there would be no limiting condition on the eventual use of 24-hour surveillance.257 The Court disagreed, suggesting that technology, in reality, was nowhere near that point. “[I]f such drag-

249. Id. at 279.
250. Id. (discussing the case below, United States v. Knotts, 662 F.2d 515 (8th Cir. 1983)).
251. Id. at 279–80.
253. Id. at 281 (quoting Cardwell v. Lewis, 417 U.S. 583, 590 (1974) (plurality opinion) (holding the warrantless search of the outside of a car to be outside the contours of the Fourth Amendment)) (also citing Rakas v. Illinois, 439 U.S. 128, 153–54 (1978) (Powell, J., concurring); South Dakota v. Opperman, 428 U.S. 364, 368 (1976)).
255. Id. at 281–82.
256. Id. at 282; see also id. at 282–83 (discussing United States v. Lee, 274 U.S. 559, 563 (1927) (finding that the use of a searchlight is comparable to the use of a marine glass or field glass and thus does not change the analysis of the reasonableness of a search on the high seas)).
257. Id. at 283.
net-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." Radio-frequency-enabled transmitters, also known as “beepers,” were merely “a more effective means of observing what is already public.”

The following year the Court confronted a similar fact pattern in United States v. Karo. The DEA had learned that James Karo and two others had ordered 50 gallons of ether to be used to extract cocaine from clothing that had been imported to the United States. Agents traced the container inside a number of homes, before tracking it to a commercial storage facility.

Unlike Knotts, where the transmitter conveyed the location of a car on public roads, in Karo the beeper informed the agent where a container was located, at a particular time and, consequently, in whose possession it was held: i.e., the person(s) whose residence was under surveillance. “Even if visual surveillance has revealed that the article to which the beeper is attached has entered the house, the later monitoring not only verifies the officers’ observations but also establishes that the article remains on the premises.” The search was less intrusive than a full-scale search, but it was still a search of the interior of the home. It therefore fell within the protections of the Fourth Amendment. The private/public distinction, and the importance of maintaining access for acquiring visual information, held. Where law-enforcement collection techniques crossed the curtilage, constitutional protections arose.

The ordinary operation of the senses continued to loom large in the Court’s jurisprudence. What individuals could observe in

258. Knotts, 460 U.S. at 284.
259. Id. (quoting United States v. Knotts, 662 F.2d 515, 518 (8th Cir. 1983)); see also id. at 285.
261. Id. at 708.
262. Id.
263. Id. at 715.
264. Id. at 716.
265. The importance of the naked eye, for instance, extends to the plain view doctrine. In Coolidge v. New Hampshire, the Supreme Court explained that under certain circumstances seizure of an item in plain view during a lawful search may be reasonable under the Fourth Amendment. 403 U.S. 443, 465 (1971). Three elements must be met: (1) the officer must be lawfully in the Fourth Amendment-protected area; (2) the item observed must be in plain view; and (3) the officer must immediately recognize the item as illegal materials, evidence, or contraband without otherwise interfering with the item. Horton v. California, 496 U.S. 128, 136–37 (1990). In Arizona v. Hicks, the Court further elaborated on what consti-
public fell outside the protections of the Fourth Amendment. Law enforcement officers should not be forced to avert their gaze to block out what the rest of the world could see.

The functional-senses test included not just what individuals could see but also what they could hear without technological assistance. A 1984 case from the Second Circuit, *United States v. Mankani*, reflected this approach. 266 Canadian law enforcement uncovered a drug-running operation that yielded nearly two tons of hashish in a barn in a rural area of Vermont. 267 Having been tipped off by Canadian authorities that two of the men involved in the shipment were in a hotel room in Burlington, a DEA agent booked the adjoining room and listened through a hole in the wall to the conversation next door. 268 The Court concluded that eavesdropping did not violate the Fourth Amendment: “[D]efendants’ conversations were overheard by the naked human ear, unaided by any . . . sensory enhancing devices. This distinction is significant because the Fourth Amendment protects conversations that cannot be heard except by means of artificial enhancement.” 269 Every time individuals spoke, they assumed the risk that someone might be privy to what they say. 270 On the other hand, once technology enhanced the senses, then the risk altered. As Justice Brennan had expressed in his dissent in *Lopez v. United States*, “There is no security from that kind of eavesdropping, no way of mitigating the risk, and so not even a residuum of true privacy.” 271

Passive observation proved central to the functional senses approach. What one could see or hear, just standing there, was not

---

266. 738 F.2d 538 (2d Cir. 1984).
267. Id. at 541; see also *United States v. Agapito*, 620 F.2d 324 (2d Cir 1980) (listening by placing one’s ear against an adjoining door does not violate the Fourth Amendment), *cert. denied*, 449 U.S. 834 (1980).
268. Mankani, 738 F.2d at 541.
269. Id. at 543; see also 1 WAYNE LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.2, at 270–72 (1st ed. 1978).
protected. But if a search involved physical manipulation, such as opening a bag, squeezing it, or feeling its contours, then the ordinary senses test did not apply.272

D. Global Positioning System Technology

GPS technology is similar to the radio frequency beepers used in *Knotts* and *Karo* in that it allows law enforcement to monitor the movements of one or more persons or objects, from a remote location, for some amount of time.273 But it differs in terms of accuracy, reliability, the verification required (impacting resources required for monitoring the device, the likelihood of detection, and the degree of intrusion), the level of detail obtained, and the potential analytical yield.274 A brief discussion of these five characteristics provides context for the types of privacy concerns raised the 2012 case of *United States v. Jones*.275

First, GPS devices are more accurate than beepers. GPS can pinpoint where a tracked device is located to within a few centimeters.276 In contrast, radio-frequency transmitters appear to provide

272. See, e.g., Bond v. United States, 529 U.S. 334, 337 (2000) (responding to the government’s claim “that by exposing his bag to the public, petitioner lost a reasonable expectation that his bag would not be physically manipulated,” by noting that *Ciraolo* and *Riley* “involved only visual, as opposed to tactile, observation.”).


only a general location.\footnote{277} The distinction means that more accu-

\footnote{(May 1, 2000), https://clinton4.nara.gov/WH/EOP/OSTP/html/0053_2.html. The decision proved essential to private sector innovation. By 2003, the technology had exploded to support a $4.7 billion market. \textit{National Workrights Institute, On Your Tracks: GPS Tracking in the Workplace} 5 (2004). Uses ranged from employers wanting to track their workers by installing GPS chips on vehicles, in badges, and on phones, to law enforcement using the information as part of criminal investigations. \textit{Id.} at 10–15.}


\footnote{277} In its reply brief in \textit{Karo}, the government stated that law enforcement officers standing on a sidewalk 25-50 feet from a home could tell whether the beeper was located in the front or back of the home, or on the right or left side. Clifford S. Fishman, \textit{Electronic Tracking Devices and the Fourth Amendment: Knotts, Karo, and the Questions Still Unanswered}, 34 Cath. U. L. Rev. 277, 282 (1985) (citing
rate data can be obtained from GPS, providing deeper insight into the individual or object under surveillance.

Second, GPS data is more reliable: beepers cannot be used in inclement weather, whereas GPS operates regardless of whether it is sunny, raining, or the middle of a blizzard.\[^{278}\] Thus for GPS, the amount (and quality) of data is not limited by natural conditions.

Third, the two systems depart in what must be done to verify the information. GPS allows for law enforcement to be located virtually anywhere.\[^{279}\] For a radio-frequency transmitter, the police have to be relatively nearby.\[^{280}\] This has several implications.

For one, it takes a considerable amount of manpower, equipment, and resources to conduct surveillance using a beeper, whereas the costs for using GPS are lower.\[^{281}\] From a resource perspective, therefore, law enforcement officers could entertain a lower level of individual suspicion before placing an individual under surveillance using GPS than might otherwise be the case for their decision to employ radio-frequency chips. Similarly, using GPS, they could choose to put multiple people under surveillance simultaneously, resulting in greater inroads into privacy because of the lowered resource commitment entailed.

For another, since police need to be nearby, drivers are more likely to be able to detect police tracking a beeper than police following GPS data.\[^{282}\] The absence of any observable government presence may have implications for the relationship of citizens to the government, as the surreptitious nature of the surveillance raises question about the extent of government activity.\[^{283}\]

---

\[^{277}\] Hutchins, supra note 273, at 418; Appellants’ Brief, supra note 274, at 57.

\[^{278}\] Scott W. Turner, GPS Surveillance, the Right to Privacy, and the Fourth Amendment, 40 COLO. L. AW. 55, 57 (2011) (“Much like [radio beepers] . . . a GPS unit can be placed on an object and observed as it is being moved. The observation can be continuous. However, because of the technology, a person does not have to be nearby to obtain its signal. The movement of an individual being tracked through a GPS device can be observed by someone sitting at a computer from essentially anywhere.”).

\[^{279}\] In Karo, the government stated that under ordinary conditions on the open road, the signal could be monitored 2-4 miles away, and up to 20 miles in the air. Once a beeper went inside premises, however, it was not always possible to identify its location. Fishman, supra note 277, at 282 (citing Reply Brief, supra note 277, at 8 n.6).

\[^{280}\] Id.

\[^{281}\] Appellants’ Brief, supra note 274, at 57.

\[^{282}\] Id.

\[^{283}\] See, e.g., Herbert, supra note 274, at 458–60 (discussing a number of incidents where individuals discovered FBI GPS surveillance devices on their cars).
extent that law enforcement agencies state that any information about GPS devices or tracking technologies is “law enforcement sensitive” (and thus refuse to release any information publicly about their use of the technologies), the concern increases.\footnote{284}

In addition, because radio-frequency enabled transmitters require the police to be in close proximity, officers cannot easily follow the person or object onto private land, within gated communities, or across borders.\footnote{285} In contrast, a GPS device may be carried virtually anywhere, including the most intimate spheres of personal and family life, without the target knowing that the information is being collected and monitored by the government. GPS data obtained on multiple people also can be correlated, showing others with whom the individual is sharing those spaces, generating insight into intimate relationships.

Fourth, GPS chips provide more detailed information than can be obtained from beepers.\footnote{286} GPS generates location data on a second-by-second basis. And it is automated, so the government can turn it on and then more or less ignore it. It can record information indefinitely, until law enforcement officials (or anyone else with access to the system) would like to look at the data, or to find (in real time) the person or object being tracked.\footnote{287} In contrast, in addition to being less accurate than GPS chips, beepers only send out periodic signals, generating smaller amounts of information. Someone has to be present to pick up the information, so less of it is captured. And beepers are only good for as long as their battery has power.

Fifth, because GPS data is detailed and digital, law enforcement can more easily combine it with other data, and synthesize and analyze an individual’s movement over lengthy periods,\footnote{288} even predicting, based on pattern analytics, the individual’s future movements. This is more than just ordinary sensory perception, to which Fourth Amendment doctrine clings. It introduces a different form of knowledge acquisition than is at stake in radio-frequency enabled transmitter tracking.\footnote{289}

\begin{footnotesize}
\begin{itemize}
\item \footnote{284. Id. at 459–61.}
\item \footnote{285. Appellants’ Brief, supra note 274, at 57.}
\item \footnote{286. Id.}
\item \footnote{287. See Hutchins, supra note 273, at 458; see also Appellants’ Brief, supra note 274, at 57, 64.}
\item \footnote{288. Appellants’ Brief, supra note 274, at 57.}
\item \footnote{289. See, e.g., State v. Jackson, 76 P.3d 217, 223 (Wash. 2003) (“We perceive a difference between the kind of uninterrupted, 24-hour a day surveillance possible through use of a GPS device, which does not depend upon whether an officer
\end{itemize}
\end{footnotesize}
In sum, compared to beepers, GPS technology is more accurate and more reliable. It requires fewer resources and is harder to detect. It provides enormous detail and can be analyzed and combined with other information to generate further insight into suspects’ lives. Law enforcement has therefore become increasingly reliant on GPS data for investigations.290 An increasing number of cases are therefore coming before the courts, challenging the warrantless use of GPS technology.

Much like the Court in *Olmstead*, when confronted by telephone communications, a number of lower courts initially treated the placement of GPS chips on vehicles consistent with the *Knotts* framework, finding that it did not constitute a search.291 Satellite-based tracking fell on the same side of the line as surveillance cameras and satellite imaging.292

A few courts, however, disagreed.293 In 2003, the state of Washington determined that, unlike binoculars or a flashlight, GPS systems did not merely enhance the natural senses.294 They provided a substitute for visual tracking, resulting in significant intrusions into individuals’ private affairs.295 The text of the Washington state constitution mattered: “no person shall be disturbed in his private af-

---


291. See, e.g., United States v. Cuevas-Perez, 640 F.3d 272, 273, 275–76 (7th Cir. 2011) (finding 60-hour GPS surveillance outside the protections of the Fourth Amendment), cert. granted and judgment vacated, 132 S. Ct. 1534 (2012); United States v. Pineda-Moreno, 591 F.3d 1212, 1217 (9th Cir. 2010), cert. granted and judgment vacated, 132 S. Ct. 1533 (2012); United States v. Marquez, 605 F.3d 604, 609–10 (8th Cir. 2010); United States v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007) (holding that GPS simply uses technology to substitute for trailing a car on a public street, which does not amount to a search within the meaning of the Fourth Amendment); United States v. McIver, 186 F.3d 1119, 1125 (9th Cir. 1999), cert. denied, 528 U.S. 1177 (2000); United States v. Moran, 349 F. Supp. 2d 425, 467 (N.D.N.Y. 2005) (holding use of a GPS device to be within the automobile exception); Osburn v. State, 44 P.3d 523 (Nev. 2002) (applying State constitution).

292. *Garcia*, 474 F.3d at 997.


294. *Jackson*, 76 P.3d at 223.

295. *Id.*
fairs, or his home invaded, without authority of law.” The Washington Supreme Court noted that the insight into individuals’ private lives that can be gleaned by GPS data is substantial:

For example, the device can provide a detailed record of travel to doctors’ offices, banks, gambling casinos, tanning salons, places of worship, political party meetings, bars, grocery stores, exercise gyms, places where children are dropped off for school, play, or day care, the upper scale restaurant and the fast food restaurant, the strip club, the opera, the baseball game, the “wrong” side of town, the family planning clinic, the labor rally.

Such information could provide details on citizens’ preferences, associations, and predilections, drawing a “detailed picture of one’s life.”

The Washington court was not alone. In People v. Lacey, a New York court similarly determined that law enforcement use of a GPS device required a warrant. In that case, a woman returned home to find two men at her back door. She chased them and took down the license plate of the black 1996 Mitsubishi Eclipse they were driving. Another incident in the same county occurred involving a black Mitsubishi, (along with a series of other local burglaries), prompting the detective in charge of the investigation to request permission from his lieutenant to place a GPS device on the car. The police then tracked the vehicle, correlated its location with a number of burglaries, and arrested the owner in the middle of a heist.

296. Wash. Const. art. 1, § 7, construed in Jackson, 76 P.3d at 222 (“The inquiry under article 1, section 7 is broader than under the Fourth Amendment to the United States Constitution.”).

297. Jackson, 76 P.3d at 223.

298. Id.


300. Id. at *1.

301. Id.

302. Id. at *1–*2.

303. Id. at *3. As the question of whether the Fourth Amendment applied to GPS devices was a case of first impression for New York, the court looked to other state cases for guidance. Id. at *5–*6, (citing, among others, State v. Jackson, 76 P.3d 217 (Wash. 2003); State v. Campbell, 759 P.2d 1040 (Or. 1988); Johnson v. State, 492 So. 2d 693, 694 (Fla. Dist. Ct. App. 1986) (holding that a beeper on a plane was “tantamount to an illegal entry and beyond the scope of the warrant’’)). However, the court in Lacey mentioned, although it did not discuss in detail, a number of cases that went the other way. 2004 WL 1040676, at *6–*7 (citing,
The court balked at the possibility that the police could place GPS devices on vehicles and follow them around indefinitely without probable cause. "The citizens of New York," Judge Joseph Calabrese stated, "have the right to be free in their property, especially in light of technological advances which have and continue to diminish this privacy."\textsuperscript{304} If it were a telephone communication, the police would have to obtain a warrant: "While the telegraph has become a relic of the past, cellular technology has become the future."\textsuperscript{305} The judge was concerned about what the future might hold:

At this time, more than ever, individuals must be given the constitutional protections necessary to their continued unfettered freedom from a "big brother" society. Other than in the most exigent circumstances, a person must feel secure that his or her every movement will not be tracked except upon a warrant based on probable cause establishing that such person has been or is about to commit a crime. Technology cannot abrogate our constitutional protections.\textsuperscript{306}

In \textit{Lacey}, Judge Calabrese boldly addressed the key question—an opportunity the Supreme Court failed to take, more than a decade later.\textsuperscript{307}

In \textit{United States v. Jones}, the Court considered a GPS chip that the police placed on the car of a suspected drug dealer’s wife and monitored for 28 days.\textsuperscript{308} Justice Scalia, writing for the Court, stated that the placement of the chip on the car, which occurred outside the period allowed by the warrant, amounted to a trespass.\textsuperscript{309} Scalia distinguished \textit{Karo}, noting that what made the placement of the
transmitter in the container of ether legal was that it was placed into the device before the target of the surveillance had possession. In contrast, the car was already in Antoine Jones’s wife’s possession when law enforcement attached the device.\textsuperscript{310} He reasoned that the case was entirely consistent with \textit{Knotts}; the holding in \textit{Knotts} merely recognized that the target had no reasonable expectation of privacy, per \textit{Katz}, in the location of the automobile carrying the container of chloroform.\textsuperscript{311} \textit{Katz}, however, had to be understood as adding to, not substituting for, the common law trespassory test. As in \textit{Karo}, “The beeper had been placed in the container before it came into Knotts’ possession, with the consent of the then-owner.”\textsuperscript{312}

Scalia reiterated that naked eye doctrine controls public space. “This Court has to date not deviated from the understanding that mere visual observation does not constitute a search.”\textsuperscript{313} What one could ascertain from ordinary senses, in public, lay beyond the reach of the Fourth Amendment. He went on to reject any privacy interest in the length of the surveillance. “[E]ven assuming that the concurrence is correct to say that ‘[t]raditional surveillance’ of Jones for a 4-week period ‘would have required a large team of agents, multiple vehicles, and perhaps aerial assistance,’ . . . our cases suggest that such visual observation is constitutionally permissible.”\textsuperscript{314} At the same time, he admitted that the Court might have to grapple with the implications of lengthy surveillance in the future: “It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.”\textsuperscript{315}

While Scalia sidestepped the hard questions presented by persistent monitoring, Justice Alito, joined in his concurrence by Justice Ginsburg, Justice Breyer, and Justice Kagan, did not.\textsuperscript{316} Alito began by drawing a parallel between the majority in \textit{Jones} and the Court in \textit{Silverman}, which (consistent with \textit{Olmstead}) had required “unauthorized physical penetration” for Fourth Amendment inter-

\begin{footnotesize}
\begin{enumerate}
\item \textit{Jones}, 132 S. Ct. at 952.
\item \textit{Id.} at 951–52.
\item \textit{Id.} at 952.
\item \textit{Id.} at 953.
\item \textit{Id.} at 953–54 (citation omitted) (quoting \textit{id.} at 963 (Alito, J., concurring)).
\item \textit{Id.} at 954.
\item \textit{Jones}, 132 S. Ct. at 958 (Alito, J., concurring).
\end{enumerate}
\end{footnotesize}
ests to arise. The \textit{Jones} majority similarly focused on physical intrusion, despite the fact that, post-\textit{Katz}, the trespass rule no longer applied. For Alito, the key question was whether the long-term monitoring of the car violated the respondent’s reasonable expectation of privacy. He concluded that it did. Technology, Alito averred, can change expectations.

Recent years have seen the emergence of many new devices that permit the monitoring of a person’s movements. In some locales, closed-circuit television video monitoring is becoming ubiquitous. On toll roads, automatic toll collection systems create a precise record of the movements of motorists who choose to make use of that convenience. Many motorists purchase cars that are equipped with devices that permit a central station to ascertain the car’s location at any time. Perhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users. Limited resources previously played a role in restricting incursions into privacy. “In the pre-computer age,” Alito explained, “the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken.” Only an important investigation would have used such means. GPS devices, however, have made “long-term monitoring relatively easy and cheap.” Short-term monitoring using the chips might be one thing, “But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.” For those offenses, society did not reasonably expect that law enforcement would “secretly monitor and catalogue every single movement of an individual’s car for a very long period.” Four weeks was too long.

\begin{itemize}
\item[317.] \textit{Id.} at 959 (citing Silverman v. United States, 365 U.S. 505, 509 (1961)).
\item[318.] \textit{Id.} at 959-60 (citing Rakas v. Illinois, 439 U.S. 128, 143 (1978); \textit{Katz} v. United States, 389 U.S. 347, 353 (1967) (finding the trespass theory “no longer controlling”)).
\item[319.] \textit{Id.} at 958.
\item[320.] \textit{Id.} at 964.
\item[321.] \textit{Id.} at 963.
\item[322.] \textit{Jones}, 132 S. Ct. at 963 (Alito, J., concurring).
\item[323.] \textit{Id.} at 963-64.
\item[324.] \textit{Id.} at 964.
\item[325.] \textit{Id.}
\item[326.] \textit{Id.}
\end{itemize}
Justice Sotomayor, in a separate concurrence, agreed. As technology advances, the government will have greater access to geolocational data. In contrast to Scalia, Sotomayor argued that longer-term monitoring impinges on expectations of privacy. Location tracking implicates other rights as well, chilling associational and expressive freedoms. “[T]he Government’s unrestrained power to assemble data that reveal private aspects of identity,” moreover, “is susceptible to abuse.” The privacy interests at stake were considerable. People did not “reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.” Such a tool, in the hands of the Executive and without any oversight, would be ripe for abuse.

While the majority decided the case on grounds of trespass, what has come to be understood as the shadow majority in Jones (the five Justices joining the Alito and Sotomayor concurrences), like the dissents in Olmstead and Goldman, and the Court in Silverman, signaled a growing concern about the impact of new technology on privacy interests protected under the Fourth Amendment.

327. See id. at 955 (Sotomayor, J., concurring).
328. See Jones, 132 S. Ct. at 955 (Sotomayor, J., concurring).
329. Id. at 955.
330. Id. at 955–56.
331. Id. at 956.
332. Id.
333. Id.
334. The Court has not limited the private/public distinction to land. In 1927 United States v. Lee considered the use of a searchlight that uncovered cases of liquor on a boat. 274 U.S. 559, 562–63 (1927). The Supreme Court determined: [N]o search on the high seas is shown. The testimony of the boatswain shows that he used a searchlight. It is not shown that there was any exploration below decks or under hatches. For aught that appears, the cases of liquor were on deck and, like the defendants, were discovered before the motorboat was boarded. Such use of a searchlight is comparable to the use of a marine glass or field glass. It is not prohibited by the Constitution. Id. at 563. Justice Brandeis, writing for the Court, was careful to note that the cases of liquor were simply sitting on the deck and not located below, so no actual entry had to occur for the officers to ascertain that the vessel was carrying contraband. Id. Following Katz, the private/public distinction persisted for searches conducted on the high seas. Like the location of the buildings on the Dow Chemical’s campus, the location of a vessel in the ocean did not “provide the setting for those intimate activities that the Fourth Amendment is intended to shelter from government interference or surveillance.” Oliver v. United States, 466 U.S. 170, 179 (1984); see also Jason R. Crance & Mike Mastry, Fourth Amendment Privacy Rights at
E. Enhanced Detection

Starting in the early 1990s, new technologies and techniques that enhanced the human senses, such as thermal imaging, or the use of narcotics dogs, began to make their way onto the Court’s docket. Despite the movement in Katz to determining privacy from the perspective of the individual (rather than the specific places being protected), the Court continued to rely upon the territorial private/public distinction, with the line drawn at the curtilage of the home.

In 1991, for instance, an agent from the U.S. Department of the Interior suspected that an Oregon resident, Danny Kyllo, was growing marijuana in his home. Knowing that successfully growing the plant indoors required the use of high intensity lamps, the

Sea and Governmental Use of Vessel Monitoring Systems: There’s Something Fishy About This, 22 J. ENVTL. L. & LITIG. 231, 246 (2007). Arguments regarding the navigation of a vessel paralleled the doctrinal approach to observing a car as it traversed public thoroughfares. See United States v. Knotts, 460 U.S. 276, 281 (1983) (quoting Cardwell v. Lewis, 417 U.S. 583, 590 (1974) (Cars have “little capacity for escaping public scrutiny” when traveling on “public thoroughfares where both its occupants and its contents are in plain view.”)). Just as the public could observe a car, so, too, could citizens see boats and ships on the open water. Combined with the nature of commercial fishing, a lower expectation of privacy held. Why should government regulators or law enforcement officers be subject to different standards?

Like radio-frequency-enabled transmitters, vessel monitoring systems (VMS) do not provide information located within the vessel, or below deck—making a Fourth Amendment search claim, under the current doctrine, somewhat questionable. Lower courts are divided on whether, and under what circumstances, a captain of a vessel has a reasonable expectation of privacy in what occurs on different parts of the vessel. Crance & Mastry, supra, at 247–48. The Fifth Circuit has adopted an approach that mirrors the distinction between open fields and matters located within the curtilage of the home. Since the Coast Guard can conduct administrative inspections of public areas without probable cause and a warrant, the captain of a vessel has no reasonable expectation of privacy in the public areas of the vessel. See id. at 247. In United States v. Freeman, the Coast Guard located the vessel by means of radar, after which it found more than 41,000 pounds of marijuana on board. 660 F.2d 1030, 1031–34 (5th Cir. 1981), discussed in Crance & Mastry, supra, at 247. In contrast to the Fifth Circuit, the First Circuit considers that the captain has a reasonable expectation of privacy to the extent that it “derives from his custodial responsibility for the ship, his associated legal power to exclude interlopers from unauthorized entry . . . and the doctrines of admiralty, which grant the captain (as well as the owner) a legal identity of interest with the vessel.” United States v. Cardona-Sandoval, 6 F.3d 15, 21 (1st Cir. 1995), quoted in Crance & Mastry, supra, at 247–48. For non-public areas of the vessel, the circuits agree that those on board do have a reasonable expectation of privacy. See, e.g., United States v. DeWeese, 632 F.2d 1267 (5th Cir. 1980), cited in Crance & Mastry, supra, at 248.

agent directed a thermal scanner at Kyllo’s triplex to detect the level of infrared radiation emanating from the structure.\(^{336}\) The scan showed a hot spot along the roof over the garage.\(^{337}\) Based on the results of the test, tips from informants, and Kyllo’s utility bills, a federal magistrate judge issued a warrant for a search that yielded 100 marijuana plants.\(^{338}\)

Justice Scalia, writing for the Court, relied on the walls of the home and the degree to which the observer’s senses had been enhanced beyond normal human abilities, to extend Fourth Amendment protections to thermal searches. “The present case,” he wrote, “involves officers on a public street engaged in more than naked-eye surveillance of a home.”\(^{339}\) Scalia acknowledged, “It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.”\(^{340}\) Aircraft had exposed the top of peoples’ homes to public view—including portions of the curtilage once considered private. Thermal imaging raised the question of whether limits existed on the “power of technology to shrink the realm of guaranteed privacy.”\(^{341}\) Detecting activity inside the home intruded upon a rule in operation since the founding of the country. “Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a ‘search’ and is presumptively unreasonable without a warrant.”\(^{342}\)

In 2013, the Court considered another sensory enhancement: this time, whether the use of canines outside of a home, to detect narcotics inside the structure, amounted to a search.\(^{343}\) The Court had previously determined that the use of dogs outside of cars, to detect narcotics inside the vehicle, was not a search.\(^{344}\) In *Florida v. Jardines*, the Miami-Dade Police Department received a tip that Joe-

\(^{336}\) *Id.*

\(^{337}\) *Id.* at 30.

\(^{338}\) *Id.*

\(^{339}\) *Id.* at 33 (emphasis added).

\(^{340}\) *Id.* at 33–34.

\(^{341}\) *Kyllo*, 533 U.S. at 34.

\(^{342}\) *Id.* at 40.


lis Jardines was growing marijuana in his home.\textsuperscript{345} Two police officers, accompanied by a drug-sniffing dog, went up onto Jardines’s front porch.\textsuperscript{346} On the basis of the dog’s positive response, as well as the tip, the police obtained a warrant to search the home and found cannabis.\textsuperscript{347}

Justice Scalia, writing for the Court, repeatedly emphasized the territorial nature of the Fourth Amendment. “The officers were gathering information in an area belonging to Jardines and immediately surrounding his house—in the curtilage of the house,” he wrote.\textsuperscript{348} “[T]hey gathered that information by physically entering and occupying the area.”\textsuperscript{349} For Scalia, the physical property proved central: “the home is first among equals.”\textsuperscript{350}

Once establishing the home as “a constitutionally protected area,” Scalia turned to whether an “unlicensed physical intrusion” had occurred.\textsuperscript{351} The naked eye, again, figured largely: “While law enforcement officers need not ‘shield their eyes’ when passing by the home ‘on public thoroughfares,’ an officer’s leave to gather information is sharply circumscribed when he steps off those thoroughfares.”\textsuperscript{352} In \textit{Ciraolo}, there had been no physical intrusion of the property.\textsuperscript{353} The fact that the police in \textit{Jardines} had used a trained animal appears to have mattered little, as the effect was the same: it altered law enforcement’s ability to detect information about a protected area that was not evident from the use of ordinary senses.

In her concurring opinion, Justice Kagan, joined by Justice Ginsburg and Justice Sotomayor, emphasized the extent to which the canine unit had augmented natural human abilities. “Here,” she wrote, “police officers came to Joelis Jardines’ door with a super-sensitive instrument, which they deployed to detect things inside that they could not perceive unassisted.”\textsuperscript{354} Not only was the use of a highly-trained dog without a warrant a violation of the Fourth Amendment, but if the officer had used “super-high-powered binoculars” to look through a window, that, too, could fall

\textsuperscript{345} 133 S. Ct. at 1413.
\textsuperscript{346} Id.
\textsuperscript{347} Id.
\textsuperscript{348} Id at 1414.
\textsuperscript{349} Id.
\textsuperscript{350} Id.
\textsuperscript{351} Jardines, 133 S. Ct. at 1415.
\textsuperscript{352} Id. (quoting California v. Ciraolo, 476 U.S. 207, 213 (1986)) (citation omitted).
\textsuperscript{353} Id.
\textsuperscript{354} Id. at 1418 (Kagan, J., concurring).
outside constitutional requirements. Kagan noted the “firm” and “bright line” that marked “the entrance to the house,” emphasizing the private/public distinction.

Even the dissent turned to some extent upon whether the officer’s ordinary senses, outside the curtilage of the home, would suffice. Justice Alito, joined by Chief Justice Roberts, Justice Kennedy, and Justice Breyer, criticized the Court for “fail[ing] to mention that, while [one detective] apparently did not personally smell the odor of marijuana coming from the house, another officer who subsequently stood on the front porch . . . did notice that smell and was able to identify it.”

F. Technological Challenges to the Private/Public Distinction

Fourth Amendment doctrine has long struggled with how to integrate new technologies into the private/public distinction. Perhaps nowhere are its failings clearer than in the realm of location tracking.

Two elements are now coming together that undermine the traditional divide. First, the proliferation of tracking technologies means that enormous amounts of locational data are being generated, providing detailed pictures of citizens’ lives. Second, the private/public distinction in Fourth Amendment doctrine ignores the possibility that the length of observation, the recording of the information, or the analysis of data obtained from the public domain could trigger a new privacy interests.

The basic argument is that if privacy is not implicated at the front end—i.e., the moment an individual sees or hears what a person says or does in public, or reads an individual’s documents or papers that are in the public domain—then the length of time that the person is placed under observation, whether the government records the information that is being generated, and whether the government later analyzes the data (potentially in combination with other information) does not give rise to any new privacy right. Zero

355. Id. (distinguishing the scenario from delivering the mail or distributing campaign flyers).
356. Id. at 1419.
plus zero is still zero. Actions in public simply are unprotected by the Fourth Amendment.

This approach is deeply problematic. Locational data, collected in bulk, yields deep insight into individuals’ lives. Continued reliance on the private/public distinction fails to capture the interests at stake in public monitoring, and in the collection and analysis of locational data.

1. Digital Tracking

The number of ways that new technologies give others the ability to follow individuals is staggering. WiFi and Bluetooth signals; GPS chips; vessel monitoring systems; RFID tags; automated license plate readers; network connection data; international mobile subscriber identity catchers; Internet protocol databases; financial transactions; consumer purchases; closed circuit televisions; remote biometric identification; and unmanned aerial systems provide just some examples.359 Tracking has become such an intrinsic feature of modern life that many people do not even realize who is tracing their footsteps. Even a brief discussion illustrates the depth of private information that is available.

Special sensors detect WiFi and Bluetooth-enabled devices, such as mobile telephones, electronic tablets, and computers, as individuals move through public space. Industry is capitalizing on this rich source of data. Companies such as LocationGenius, for instance, guarantee “crowd-sourced scoring and analytics for any location”—including retail analytics, audience profiles and impressions, on-demand real estate data, and data related to entire cities or counties for use in urban planning, migration, security, and local law enforcement.360

LocationGenius generates customer profiles based on data collected by mobile carriers. The company guarantees that the retailer will instantly know where the customer just was, as well as where their next stop is likely to be.361 It uses cellular network and device data, sensors, beacons, as well as social media data, to populate a

359. Mobile devices, Internet-connected products, and online activity constantly create data, which can be collected not just by the government, but by private companies that can then trace where people go, how long they spend in each location, and who they are with when they do so. See Armina Ligaya, You’re Being Followed: New Digital Tracking Technologies Keep Tabs on Your Every Move, FINANCIAL POST MAGAZINE, May 7, 2014, http://business.financialpost.com/financial-post-magazine/digital-tracking-privacy?__lsa=0f20-ef2c.


361. Id.
profiling engine that “plugs into postal code data, behavioural streams, census data, and . . . other in-house and third party sources,” providing retailers with customers’ household income, ethnicity, gender, educational level, employment, consumer spending, and brand preferences.\footnote{362}

LocationGenius is just one example of a burgeoning industry. The 2016 global market in consumer location information is estimated to be worth more than $16 billion.\footnote{363} Mobile marketing (the provision of personalized, time- and location-sensitive information to individuals’ mobile devices to promote goods and services) has become standard business practice.\footnote{364} The number of applications on a smart phone that collect—and sell—data about the user’s movements is extraordinary.\footnote{365} Facebook, Google, Foursquare, and Twitter are well known for this. But even seemingly innocuous applications, like Android’s popular Brightest Flashlight Free, have tracked and sold users’ location information without their knowledge.\footnote{366}


\footnote{363. See Ligaya, supra note 359.}


\footnote{365. See, e.g., About Privacy and Location Services for iOS 8 and iOS 9, Apple, https://support.apple.com/en-gb/HT203053 (last visited Nov. 19, 2016) (noting that iOS devices allow maps, camera, weather, traffic, and other apps to use information from cellular, WiFi and GPS networks, and Bluetooth, to determine users’ location; also explaining that Location Services triggers location-based system services such as Location-Based Apple Ads, Location Based Alerts, and Share My Location); see also Sig Ueland, 10 Geolocation Apps for Business, Practical Ecommerce (May 13, 2011), http://www.practicalecommerce.com/articles/2780-10-Geolocation-Apps-for-Business (describing Google Latitude; Google Maps; Google Buzz; Double Dutch; Neer; Plancast; Glympse; Foursquare; GroupMe; Hashable; Geoloqi; LiquidSpace).}

GPS chips that record locational data also have become integrated into our daily lives. In 1996, the FCC adopted rules (implemented by 2001) that required all mobile telephones to be GPS-enabled to facilitate emergency services. By 2004, even small carriers had to comply. In 2015, the FCC expanded the rule to require mobile telephone providers to build in the capability to locate cell phones indoors, including the height above ground, enabling law enforcement to pinpoint the precise location of a mobile phone inside a home, office building, or other structure. Wireless carriers do not inform users of any way to disable this function. As long as the phone is turned on, service providers can locate the telephone either through hardware built into the device, or through examining where it connects to the cell site network.

When NAVSTAR opened to commercial interests in 2000, the use of GPS expanded beyond mobile telephones to enable such varied services as access to local resources, time synchronization, and air and ground navigation. The technology is now used by airlines, farming, mining, prisons, security companies, hobbyists, and others to program and track people and objects, and to create virtual borders to monitor people, animals, or objects that enter or leave pre-set boundaries.
Vessel Monitoring Systems (VMS) consist of electronic devices that transmit the location of vessels via satellite link to a land-based receiver. The Magnuson-Stevens Fishery Conservation and Management Reauthorization Act of 2006 required that the government increase VMS data sharing among state and federal agencies. On August 9, 2006, the National Marine Fisheries Service published a regulation requiring that all vessel owners operating in the Gulf of Mexico outfit their vessels with a VMS unit. The devices must remain on and able to transmit twenty-four hours a day, regardless of where the vessel is located and irrespective of whether the vessel is engaged in commercial fishing. Although supported by environmentalists, the constitutional implications of increased use of VMS mostly have gone unnoticed.


376. But see Crance & Mastry, supra note 334, at 233–34.
tions in *Knotts* and *Karo*. As small as a grain of rice, they can be used to track goods, persons, or animals; to collect tolls; to read travel documents; to verify the authenticity of items; to time sporting events; or to regulate entry into buildings.  

---

377. A two-way radio with a microprocessor, the device sends out data that is picked up by electronic readers or antennas, to identify the location of people, cars, or objects. Battery-powered RFID chips can typically be read from a range of 300 feet (100 meters) away. *RFID Frequently Asked Questions*, RFID *Journal*, https://www.rfidjournal.com/faq/show?139.  


ties as disparate as Wal-Mart\(^\text{386}\) and the Department of Defense\(^\text{387}\) require that vendors use RFID tags to ensure more efficient supply chain management. In 2015, the global RFID market was worth just over $10 billion.\(^\text{388}\) By 2020, the market is expected to exceed $13 billion.\(^\text{389}\)

Automated license plate readers (ALPRs) pair fixed, portable, and mobile cameras with searchable databases.\(^\text{390}\) The small, high-speed cameras, which can capture thousands of car license plates per minute, can be mounted on police cars or city vehicles, as well as stationary objects, such as signs, tollbooths, or bridges. They record the license plate, as well as the date, time, and location of each car. The information is then fed into a local, state, or regional database, with differing levels of retention, depending upon the state.\(^\text{391}\)

Network-based data also yields locational data. Service providers record where users’ mobile devices connect to local towers—and not just when a telephone call is made or a text message is


\(^{390}\)Id.

\(^{391}\)Automated License Plate Recognition, INT’L ASS’N OF CHIEFS OF POLICE, http://www.iacp.org/ALPR-FAQs; AM. CIVIL LIBERTIES UNION, YOU ARE BEING TRACKED: HOW LICENSE PLATE READERS ARE BEING USED TO RECORD AMERICANS’ MOVEMENTS 18 (July 2013), https://www.aclu.org/feature/you-are-being-tracked. For differing lengths of retention compare Ark. Code (2013) §12-12-1801 to 12-12-1805 (prohibiting data retention beyond 130 days), Cal. Veh. Code (2011) §2413 (prohibiting the California Highway Patrol from retaining data from a license plate reader more than 60 days, unless the information is to be used as evidence in a felony case), Maine (2009), 29-AMRSA §2117-A(2) (setting a 21-day limit on the retention of data obtained via ALPRs), and Tenn. Code (2014) §55-10-302 (putting a 90 day limit on data retention unless the information is part of an ongoing investigation).
received, but constantly, as the user moves through space. The information provides a picture of where individuals go. The courts that have confronted the question of historical cell site location information (CSLI) have struggled with—and split over—whether or not such information is protected. In 2015, the Fourth Circuit held that “the government conducts a search . . . when it obtains and inspects a cell phone user’s historical CSLI for an extended period of time.” When the case went en banc, however, the court reversed its decision. Smith controlled. The Eleventh Circuit similarly argued that by using a telephone, mobile users voluntarily provide “location information to telephone com-


394. Law enforcement has tried to use the Stored Communications Act, as well as the Electronic Communications Privacy Act, to obtain this information. Appellants’ Brief, supra note 274, at 65. A number of courts, looking to the private nature of the information, the ex parte nature of the proceedings, and the reduced resources required, have required that law enforcement first demonstrate probable cause of a particular crime. See Appellants’ Brief, supra note 274, at 66 (citing In re United States for an Order Directing Provider of Elec. Commun. Serv. To Disclose Records to the Gov’t, 534 F. Supp. 2d 585, 586-87 (W.D. Pa. 2008)); In re Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register Device, a Trap and Trace Device, and for Geographic Location Information, 497 F. Supp. 2d 301, 302 (D.P.R. 2007); In re the Application of the United States of America for an Order Authorizing the Disclosure of Prospective Cell Site Information, 2006 U.S. Dist. LEXIS 73324, at 18, 22 (E.D. Wis. Oct. 6, 2006); In re Application of the United States for an Order Authorizing (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking, 441 F. Supp. 2d 816, 818–19 (S.D. Tex. 2006); In re United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., No. 06 CRIM. MISC.01, 2006 WL 468300 (S.D.N.Y. Feb. 28, 2006); In re United States for Orders Authorizing Installation & Use of Pen Registers & Caller Identification Devices on Tel. Nos., 416 F. Supp. 2d 390, 392 (D. Md. 2006); In re the Applications of the United States of America for Order Authorizing the Disclosure of Cell Site Information, 2005 U.S. Dist. LEXIS 43756 (D.D.C. Oct. 26, 2005); In re the Application of the United States for an Order Authorizing the Release of Prospective Cell Site Information, 407 F. Supp. 2d 132 (D.D.C. 2005).

395. United States v. Graham, 796 F.3d 332, 344–45 (4th Cir. 2015), reh’g en banc granted, 624 F. App’x 75 (4th Cir. 2015).

panies,” removing collection of that data by law enforcement from Fourth Amendment protections.\(^\text{397}\)

Myriad other ways of obtaining locational data exist. Cell-site simulators, known as “IMSI catchers,” can be used to locate mobile telephones within a particular area.\(^\text{398}\) The devices essentially pretend to be local cell towers used by mobile service providers, forcing all telephones in a given area that subscribe to the service to issue signals that can be used to locate all phones in the area.\(^\text{399}\) The location of an aircard—i.e., a cellular modem that attaches to a computer through the USB port to provide Internet access via a cellular network—can be obtained through similar means.\(^\text{400}\) Law enforcement is increasingly turning to IMSI catchers to search for individuals both inside buildings (including homes), as well as in public.\(^\text{401}\)

Individuals also can be tracked through databases that map IP addresses to geographic locations.\(^\text{402}\) Financial transactions and credit card information can be used to place individuals at a particular location at a particular time.\(^\text{403}\) Video cameras, enabled with remote biometric identification, can track individuals as they move through public space.\(^\text{404}\) Not only are there more of them, but the

\text{397. United States v. Davis, 785 F.3d 498, 512 n. 12 (11th Cir. 2015).}
\text{398. See Maryland v. Andrews, 134 A.3d 324, 345 (2016) (holding that the police violated defendant’s reasonable expectation of privacy under the 4th Amendment by using real-time cell phone information to find the precise location of an individual within a home); see also Dan Goodhin, Low-cost IMSI Catcher for 4G/LTE Networks Tracks Phones’ Precise Locations, Ars Technica (Oct. 28, 2015), http://arstechnica.com/security/2015/10/low-cost-imsi-catcher-for-4glt-networks-track-phones-precise-locations/; Stingray Tracking Devices: Who’s Got Them?, ACLU, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them (last visited Oct. 16, 2016). Note that “Stingray,” made by Harris Corporation, is one of the most well-known IMSI catchers, but there are various other models on the market.}
\text{400. See, e.g., 844 F. Supp. 2d 982, 987 (D. Ariz. 2013).}
\text{401. See, e.g., United States v. Patrick, No. 13-CR-234, 2015 WL 106158, at *2-*3 (data from carrier used to identify general location of a telephone, with an IMSI catcher, then employed to pinpoint the precise location of the telephone within an apartment), argued, No. 15-02443 (7th Cir. May 24, 2016).}
\text{402. See, e.g., What Is Geolocation of an IP Address?, IP Location Finder, www.iplocation.net.}
technologies involved in storing, analyzing, and combining the data with other sources is steadily “growing exponentially more powerful.” Even kinetic photos taken by a smart phone include location data and time and date stamps (when these functions are not disabled). Images can be read using facial recognition technology, placing particular individuals in particular places at particular times.

When cameras are mounted on unmanned aerial systems (UAS), mobile monitoring may be enabled. Drones open new ways to conduct surveillance. They can fly virtually undetected at higher altitudes, remain stationary outside buildings at lower altitudes, and follow individuals in real time. They can be programmed to track GPS chips and can be fitted with video and audio surveillance equipment, with the information continuously recorded either on the device or at a remote location. Drones can incorporate technologies ranging from remote biometric identification and heat sensors, to radar, infrared cameras, and “sniffers,” enabling them to detect particles suspended in the air.


408. See also Koerner, supra note 407, at 1133, 1150–53 (noting the unique qualities of drones and the range of technologies that they carry).


the battery time for most commercial drones is limited (up to 90 minutes in the air),\(^ {411}\) custom builds can be designed to stay aloft longer, with replacements sequenced to provide for continuous surveillance.\(^ {412}\) Not only are drones more maneuverable and in many ways more technologically sophisticated than helicopters, but they also require fewer resources to operate. While a police helicopter may cost upwards of one million dollars just for the aircraft (not to mention fuel, pilots, and other equipment), drones run in the tens to hundreds of dollars.\(^ {413}\)

Together, these and other technologies enable industry and government to collect massive amounts of information about individuals as they move through public space.\(^ {414}\) Four points here deserve notice.

First, it appears that law enforcement is making increasing use of locational information. For example, according to RAND, by 2014, 71% of state police departments were using license plate readers, while 85% of police departments stated that they planned to obtain or to expand their use of the technology.\(^ {415}\) Vermont’s statewide ALPR system yielded nearly nine million records between July 2013 and December 2014.\(^ {416}\) The Northern California Regional Intelligence Center, which covers the area from Monterey County up to Humboldt County, collected more than forty-six million

applications/areas-of-application/monitoring/ (noting use of “a thermal camera payload so that living beings . . . can be more easily detected in darkness or in dense vegetation,” and listing the range of surveillance activities that the drone can undertake).


\(^{412}\) Military drones can stay aloft for hours or days at a time, with coverage of entire cities, as well as the ability to read a milk carton from 60,000 feet in the air. Surveillance Drones, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/issues/surveillance-drones (last visited Oct. 17, 2016).

\(^{413}\) Koerner, supra note 407, at 1148–49.

\(^{414}\) Transit passes, access cards, and automated toll booth systems provide just a few of many more examples of location tracking.


lion images between May 2014 and April 2015. The impact of even a single officer using a license reader is significant: one policeman in Maryland was able to scan more than 48,000 vehicles over a 27-day period, in the process issuing 255 traffic citations and finding 26 drivers with suspended licenses, 16 vehicle-emission violations, 4 stolen cars, and 1 expired license plate.

Private industry has moved into the ALPR field. Digital Recognition Network, for instance, claims to scan 40% of all U.S. vehicles each year. They operate in conjunction with approximately 400 car repossession companies across the country, scanning up to 1800 plates per minute. The involvement of private industry has, in turn, generated more government use of the technology. Vigilant states that its ALPR database includes more than 2.8 billion plate scans, which it expands by more than seventy million scans per month. It provides the system for free to Texas law enforcement. In return, the government gives Vigilant access to outstanding court fees, which the company links to the license plates of those owing the fees. It then alerts law enforcement when the cars are found, giving officers the opportunity to pull over the cars to obtain the fees, along with a 25% processing fee, which is then given directly back to Vigilant. Vigilant’s privacy policy notes, "The images stored in the system are collected from areas visible to


418. Jeremy Hsu, 70 Percent of U.S. Police Departments Use License Plate Readers, IEEE SPECTRUM (Jul. 8, 2014), http://spectrum.ieee.org/cars-that-think/transportation/sensors/privacy-concerns-grow-as-us-police-departments-turn-to-license-plate-readers; Weigel, supra note 417 (noting that one patrol car, with four mounted ALPRs, can obtain some 10,000 images during a 12-hour shift).


420. Id.


422. Maass, supra note 421.

423. Id.

424. Id.
the public where there is no reasonable expectation of privacy.”\textsuperscript{425} The company further claims a First Amendment right to collect and disseminate the information.\textsuperscript{426} Vigilant retains the right to sell the data to anyone for commercial purposes, as well as for market research purposes.\textsuperscript{427} And it retains the information “as long as it has commercial value.”\textsuperscript{428}

Like companies, individuals also can make use of the technology. Whether in public, commercial, or private hands, the price of the scanners is steadily falling,\textsuperscript{429} even as they are subject to few, if any, legal limits.

As for cell site simulators, the ACLU, has documented sixty-six agencies in two dozen states, as well as Washington, D.C., that own and use them.\textsuperscript{430} At the federal level, the FBI; DEA; U.S. Secret Service; Immigration and Customs Enforcement; U.S. Marshals Service; Bureau of Alcohol, Tobacco, Firearms, and Explosives; Internal Revenue Service; U.S. Army; U.S. Navy; U.S. Marine Corps; U.S. National Guard; U.S. Special Operations Command; and National Security Agency all own IMSI catchers.\textsuperscript{431}

Network data collected by companies similarly appears to be a growing source of government data. Seven years ago, a Sprint/Nextel executive claimed that over the previous thirteen months, the company had received some eight million requests from law enforcement for location data.\textsuperscript{432} In 2012, a Congressional inquiry found that cell phone carriers had provided subscriber information relating to texts, locational data, and calling records, to law enforcement some 1.3 million times.\textsuperscript{433}

\begin{footnote}
\textsuperscript{426} Id.
\textsuperscript{427} Id.
\textsuperscript{428} Id.
\textsuperscript{431} Id.
\textsuperscript{432} Herbert, supra note 274, at 462 (citing Kevin Bankston, Surveillance Shocker: Sprint Received 8 Million Law Enforcement Requests for GPS Location Data in the Past Year, Electronic Frontier Foundation (Dec. 1, 2009, 1:45 PM), http://www.eff.org/deeplinks/2009/12/surveillance-shocker-sprint-received-8-million-law).
\end{footnote}
As for drones, in 2014, when a rancher refused to turn over six cows that had wandered onto his property, North Dakota law enforcement enlisted the aid of a DHS Predator drone to locate and arrest him.\textsuperscript{434} Although the state prosecutor stated that it was the first time unmanned surveillance aircraft had been used by North Dakota, between 2010 and 2012 Customs and Border Patrol had already flown nearly 700 surveillance missions for federal, state, and local law enforcement agencies.\textsuperscript{435}

Quite apart from the federal arsenal, Grand Forks County, North Dakota operates its own drones.\textsuperscript{436} In 2011, the Sheriff’s Department began training a Small Unmanned Aircraft Unit in collaboration with the University of North Dakota’s John D. Odegard School of Aerospace Sciences.\textsuperscript{437} In March 2013, the FAA explicitly authorized the Sheriff’s Department to use drones for law enforcement purposes.\textsuperscript{438} The first use of a drone during a police mission was in May 2013.\textsuperscript{439} Two years later, North Dakota became the first


\textsuperscript{437} See Press Release, supra note 436.

\textsuperscript{438} See Atherton, supra note 436.

\textsuperscript{439} Id.
state to legalize the use of armed drones, pairing surveillance concerns with non-lethal force.\textsuperscript{440}

The number of police departments using drones continues to expand.\textsuperscript{441} By 2015, some two dozen had been fully equipped in their use, with sixty more requesting FAA certification.\textsuperscript{442} Only fourteen states require a warrant prior to law enforcement using drones for surveillance.\textsuperscript{443}

The second observation to be made is that the insight provided by such data into individuals’ private lives is profound. Locational tracking shows where you go, what you do, and who you are with when you do so.\textsuperscript{444} It can reveal an individual’s identity,\textsuperscript{445} race,\textsuperscript{446}

\begin{itemize}
  \item \textsuperscript{441} Not only do police departments operate their own devices, but private drone footage has also been used in arrests. See, e.g., Jordan Pearson, \textit{Meet the ‘Drone Vigilante’ Who Spies on Sex Workers}, Motherboard (Apr. 4, 2016), http://motherboard.vice.com/read/drone-vigilante-brian-bates-johntv-oklahoma-spies-on-sex-workers?trk_source=popular.
  \item \textsuperscript{444} See generally Andrew J. Blumberg & Peter Eckersley, \textit{On Locational Privacy, and How to Avoid Losing it Forever}, \textit{Electronic Frontier Foundation}, 1–2 (Aug. 2009), https://www.eff.org/files/eff-locational-privacy.pdf (discussing how systems have “strip[ped] away” locational privacy by allowing other people to find out personal information by “consulting location databases”).
\end{itemize}
gender,\textsuperscript{447} age,\textsuperscript{448} marital status,\textsuperscript{449} religious beliefs, medical conditions, occupation,\textsuperscript{450} and intimate relationships.\textsuperscript{451} It records hobbies and predilections. And it can be used to predict where an individual is likely to be and what an individual is likely to do—and with whom—in the future.\textsuperscript{452} In 2011, the Information Systems Audit and Control Association (ISACA), a non-profit, multi-national trade organization, noted “a growing consensus that geolocation data should be classified as sensitive.”\textsuperscript{453} The organization evinced concern that “current law does not articulate a stance on the privacy and security aspect of geolocation.”\textsuperscript{454} More recently, a team of researchers from Louvain University in Belgium, and Harvard and MIT in the United States, warned that “Given the amount of information that can be inferred from mobility data, as well as the potentially large number of . . . mobility datasets available,” significant implications for privacy are on the line.\textsuperscript{455}


\textsuperscript{446} Christopher J. Riederer, Sebastian Zimmeck, Coralie Phanord, Augustin Chaintreau & Steven M. Bellovin, “I Don’t Have a Photograph, But You Can Have My Footprints.”—Revealing the Demographics of Location Data, COSN’15: PROC. 2015 ACM Conf. on Online Soc. Networks 185, 192 (Nov. 2, 2015).


\textsuperscript{448} See Brdar et al., supra note 447.

\textsuperscript{449} See Yuan et. al, supra note 447, at 297; see also Brdar et al., supra note 447.

\textsuperscript{450} See Brdar et al., supra note 447.


\textsuperscript{452} See Riederer, et al., supra note 446, at 192; Bellovin, et al., supra note 447, at 558 n.9.


\textsuperscript{454} Id.

\textsuperscript{455} See Montjoye, et al., supra note 445, at 4.
Third, the fact that industry itself is collecting this data has implications for government access to the information. As a matter of law, the Supreme Court in *Kyllo* cited the ubiquitous nature of technology as a consideration in whether individuals held a privacy interest in it. Underlying the legal argument is the same approach that marks the private/public distinction: if private corporations have access to the information, then why should the government be forced to close its eyes or cover its ears? And legal doctrine goes further: since the 1970s, the decision by consumers to entrust this data to third parties means that individuals no longer hold a privacy right in the information (see discussion, *infra* Part IV).456

Fourth, to the extent that the Fourth Amendment analysis hinges on an initial determination at the moment of collection, it does not provide for a later interest to arise as the volume of information expands. The basic argument, which Foreign Intelligence Surveillance Court (FISC) Judge Claire Eagan expressed with regard to the NSA collection of telephony metadata under Section 215 of the USA PATRIOT Act, is that zero plus zero still equals zero.457 If there is no privacy interest at the front end, then increasing the amount of time, or the volume of information, does not bring a privacy interest into being *ex nihilo*.458

The problem with applying this approach to the collection of locational data is that the private/public distinction on which it is based fails to acknowledge the additional privacy interests entailed in repeated observation. The value of aggregated information changes when there is more of it.459

As the lower courts have confronted the questions raised by these new technologies, a number have eschewed privacy considerations. In 2012, for instance, the Sixth Circuit considered law enforcement’s use of subscriber information, cell site information,


457. *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted Text]*, BR 13-09, at 9 (FISA Ct. Aug. 29, 2013), https://www.aclu.org/files/assets/br13-09-primary-order.pdf; *see also* Donohue, *Bulk Metadata*, *supra* note 6, at 867 (discussing Judge Eagan’s approach); Donohue, *Future*, *supra* note 6, at 120–21.

458. See Donohue, *Bulk Metadata*, *supra* note 6, at 867 (discussing Judge Eagan’s approach).

459. Bellovin et al., *supra* note 447, at 558–59. This approach also ignores the important role of limited resources in protecting privacy. Law enforcement only has access to a certain amount of police time. Thus, the placement of a tail on a suspect has to rise to a level of importance that would justify using the resources.
GPS real-time location, and “ping” data to find the location of a
drug dealer. The Court considered Knotts as controlling.

Judge Rogers began United States v. Skinner by stating, “When
criminals use modern technological devices to carry out criminal
acts and to reduce the possibility of detection, they can hardly com-
plain when the police take advantage of the inherent characteristics
of those very devices to catch them.” The drug runners had used
“pay as you go (and thus presumably more difficult to trace) cell
phones to communicate.” For the court, Skinner had no “reason-
able expectation of privacy in the data given off” by his phone.
Collecting the data was akin to “trailing a defendant.” That it was
more efficient, or effective, did not make it unconstitutional. A
few other courts have come to a similar conclusion for historic cell
site data.

Not all courts agree. Some state courts have come out on the
other side of the question, finding constitutional protections. The
Massachusetts Supreme Judicial Court considers mobile phone lo-
cation data to be even more concerning than the use of GPS for
cars, because of the greater privacy interests at stake. The New
Jersey Supreme Court similarly has held that cell phone location
data, in particular, blurs the distinction between public and private
space. The Florida Supreme Court similarly considers the use of
Cell site location information to constitute a search within the
meaning of the Fourth Amendment—thus triggering the need for
a prior warrant. The court warned, “the ease with which the gov-
ernment, armed with current and ever-expanding technology, can
now monitor and track our cellphones, and thus ourselves, with
minimal expenditure of funds and manpower, is just the type of
‘gradual and silent encroachment[ ]’ into the very details of our

---

461. Id. at 777.
462. Id. at 774.
463. Id.
464. Id. at 777.
465. Id. at 778.
466. See United States v. Forest, 355 F.3d 942, 951 (6th Cir. 2004) (pinging a
cell phone to make up for having lost visual contact with a suspect considered
outside Fourth Amendment protections because “the DEA agents could have ob-
tained the same information by following the car”).
467. See, e.g., United States v. Davis, 785 F.3d 498, 518 (11th Cir. 2015) (en
banc), cert. denied, 135 S. Ct. 479 (2015) (mem.); In re Application for Cell Site
Data, 724 F. 3d 600, 600 (5th Cir. 2013).
470. Tracey v. State, 152 So. 3d 504, 526 (Fla. 2014).
lives that we as a society must be vigilant to prevent.”

Other courts have taken a similar approach for historic cell site data as well as live tracking.

In sum, despite Katz’s recognition that the Fourth Amendment protects people, not places, the doctrine has doggedly held on to the property assumptions that marked Olmstead. The Supreme Court continues to rely on the curtilage of the home, and the operation of the senses as the litmus test for whether new technologies trigger Fourth Amendment interests at the outset—placing further privacy claims beyond constitutional reach. The Court’s logic is that when an individual leaves the protections of the home, anything one says or does can be seen and heard by others. Law enforcement officers, in turn, should not be forced to close their eyes or to cover their ears. They have a right to be in public, and to observe what others witness.

That may be true as far as walking down the street on a particular occasion. But for all such movements to be observed, recorded, and analyzed, another individual would have to follow us around twenty-four hours a day, for days, even months or years on end. There are two problems with this claim.

First, what one person could observe at a particular moment can be considered qualitatively different from what one person could observe at all times. There is a distinction to be drawn here between single observation and multiple incident observations. When driving down the street, for instance, it is not just unlikely, but virtually impossible for a bystander to track all of our movements in a car. Another person also could be in a car, tailing us, but as most people who have had to follow a friend just to get to one destination could attest, even on a limited basis, when both drivers know that that is the pre-arranged plan and are trying to do it,


472. See, e.g., United States v. Graham, 796 F.3d 332, 344–45 (4th Cir. 2015), rehearing en banc granted, 624 F. App’x 75 (4th Cir. 2015); In re Application for Tel. Info. Needed for a Criminal Investigation, 2015 WL 4594558 at *12 (N.D. Cal. 2015), appeal dismissed, No. 15-16760 (9th Cir. 2016).


tailing can be difficult to put into execution. Lights change. The
second car may miss the light. If the first car does not pull over to
wait, it can be difficult for the second car to catch them. One car
may need to stop at a train junction, or when a school bus stops to
let off children. An emergency vehicle may block the road, or a
pedestrian may enter a crosswalk. Other cars may cut between the
two vehicles, making it difficult to see the lead car. This may cause
the second car to miss a turn. One car may have car trouble and
have to pull over. Myriad hindrances may arise—even while follow-
ing one car, for a limited time, to get to one destination. Multiply
these factors for every destination over an indefinite period, and
the sheer unlikelihood of successfully observing every moment be-
comes clear. No bystander could collect this kind of information.

Second, no one reasonably expects that another person would
engage in such behavior. To the contrary, if someone did attempt
to monitor one’s every move, many people would regard it as not
just unacceptable but downright creepy. This is why we have tempo-
rary restraining orders. They are used to prevent others from in-
vading our private lives—even if their actions are limited to
tracking our every move in the public domain.

2. Recording and Analysis: Informants and the First Amendment

New technologies allow not just for public tracking, but also
for the recording and analysis of the data. These are two separate
steps. Yet neither operation triggers protections under the Fourth
Amendment—even though the act of recording allows for more in-
formation to be obtained, which, when analyzed, yields yet deeper
insight into an individual’s life.

a. Recording of Data

In United States v. Caceres, another case from the 1970s, the Su-
preme Court considered whether the secret recording of a private
conversation by someone privy to the communication qualified as a
search within the meaning of the Fourth Amendment. It con-

under federal law, an individual must, inter alia, demonstrate the other person’s
intent to “harass, or place under surveillance with intent to kill, injure, harass, or
intimidate another person”); Domestic Violence Civil Protection Orders (CPOs), Am. Bar
Ass’n Comm’n on Domestic & Sexual Violence (Mar. 2014) (listing all state TRO
laws, also known as civil protection orders, civil harassment restraining orders, or
stalking protective orders), http://www.americanbar.org/content/dam/aba/adminis-
trative/domestic_violence1/Resources/statutorysummarycharts/2014%20
CPO%20Availability%20Chart.authcheckdam.pdf.

cluded that it did not: "Neither the Constitution nor any Act of Congress requires that official approval be secured before conversations are overheard or recorded by Government agents with the consent of one of the conversants." The information merely reproduced what the agent could have written down, so no further privacy interest was implicated.

In its ruling, the Court relied on a series of cases, in which the Court had considered whether the recording of the information altered the quality of the privacy intrusion and concluded that it had not.

The first case in the series was the 1952 case of On Lee v. United States, in which an undercover agent, wired with a microphone, was sent into the suspect’s laundromat to obtain incriminating evidence. An agent from the Bureau of Narcotics, who listened to the conversations inside the laundromat from a remote location, later testified at trial. Writing on behalf of the Court, Justice Jackson suggested that by allowing the agent onto his premises, and divulging incriminating information, On Lee had consented to law enforcement access to the information.

Just over a decade later, the Court considered a similar fact pattern in Lopez v. United States. This time, an agent from the Internal Revenue Service wore a recording device. The Court rejected the argument that the defendant had a "constitutional right to rely on possible flaws in the agent’s memory, or to challenge the agent’s credibility without being beset by corroborating evidence that is not susceptible of impeachment." To the contrary, “the risk that petitioner took in offering a bribe . . . fairly included the risk that the offer would be accurately reproduced in court, whether by faultless memory or mechanical recording.” The device had not intercepted new information. It had just allowed for the information that was conveyed to the informant to be relayed more accurately in court.

The pattern continued. In Hoffa v. United States, the Supreme Court determined that a government informant relaying conversa-
tions to federal law enforcement agents did not violate the Fourth Amendment, on the grounds that Jimmy Hoffa invited the informant into the room. In *Lewis v. United States*, the Court again ruled the evidence admissible on the grounds that the defendant had invited the undercover agent into his home on numerous occasions. These cases emphasized the voluntariness of the person confiding information in another person.

The informant cases also came down on the side of encouraging, rather than discouraging, the collection of *more accurate* information. That it was done with the aid of technology, and not via ordinary recall using human capacities, mattered little. In the Court’s view, it was not different information that was being obtained, but simply information that more closely reflected what actually occurred. If it could be heard in the first place, then whether or not the brain had the ability to recall such detailed information was of little or no consequence.

*Katz* did little to alter the Court’s view of the recording of information. Justice White cited the informant cases in his concurrence, stating (in dicta) that they had been “undisturbed” by the Court’s ruling.

Subsequent cases substantiated Justice White’s claim. In 1971, in *United States v. White*, law enforcement officers recorded conversations between an informer and a suspect. When the informer could not be located for the trial, the prosecution substituted the electronic recording. The Court found no Fourth Amendment issue: “[A] police agent who conceals his police connections may write down for official use his conversations with a defendant and testify concerning them, without a warrant authorizing his encounters with the defendant and without otherwise violating the latter’s Fourth Amendment rights.”

For the Supreme Court, there was no difference among an informer (a) writing down his recollections of the conversation, (b) recording the conversation with equipment secreted on his person, or (c) carrying equipment that transmitted the conversation to law enforcement officers or to recording devices. The Court ex-

---

490. Id.
491. Id. at 751 (citing Hoffa v. United States, 385 U.S. 293, 300–03 (1966)).
492. Id.
plained, “If the conduct and revelations of an agent operating without electronic equipment do not invade the defendant’s constitutionally justifiable expectations of privacy, neither does a simultaneous recording of the same conversations made by the agent or by others from transmissions.”

In undertaking criminal enterprises, one of the risks is that those with whom one deals are untrustworthy. While the informer’s unavailability at trial might raise evidentiary problems or introduce potential questions of prosecutorial misconduct, it was immaterial as to whether the recording itself invaded the target’s Fourth Amendment rights.494 There was no appreciable difference between someone witnessing something happen and later recording it, and documenting what was said real-time, by, or with the consent of, individuals privy to the conversation.

Translated into private/public space doctrine, the potential for the government to record activity would fall outside the confines of the Fourth Amendment. What a police officer—or, indeed, any citizen—could witness in public would incur no further intrusion into an individual’s privacy if the officer—or citizen—recorded it as it was happening.

In 1972, the Court confronted a similar private/public scenario and, in the context of the First Amendment, adopted a parallel approach. It was an era of civil unrest. The Department of the Army was called upon to assist local authorities in Detroit. Protesters brought a class action suit in District Court, seeking relief for their claim that the military’s surveillance of lawful political activity undermined their First Amendment rights.495 The data-gathering system used by the military placed the Army in a law enforcement role.

Just as the Court in the Fourth Amendment cases looked to the ability of ordinary citizens to access the same data as a metric for the scope of government power, so, too, did the Appellate Court and, later, the Supreme Court, look to ordinary police powers to assess what access to information should be provided to the military. The Court of Appeals explained, “To quell disturbances or to prevent further disturbances, the Army needs the same tools and, most importantly, the same information to which local police have

---

493. Id.
494. White, 401 U.S. at 754.
access.” Indeed, it may have even greater need than the local police, since they may be unfamiliar with the local population.\footnote{496. \textit{Id.} at 5 ("Since the Army is sent into territory almost invariably unfamiliar to most soldiers and their commanders, their need for information is likely to be greater than that of the hometown policeman.").}

The Army discharged its mission by collecting information about public meetings. It came from various sources:

\[\text{T}\]he principal sources of information were the news media and publications in general circulation. Some of the information came from Army Intelligence agents who attended meetings that were open to the public and who wrote field reports describing the meetings, giving such data as the name of the sponsoring organization, the identity of speakers, the approximate number of persons in attendance, and an indication of whether any disorder occurred.\footnote{497. \textit{Id.} at 6.}

Other information was derived from local police and other civilian law enforcement agencies.\footnote{498. \textit{Id.}.}

The Supreme Court considered—and rejected—the proposition that recording public meetings had any First Amendment chilling effect. To the contrary, the burden lay on those who attended the meetings to demonstrate the danger of direct injury.\footnote{499. \textit{Id.} at 14–15.}

\textit{White} dealt with taking notes from a recorded conversation.\footnote{500. 401 U.S. 745, 746–47 (1971) (plurality opinion).} The Supreme Court has not yet addressed video recordings or photographs. But two lower decisions have.

The first was the 1975 case of \textit{Philadelphia Yearly Meeting of Religious Society of Friends v. Tate}.\footnote{501. Phila. Yearly Meeting of Religious Soc’y of Friends v. Tate, 519 F.2d 1335, 1336–37 (1974).} The Philadelphia Police Department had amassed files on about 18,000 people and organizations, including information about their political views, personal associations, personal lives, and habits. In June 1970, officers publicly announced the names of some of the individuals who had been placed under surveillance. People involved brought suit, asserting that the practice of collecting information on citizens lacked any nexus to legitimate police purposes and deprived them of their right to anonymity with regard to their political activities and associations. The plaintiffs argued that the collection chilled their free exercise of speech and assembly and interfered with their abil-
ity to form lawful political associations that represented unpopular views.\textsuperscript{502}

The District Court disagreed. Consistent with \textit{Laird v. Tatum}, the fact that the police were engaged in an investigation did not chill the citizens’ right to free speech.\textsuperscript{503} The Court of Appeals reversed in part and affirmed in part, finding no additional Fourth Amendment interest.\textsuperscript{504} “[M]ere police photographing and data gathering at public meetings” did not create any constitutional questions—nor did sharing it with other agencies with law enforcement interests.\textsuperscript{505} Where the department went outside acceptable bounds was by going on national television and informing the public who they had under surveillance.\textsuperscript{506}

This decision reflected the private/public distinction, and it accepted that the recording of the information itself did not change the quality of its collection as a matter of constitutional law. What is odd about the case is that the distinction it drew—namely with whom the information was shared—was determined after collection. It sidestepped whether the recording of the data in the first place qualified as a search within the meaning of the Fourth Amendment.

In the 1970s, the Fourth Circuit considered the potential First Amendment violation by law enforcement taking pictures at public meetings and demonstrations.\textsuperscript{507} It was common practice at the time for police to photograph vigils, demonstrations, protests, and political meetings, regardless of whether they were peaceful or threatened violent behavior.\textsuperscript{508} Judge Donald Russell, writing for the Court, determined that there had not been any constitutional intrusion.\textsuperscript{509} He discounted any feeling of intimidation, citing to \textit{Laird v. Tatum}, to claim that simply knowing one was under surveil-

\begin{thebibliography}{99}
\item 502. \textit{Id.} at 1337.
\item 503. Phila. Yearly Meeting of Religious Soc’y of Friends v. Tate, 382 F.Supp. 547, 549 (1974); 408 U.S. 14 (Burger, J.), (noting that a broad-scale investigation was underway).
\item 504. \textit{Tate}, 519 F.2d at 1339.
\item 505. \textit{Id.} at 1337–38.
\item 506. \textit{Id.} at 1339 (“It cannot be doubted that disclosure on nationwide television that certain named persons or organizations are subjects of police intelligence files has a potential for a substantial adverse impact on such persons and organizations even though tangible evidence of the impact may be difficult, if not impossible, to obtain.”).
\item 508. \textit{Id.} at 197–98.
\item 509. \textit{Id.} at 199.
\end{thebibliography}
lance was not sufficient to find a chilling effect.\textsuperscript{510} The court was skeptical that those attending the rally really did feel intimidated by the presence of the cameras: “They did not object to being photographed; to the contrary, they solicited publicity both for their meetings and for themselves by inviting representatives of the news media, including photographers, to be present.”\textsuperscript{511} By holding a public meeting, in a public space, where ordinary citizens and news outlets would see and hear what was being said, the targets of the surveillance relinquished their right to prevent the government from recording what they said and did.

In his dissent, Judge Winter distinguished the case from \textit{Tatum}, noting that a number of individuals were photographed “without their permission and inferably against their will, while they were engaged in the peaceful exercise of their First Amendment right to assemble and [in some cases] to petition their government for a redress of their grievances.”\textsuperscript{512} In \textit{Tatum} there was only knowledge of the surveillance program; in contrast, “here there was actual exposure to the challenged police methods.”\textsuperscript{513} That, in itself, provided “proof that actual harm and an actual violation of rights had occurred.”\textsuperscript{514}

The Chief of Police in Richmond, Virginia, and those who reported to him, decided which meetings to attend to identify leaders, to track people who may be travelling between meetings to stir up trouble, to deter violence and vandalism, and to protect peaceful demonstrators from counterdemonstrations.\textsuperscript{515} Judge Winter was not persuaded that these objectives were furthered by the practice of photographing all attendees, or that the same objective could not be accomplished by means that did not interfere with otherwise protected First Amendment activities.\textsuperscript{516} Law enforcement already knew who the leaders were, which made the efforts to intimidate the entire crowd concerning. He rejected the possibility that the police would use the photographs to identify unknown people.\textsuperscript{517}

\textsuperscript{510} \textit{Id.} at 201.
\textsuperscript{511} \textit{Id.} at 200.
\textsuperscript{512} \textit{Id.} at 204 (Winter, J., dissenting).
\textsuperscript{513} \textit{Donohoe}, 465 F.2d at 205.
\textsuperscript{514} \textit{Id.}
\textsuperscript{515} \textit{Id.} at 206.
\textsuperscript{516} \textit{Id.} at 207.
\textsuperscript{517} \textit{Id.} at 206 (“I cannot suppose that every time a picture is taken of an unknown person it is sent to the FBI in order to determine whether that person is dangerous.”).
Judge Winter’s words appear almost quaint in an age of drones, big data, and biometric identification. In June 2015, the Associated Press reported that the Federal Bureau of Investigation (FBI) was using low-flying planes carrying video and cellphone devices. Over a thirty-day period, the FBI flew the planes over more than thirty cities in eleven states across the country. Using a quadcopter fitted with cameras, facial recognition technologies, and social media, it is conceivable that most people in a crowd could be instantaneously identified. Yet, under the current doctrine, even if a chilling effect might result, it might well be insufficient to prevent law enforcement from collecting the information. In the words of Justice Black in 1971:

Where a statute [or police practice] does not directly abridge free speech, but – while regulating a subject within the State’s power—tends to have the incidental effect of inhibiting First Amendment rights, it is well settled that the statute [or police practice] can be upheld if the effect on speech is minor in relation to the need for control of the conduct and the lack of alternative means for doing so.

The recording of the information enhances the information beyond normal senses, or even the human brain. The data, moreover, can be combined with other input to construct detailed pictures of individuals’ lives.

Far from appreciating the privacy interests entailed, the courts are refusing to acknowledge the considerable interests at stake. In February 2016, the Sixth Circuit Court of Appeals considered a case in which law enforcement placed a suspect’s home under surveillance for two and a half months. In 2012, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) had received a tip from the local sheriff in Tennessee that Rocky Houston, a convicted felon, had firearms at his residence. ATF, claiming that they were unable to observe the farm for any length of time because their cars “[stuck] out like a sore thumb,” installed a camera at the top of a public utility pole overlooking his farm. For ten weeks, the cam-

519. Id.
523. Id. at 280.
era broadcast its recordings via an encrypted signal to an IP address accessed with a login and password. At trial, ATF showed footage of Houston holding firearms seven times during the ten week period.

The Court dismissed the possibility that any constitutional interest was at stake:

There is no Fourth Amendment violation, because Houston had no reasonable expectation of privacy in video footage recorded by a camera that was located on top of a public utility pole that captured the same views enjoyed by passersby on public roads. The ATF agents only observed what Houston made public to any person traveling on the roads surrounding the farm.

The length of the surveillance had no effect, “because the Fourth Amendment does not punish law enforcement for using technology to more efficiently conduct their investigations.” That technology made it easier and cheaper to track people for a longer time was of no consequence. “While the ATF agents could have stationed agents round-the-clock to observe Houston’s farm in person, the fact that they instead used a camera to conduct the surveillance does not make the surveillance unconstitutional.”

If a member of the public could observe, with his/her naked eye, what was happening on the farm, the fact that the same person could observe it for weeks on end was unremarkable—as was the fact that the information happened to be recorded. So why could law enforcement not do the same? And if there was no privacy interest at the outset, then the fact that the observation went on for ten weeks at a time had little import. Zero plus zero equals zero.

This approach is disturbing in a digital age, in which the privacy interests implicated by new and emerging tracking technologies are considerable. It also sidesteps the important role that resource limitations have previously played in protecting citizens’ privacy. Regardless of who is watching, ten weeks of surveillance implicates a range of privacy interests. As more information can be obtained from public space about the actions of individuals, incursions into the privacy sphere become deeper. The failure of Fourth Amendment doctrine lies in its inability to stem the steady constriction of the right to privacy based on the private/public distinction.

524. Id.
525. Id.
526. Id. at 286–88.
527. Id. at 288.
528. Houston, 813 F.3d at 288.
IV. PERSONAL INFORMATION VERSUS THIRD-PARTY DATA

A second distinction in Fourth Amendment doctrine centers on the difference between private information and data entrusted to others. So-called “third-party doctrine” finds its origins in the informer cases, where the Court consistently held that information entrusted to others became divested of any privacy interest.

As aforementioned, in his concurrence in *Katz*, Justice White cited to *On Lee*, *Hoffa*, and *Lopez* in support of the proposition that what is exposed to other people implies an assumption of risk that the individual in whom one confides will make public what he has been told. As the Fourth Amendment does not protect against unreliable associates, “[i]t is but a logical and reasonable extension of this principle that a man take the risk that his hearer, free to memorize what he hears for later verbatim repetitions, is instead recording it or transmitting it to another.”529 White distinguished the informer cases from *Katz*, noting that in the case of the gambler, he had “‘sought to exclude . . . the uninvited ear,’ and spoke under circumstances in which a reasonable person would assume that uninvited ears were not listening.”530

While White’s concurrence sought to preserve the informer doctrine, it also laid the groundwork for third-party doctrine, which came to fruition in cases from the 1970s. *Miller v. United States*531 and *Smith v. Maryland*,532 and their progeny, stand for the proposition that while an individual may have an interest in information in her possession, as soon as it is conveyed to a third party, it no longer enjoys the same protections under the Fourth Amendment.

The concept of secrecy lies at the heart of the doctrine: what one keeps secret is private, while what one voluntarily exposes to others is no longer so. Relatedly, the most trenchant criticism of the private information/third-party data distinction revolves around the claim of voluntariness. In the contemporary world, it is impossible to live one’s daily life without entrusting a significant amount of information to third parties.533 To say that we therefore voluntarily

---

530. Id. (quoting id. at 351 (majority opinion)).
assume the risk that such information will be made public denies
the role that technology plays. This phenomenon can be thought of
as "digital dependence."

A. Information Entrusted to Others

In 1976, the Court took up a critical question raised by Katz,
which was whether the terrestrial distinction drawn at the border of
the home would break down with regard to information held by a
bank. In Miller v. United States, ATF suspected that Mitch Miller had
failed to pay a liquor tax on whiskey and distilling equipment in his
possession. ATF agents served subpoenas on the Citizens and
Southern National Bank of Warner Robins and the Bank of Byron
to obtain Miller's financial records. The banks subsequently pro-
vided all checks, deposit slips, financial statements, and monthly
statements for grand jury deliberations.

Justice Powell, delivering the opinion of the Court, cited back
to Hoffa in support of the idea that an actual intrusion into a private
sphere had to occur for a Fourth Amendment interest to be impli-
cated. He rejected any privacy interest in the records on the
grounds that “checks are not confidential communications but neg-
gotiable instruments to be used in commercial transactions.” Powell
underscored the voluntary nature of the relationship be-
tween Miller and the bank: “All of the documents obtained, includ-
ing financial statements and deposit slips, contain only information
voluntarily conveyed to the banks and exposed to their employees
in the ordinary course of business.” Referencing the informer
cases, Powell asserted, “The depositor takes the risk, in revealing his
affairs to another, that the information will be conveyed by that per-
to the Government.” He concluded, “Since no Fourth
Amendment interests of the depositor are implicated here, this case
is governed by the general rule that the issuance of a subpoena to a
third party to obtain the records of that party does not violate the

service providers for their daily lives and suggesting that companies, in turn, are
becoming increasingly intermingled with government agencies); Brenner, supra
note 78, at 52–59 (underscoring the danger of failing to recognize any privacy
interest in the rapidly expanding amount of information entrusted to third
parties).

534. Miller, 425 U.S. at 436.
535. Id. at 437.
536. Id.
537. Id. at 440.
538. Id. at 442.
539. Id.
540. Miller, 425 U.S. at 443 (citing White, Lopez, and Hoffa).
rights of a defendant, even if a criminal prosecution is contemplated at the time the subpoena is issued.\footnote{541}

Justice Brennan strenuously objected to the Court’s decision. He noted that the Supreme Court of California, which had a clause virtually \textit{in haece verba} as the Fourth Amendment, had come to precisely the opposite conclusion. In \textit{Burrows v. Superior Court}, a bank had voluntarily turned over an accused’s financial records to the government.\footnote{542} The California Supreme Court had determined that individuals do have a reasonable expectation of privacy in their bank records, and Brennan agreed: “That the bank alters the form in which it records the information transmitted to it by the depositor to show the receipt and disbursement of money on a bank statement does not diminish the depositor’s anticipation of privacy in matters which he confides to the bank.”\footnote{543} The reasonable expectation was that, absent compulsion via legal process, whatever a customer reveals to a bank would only be used for internal banking purposes.\footnote{544} For the Supreme Court of California, whether or not a bank voluntarily turned its customer’s records over to the police was irrelevant. Brennan agreed.

Justice Marshall also dissented in \textit{Miller}, arguing, like Brennan, that the Bank Secrecy Act, which required banks to maintain customers’ records, was unconstitutional on its face.\footnote{545} He also pointed out an apparent irony: while the majority in \textit{California Bankers Association v. Shultz} had deemed the Fourth Amendment claims to be too premature to challenge the mandatory recordkeeping provisions in the statute, the Court now concluded that once the banks had been forced to keep customer records, any effort by the customer to assert a Fourth Amendment interest was too late.\footnote{546}

Three years later, the Court again considered third-party information in \textit{Smith v. Maryland}.\footnote{547} In that case, Patricia McDonough had been robbed.\footnote{548} She provided a description of a 1975 Monte

\footnotesize
\begin{itemize}
\item \footnote{541}{\textit{Id.} at 444.}
\item \footnote{542}{\textit{Id.} at 447–48 (Brennan, J., dissenting) (citing \textit{Burrows v. Superior Court}, 529 P.2d 590, 593 (Cal. 1974)).}
\item \footnote{543}{\textit{Id.} at 448–49.}
\item \footnote{544}{\textit{Id.} at 449.}
\item \footnote{545}{\textit{Id.} at 455–56 (Marshall, J., dissenting).}
\item \footnote{547}{\textit{Smith v. Maryland}, 442 U.S. 735, 743–44 (1979); \textit{see also Donohue, Future}, supra note 6, at 119–21; Donohue, \textit{Bulk Metadata}, supra note 6, at 868–69 (summarizing \textit{Smith}).}
\item \footnote{548}{\textit{Smith}, 442 U.S. at 737.}
\end{itemize}
Carlo parked at the scene of the crime to the police. When she returned home, a man telephoned her repeatedly, identifying himself as the person who had robbed her, and threatening her. At one point, he directed that she come out onto her porch, where she saw the Monte Carlo drive slowly past her home. McDonough telephoned the police, who saw the vehicle and ran the plates, determining that it belonged to Michael Lee Smith. They approached the telephone company and asked if it would be possible to put a pen register and trap and trace device on Smith’s telephone line to see whether he was the person calling McDonough. The telephone company agreed. Within hours, Smith again telephoned McDonough. The police used the information to obtain a search warrant of Smith’s home which, when executed, yielded a phone book, with a page turned down to McDonough’s name.

Citing New York Telephone Company, the Court noted that the collection of the numbers dialed from the landline had not intercepted any content. “Given a pen register’s limited capabilities, therefore,” Justice Blackmun wrote, the argument that the installation and use of a pen register constituted a search rested upon whether petitioner had a legitimate expectation of privacy in the numbers dialed from his phone. The Court determined that he did not.

For the Court, telephone subscribers knew, when dialing, that they were conveying the numbers to the company, since the information was required to connect the call. They further realized that the company would make records of the numbers dialed. This is what allowed customers to be billed for long-distance calls. Similarly, even if most people were oblivious as to how telephone companies operated, they would nevertheless have some

549. Id.
550. Id.
551. Id.
552. Id.
553. Id.
554. Smith, 442 U.S. at 737.
555. Id.
556. See discussion, infra.
557. Smith, 442 U.S. at 741.
558. Id. at 742.
559. Id.
560. Id.
561. Id.
562. Id.
awareness that a pen register might be employed to identify individuals “making annoying or obscene calls.” The site of the call—in this case, inside the home—was immaterial:

Although petitioner’s conduct may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed. Regardless of his location, petitioner had to convey that number to the telephone company in precisely the same way if he wished to complete his call.

Even if the petitioner did have an expectation of privacy, the Court determined that he did not have one that society was willing to recognize as reasonable. Citing to Miller, as well as a string of informer cases (Lopez, Hoffa, and White), Justice Blackmun noted that the Court had consistently “held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.”

Justice Stewart, joined by Justice Brennan, dissented, as did Justice Marshall, joined by Justice Brennan. Stewart began by noting that in the years that had elapsed since Katz, telephones had become even more embedded in contemporary culture. The fact that the telephone company used the numbers dialed for billing purposes said nothing about the underlying privacy interests. To place a call, individuals had to contract with the company. Yet the Court had recognized a privacy interest in the conversation conducted over the wires—even though the telephone company had the capacity to record it. Just because individuals also confided the number dialed to the telephone company, it did not follow that they necessarily had no interest in the information. “I think,” Stewart wrote, “that the numbers dialed from a private telephone—like the conversations that occur during a call—are within the constitutional protection recognized in Katz.” The numbers might be more prosaic than the actual conversation, but they were “not without ‘content.’” They could reveal the identities of those with

563. Smith, 442 U.S. at 742.
564. Id. at 743.
565. Id. at 743–44.
566. Id. at 746 (Stewart, J., dissenting); Id. at 748 (Marshall, J., dissenting).
567. Id., 442 U.S. at 746 (Stewart, J., dissenting).
568. Id. at 746–47.
569. Smith, 442 U.S. at 747 (Stewart, J., dissenting).
570. Id. at 748.
whom an individual was in contact, divulging “the most intimate
details of a person’s life.”

Justice Marshall, in turn, attacked the Court’s surmise that sub-
scribers have no subjective expectation of privacy in the numbers
dialed. Even assuming that they know that the company may moni-
tor communications for internal reasons, it did not follow that they
expected the company to turn the numbers dialed over to the pub-
lic or to the government. “Privacy,” he wrote, “is not a discrete com-
modity, possessed absolutely or not at all. Those who disclose
certain facts to a bank or phone company for a limited business
purpose need not assume that this information will be released to
other persons for other purposes.”

Marshall raised further concerns that the Court’s holding
meant that those who contract with third parties assume the risk
that the third party might disclose the information to the govern-
ment. He laid forth two objections. First, “[i]mplicit in the concept
of assumption of risk is some notion of choice.” In the informant
cases, this was how the Court had considered the information later
related during court proceedings. But in the case of a pen register,
“unless a person is prepared to forego use of what for many has
become a personal or professional necessity, he cannot help but
accept the risk of surveillance.” It made no sense to talk about
“assuming the risk,” as if it were a choice, when, in order to live in
the contemporary world, one in effect had no choice but to use a
telephone.

Marshall’s second objection was that risk analysis was an inap-
propriate tool. It allowed the government to set the contours of the
Fourth Amendment. Under the Court’s logic, “law enforcement of-
fficials, simply by announcing their intent to monitor the content of
random samples of first-class mail or private phone conversations,
could put the public on notice of the risks they would thereafter
assume in such communications.” The question ought not to be
what risks an individual presumably accepts by providing informa-
tion to third parties, but what risks an individual “should be forced
to assume in a free and open society.”

571. Id.
572. Id. at 749 (Marshall, J., dissenting) (citing his own dissent in California
573. Id.
574. Id. at 750.
576. Id.
Marshall’s words proved prescient. He noted that the use of pen registers constituted “an extensive intrusion. To hold otherwise ignores the vital role telephonic communication plays in our personal and professional relationships.” Marshall’s words hearkened back to the majority in *Katz*, which had acknowledged the “vital role that the public telephone has come to play in private communication[s].” Increasing dependence on the telephone meant that Fourth Amendment protections needed to come into play. For Marshall, the privacy rights of all citizens were at stake: “The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide. Many individuals, including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts.” The costs of allowing the government access to such data are borne in freedom of association and freedom of the press—both hallmarks “of a truly free society.” The government, moreover, was prone to abuse such powers: “Particularly given the Government’s previous reliance on warrantless telephonic surveillance to trace reporters’ sources and monitor protected political activity, I am unwilling to insulate use of pen registers from independent judicial review."

**B. Digital Dependence**

In an era of increasing digital dependence, the arguments that Justices Stewart and Marshall put forth in *Smith v. Maryland* have become even more poignant. To say that every time individuals

---

577. *Id.* at 751.
580. *Id.*
582. Some scholars have argued, for similar reasons, for limits on subpoena powers. *See, e.g.*, Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 *COLUM. L. REV.* 279, 309–10 (2005) (suggesting that “[t]he increase in the amount and importance of information stored with third parties in a network environment creates the need for new limits on the subpoena power,” and arguing that “new
use their mobile phone they assume the risk that their data will be
turned over to the government implies that people have no privacy
interest in their communications, regardless of their substance and
any effort to keep the information confidential.\footnote{583} But unlike the
informer cases, where one has the capacity to mediate one’s inti-
mate relations, there is no meaningful choice in today’s world as to
whether or not a digital footprint is created as we go about our daily
lives. Every time we make a call, drive our car, send an email, con-
duct an online search, or even walk down the street carrying a mo-
bile device, we leave a trail.

For more than a decade, scholars have written about the
changing world in which we live, raising the alarm that our increas-
ing digital dependence is leading to a loss of privacy.\footnote{584} Never-
theless, the judiciary has failed to provide a backstop on the steadily
diminishing zone of privacy that results from third party doc-
trine.\footnote{585} The Court’s view, however, may be evolving.

In United States v. Jones, Justice Sotomayor suggested in her con-
currence that in light of the deep privacy interests implicated by
data entrusted to third parties, she might jettison third party doc-
trules should respond to the new privacy threats raised by third-party possession of
private information made commonplace by computer networks and the Internet”).

583. See Brenner, supra note 78, at 68 (“[T]he assumption of risk’ calculus is
an unreasonable methodology for a non-spatial world. It assumes . . . that I have a
choice: to reveal information by leaving it unprotected or to shield it from ‘public’
view. In the real, physical world, these options make sense . . . . But how can I do
this in a world of pervasive technology, a world in which I am necessarily sur-
rounded by devices that collect data and share it with external entities?”).

584. See e.g., Patricia L. Belia & Susan Freiwald, Fourth Amendment Protection for
Stored E-Email, 2008 U. Chi. Legal F. 121, 123–24 (2008); Daniel J. Solove, Digital
Dossiers and the Dissipation of Fourth Amendment Privacy, 75 S. Cal. L. Rev. 1083, 1084
(2002); see also Ilana R. Kattan, Note, Cloudy Privacy Protections: Why the Stored
Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud, 13
Vand. J. Ent. & Tech. L. 617, 619 (2011); Christopher R. Ott, Note, Your Digital
Leash: The Interaction Between Cell Phone-Based GPS Technology and Privacy Rights in
United States v. Skinner, 45 U. Tol. L. Rev. 377, 377–78 (2014); see generally Bag-
ley, supra note 534; Bellovin et al., supra note 447 at 559, n.8; Marc Jonathan Blitz,
The Fourth Amendment Future of Public Surveillance: Remote Recording and Other Searches
in Public Space, 63 Am. U. L. Rev. 21, 26 (2013); Marc Jonathan Blitz, Video Surveil-
ance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that
Tracks Image and Identity, 82 Tex. L. Rev. 1349, 1353 (2004); Brenner, supra note
78; Jonathan Zittrain, Searches and Seizures in a Networked World, 119 Harv. L. Rev. F.

585. Lower courts continue to hold the doctrinal line. See, e.g., United States
As aforementioned, in *Jones*, law enforcement had placed a GPS chip on a car without a warrant and tracked it for twenty-eight days. Although the Court ruled on grounds of trespass, Sotomayor raised concern about the extent to which surveillance techniques that did not require physical intrusion impacted significant privacy interests. In light of the ubiquitous nature of digital technologies, she wrote, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." Citing to *Smith* and *Miller*, she recognized, "[t]his approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." Sotomayor explained:

People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.

Warrantless disclosures of, for instance, every web site visited over the past year surely held an implication for individual privacy. "[W]hatever the societal expectations," Sotomayor contemplated, "they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy." Not to put the point too bluntly, "I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."

---


587. 132 S.Ct. at 948 (Scalia, J.).

588. *Id.* at 957 (Sotomayor, J., concurring).

589. *Id.*

590. *Id.*

591. *Id.*

592. *Id.*
The Supreme Court’s continued emphasis on voluntary disclosure, and not on the government’s requirement that the third party turn over the information in question, departs from the facts of Smith with lasting implications for individual rights. In that case, recall that the telephone company voluntarily relinquished the information to the government. Had the subscriber contracted with the company specifically to prevent the information from being forwarded to others, the individual would have had at least a contractually-protected right to prevent the information from being made available. The mere evidence rule, until 1967, would have prevented the forced disclosure of similar information by a warrant.

The Court has, at times, been at pains to distinguish the warrant process from the subpoena process. In the 1911 case of Wilson v. United States, the Court distinguished Boyd v. United States, in which the production “of the private books and papers’ of the owner of the goods sought to be forfeited” compelled him to be a witness against himself in violation of the Fifth Amendment and also amounted to an unreasonable search and seizure under the Fourth Amendment. By contrast, the use of a “suitably specific and properly limited” writ, calling “for the production of documents which, as against their lawful owner to whom the writ is directed, the party procuring its issuance is entitled to have produced.”

It is important to recall here that the context for the subpoena power was the actual workings of either the grand jury or the court. The difference between this context, and an investigation conducted by any law enforcement officer who obtains a warrant to obtain private information about individuals, is significant, indeed. By emphasizing the voluntariness of to whom the information is given, instead of the compulsion then exercised by the government on the entity providing the information, the Court misses an important way in which individual rights would otherwise have been guarded.

594. Id. at 376.
595. See, e.g., Hale v. Henkel, 201 U.S. 43, 59–60 (1906) (allowing a grand jury to proceed to issue a subpoena absent a formal charge having been entered and relying on the oath given to the grand jury—that “you shall diligently inquire and true presentments make of all such matters, articles, and things as shall be given to you in charge, as of all other matters, and things as shall come to your own knowledge touching this present service,” etc.—as demonstrating that “the grand jury was competent to act solely on its own volition”).
At the same time, Sotomayor has it right, at least insofar as modern technology impacts the rights of individual actors. Individuals do have a clear privacy interest in a range of data entrusted to corporate entities. But even where information may not appear to entail a privacy interest at the outset, when accumulated, much less when analyzed, possibly even in conjunction with other information, staggering insight into individuals’ private lives may result.

V. CONTENT VERSUS NON-CONTENT

As was discussed in Part II(B), prior to Katz, the Court determined that the contents of a letter deserved higher protection than the address on the outside of the envelope. This general framing (content versus non-content) gained ground after Katz. Technology, however, is now blurring the doctrinal distinction.

On the one hand, new forms of electronic communication (such as email, IMs, and text messages), which for all intents and purposes ought to be considered content, do not fall within the protections of the Fourth Amendment to the same degree that letters traditionally would—despite the fact that much of the same information is at stake.

On the other hand, data traditionally considered to be non-content, such as pen register and trap and trace data, or envelope information, in light of digital dependence and the growth of social network analytics, generates a tremendous amount of information about individuals’ relationships, beliefs, and predilections—precisely the interests that the distinction was meant to protect. The continued reliance on the content/noncontent distinction thus fails to capture the privacy interests at stake.

A. Electronic Communications

In Katz, the Court confronted whether an individual had a privacy interest in the contents of an individual’s communications over

596. An argument could be mounted that “secrecy” is to an organization what “privacy” is to a natural person: namely, the right and the ability to keep individuals not part of the entity or privy to the relationship from knowing things. In some sense, “secrecy” and “privacy” thus represent the same interest expressed by different actors. Justice Sotomayor’s formulation, however, considers third party doctrine to stand for the proposition that “secrecy” serves “as a prerequisite for privacy.” The author understands her point as not being to confuse the two, but rather to suggest that the Constitutional right to individual privacy should not be premised upon the complete bar of anyone having access to the information in question.
a telephone line. In extending protections to the phone booth, the Court acknowledged the central role that telephones had come to play in the modern era.\footnote{597. Katz v. United States, 389 U.S. 347, 352 (1967); see also Smith v. Maryland, 442 U.S. 735, 751 (1973) (Marshall, J., dissenting).} Congress followed \textit{Katz} with introduction of the 1968 Omnibus Crime Control and Safe Streets Act.\footnote{598. See Berger v. New York, 388 U.S. 41, 63–64 (1967) (holding the New York wiretap law to be unconstitutional, precipitating federal legislation on the acceptable limits of wiretap authorities).} Title III laid out the rules that would henceforward govern the electronic intercepts. The law focused on the content of aural or wire communications.

While the Court has taken steps to protect the content of telephone communications, it has been slow to recognize a Fourth Amendment interest in digital communications.\footnote{599. \textit{But see} City of Ontario v. Quon, 560 U.S. 746, 762–63 (2010) (suggesting that “a search of [someone’s] personal email account” would be as intrusive as “a wiretap on his home phone line”).} The Supreme Court has not held, for instance, that individuals have a reasonable expectation of privacy in their e-mail. Instead, this realm is largely governed by statute.\footnote{600. Within the Electronic Communications Privacy Act (ECPA), the Wiretap Act, 18 U.S.C. §§ 2510-22 governs the interception of e-mail communications en route while the Stored Communications Act, 18 U.S.C. §§ 2701–12 (2012) regulates e-mails stored by certain entities.} Where the e-mail is located in the chain of communication alters how much statutory protection it receives. If an e-mail is sitting on a server and has not yet been read, for instance, it is subject to a different set of procedures than one that has been read. Similarly, if the e-mail is actually in transit, as opposed to just waiting to be read (or having been read), then it receives different protections. The complex statutes further take into account considerations such as the type of communications provider in possession of the information, and the length of time the communication has been stored.\footnote{601. For a good discussion of the different aspects of ECPA as applied to electronic communications, see generally \textsc{Clancy, supra} note 79, at § 1.5. These nuances run counter to the Court’s approach in \textit{Ex parte Jackson}, discussed \textit{infra}, in which the mere fact that a letter had left the home did little to alter the privacy interests entailed. An effort to amend the SCA failed in December 2012, when the Senate removed from proposed legislation a measure that would have stopped federal law enforcement from warrantless acquisition of e-mail. Adrian Fontecilla, \textit{The Ascendance of Social Media as Evidence}, 28 CRIM. JUSTICE 1, 2 (2013).}
21st century communications. By 2011, ninety percent of those using the Internet had sent or received e-mail, with half of the U.S. population using it daily.\footnote{602} E-mail has essentially replaced the paper correspondence at issue in \textit{Ex parte Jackson}.

In the meantime, the lower courts remain divided. Some have come out in support of the proposition that e-mail falls within the remit of the Fourth Amendment. In 2008, the Ninth Circuit in \textit{United States v. Forrester} recognized that “[t]he privacy interests in [letters sent through the post and email] are identical.”\footnote{603} Two years later, the Sixth Circuit Court of Appeals catapulted the conversation forward in \textit{United States v. Warshak}, finding that individuals do, indeed, have a reasonable expectation of privacy in their e-mail.\footnote{604}

Steven Warshak owned a company that sold an enormously popular product.\footnote{605} Its auto-ship program, however, failed to warn consumers that by requesting a free sample, they were being enrolled in a delivery schedule from which they would have to opt out to avoid being charged.\footnote{606} As complaints mounted, a grand jury returned a 112-count indictment against Warshak, ranging from mail, wire, and bank fraud, to money laundering.\footnote{607} In the course of its investigation, the government obtained 27,000 e-mails from Warshak’s Internet Service Providers.\footnote{608} On appeal, Warshak argued that the warrantless seizure violated the Fourth Amendment.\footnote{609} The Court ultimately agreed, although it determined that, in this case, the government had relied in good faith on the Stored Communications Act, leaving the judgment undisturbed.\footnote{610}

In finding a Fourth Amendment interest, the Court observed, “[E]-mail was a critical form of communication among Berkeley

\begin{flushright}

603. United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008).


605. \textit{Id.} at 276. The product, Enzyte was “purported to increase the size of a man’s erection.” As the court noted, “[t]he product proved tremendously popular, and business rose sharply.” By 2004, the company was making around $250 million per year.

606. \textit{Id.} at 278.

607. \textit{Id.} at 278, 281.

608. \textit{Id.} at 282.

609. \textit{Id.}

610. Warshak, 631 F.3d 266, at 282.
\end{flushright}
personnel."611 Warshak, in particular, expected “that his emails would be shielded from outside scrutiny.”612 The Court continued, “given the often sensitive and sometimes damning substance of his e-mails, we think it highly unlikely that Warshak expected them to be made public, for people seldom unfurl their dirty laundry in plain view.”613

The court underscored the relationship between written materials, telephone calls, and Internet communications. The growth of society’s dependence on e-mail had shrunk the role of telephone calls and letters:

People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. Commerce has also taken hold in email. Online purchases are often documented in email accounts, and email is frequently used to remind patients and clients of imminent appointments. . . . By obtaining access to someone’s email, government agents gain the ability to peer deeply into his activities.614

The Fourth Amendment had to “keep pace with the inexorable march of technological progress, or its guarantees” would “wither and perish.”615

“Over the last decade,” the Sixth Circuit explained, “email has become so pervasive that some persons may consider [it] to be [an] essential means or necessary instrument[ ] for self-expression, even self-identification.”616 It required strong protections, without which the Fourth Amendment would not prove an effective guardian of private communication. It was not so much that e-mail had become an additional type of communication, as that it appeared to be replacing the traditional modes of communication, which increased the need for it to be protected.

The fact that the e-mail passed through an ISP was irrelevant. “If we accept that an e-mail is analogous to a letter or phone call, it is manifest that agents of the government cannot compel a commercial ISP to turn over the contents of an e-mail without trigger-

611. Id. at 283.
612. Id. at 284.
613. Id.
614. Id.
615. Id. at 285.
616. Warshak, 631 F.3d at 286 (quoting City of Ontario v. Quon, 560 U.S. 746, 760 (2010)).
The ISP was an intermediary—the functional equivalent of a post office or telephone company. Just as law enforcement could not walk into a post office or a telephone company to demand the contents of letters or phone calls, neither could it demand that an ISP turn over e-mails absent a warrant.

Even as Sixth Circuit extended its protections to e-mail, it relied on the traditional content/non-content distinction. The court hastened to distinguish *Miller*, which involved “simple business records” used “in the ordinary course of business.” In contrast, the e-mails sent and received by Warshak were not directed to the ISP as an “intended recipient.”

The U.S. Court of Appeals for the Armed Forces (USCAAF) reached a similar conclusion with regard to the content of e-mails. In *United States v. Long*, it held that Lance Corporal Long had both an objective and a subjective expectation of privacy in e-mails retrieved from a government server. The e-mails indicated that she had been afraid that “her drug use would be detected by urinalysis testing,” and documented the steps she had taken to try to avoid discovery.

USCAAF looked to *O’Connor v. Ortega*, in which the Supreme Court had recognized that government employees may have a reasonable expectation of privacy. In *Long*, USCAAF acknowledged that the military workplace was not exactly the type of environment pictured in *O’Connor* (which had involved a physician at a state hospital). Nevertheless, military personnel could, under some circumstances, have a reasonable expectation of privacy in their e-mail.

Long had used a password (one that the network adminis-

---

617. *Id.*

618. *Id.* at 288 (quoting United States v. Miller, 425 U.S. 435, 442 (1976)).

619. *Id.*


621. *Id.*

622. *Id.* at 61 (citing *O’Connor v. Ortega*, 480 U.S. 709, 716 (1987) (plurality opinion)). In *O’Connor*, the Court acknowledged that the reasonable expectation could be reduced with regard to the employee’s office, desk, or filing cabinet in accordance with the “efficient and proper operation of the agency.” It also recognized a lesser expectation where the search by the employer was related to workplace misconduct. *O’Connor* 480 U.S. at 720–22 (plurality opinion).


624. *Long*, 64 M.J. at 64. See, e.g., United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996) (holding that Maxwell possessed a reasonable expectation of privacy in an America Online e-mail account). But see United States v. Monroe, 52 M.J. 326, 330 (C.A.A.F. 2000) (finding that because the e-mail system in question was owned by the government, Monroe had no contractual agreement guaranteeing privacy from those maintaining the e-mail system).
The fact that the e-mails were originally prepared in an office in Marine Corps’ headquarters (HQMC), on a computer owned by the Marine Corps, and that the e-mails had been transmitted over the HQMC network, stored on the HQMC server, and retrieved by the HQMC network administrator, did not erode Long’s Fourth Amendment rights.\(^6^{26}\)

Although the Ninth and Sixth Circuits, and USCAAF, have extended an expectation of privacy to e-mail, others, looking at the “totality of the circumstances” have come to a different conclusion. In *United States v. Simons*, the Fourth Circuit relied upon the CIA’s Foreign Bureau of Information Services’s Internet policy, which restricted employees’ use of the system to official government business and informed them of ongoing audits, to find that the Fourth Amendment did not apply.\(^6^{27}\) The policy provided fair warning to employees and contractors that their use of the system might be monitored, even as it established the limits of how the system could be used. As a result, a government contractor who used the network to access and download photos from pornographic web sites could not claim the protection of the Fourth Amendment.\(^6^{28}\)

The Fourth Circuit again determined in *United States v. Richardson* that AOL e-mail scans to detect child pornography, and the provision of that information to law enforcement, did not raise the specter of the Fourth Amendment.\(^6^{29}\) AOL initiated its own process, outside of any government direction or control. As federal law enforcement neither required AOL to place e-mails under surveillance, nor directed how such searches should be conducted, no constitutional right came into being. The Fourth Amendment did not restrain private industry.

Similarly, in *United States v. Angervine*, the Tenth Circuit considered Oklahoma State University’s log-on banner, which expressly disclaimed any right of privacy or confidentiality.\(^6^{30}\) Together with "a computer policy that explains the appropriate computer use, warns employees about the consequences of misuse, and describes how officials monitor the University network," the banner provided

---

626. *Id.* at 64.
628. *Id.*
629. U.S. v. Richardson, 607 F.3d 357, 364, 367 (4th Cir. 2010).
630. 281 F.3d at 1130, 1133 (2002).
sufficient notice to users that Fourth Amendment protections did not apply.631

As for text messages, as a doctrinal matter, it is far from clear whether they fall within Fourth Amendment protections. In 2010, the Supreme Court heard *City of Ontario v. Quon*, a case that centered on whether a government employer could read text messages sent and received on a pager owned by the government and issued to an employee.632 In considering the reasonableness of the search Justice Kennedy, writing for the Court, recognized, “[C]ell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification.”633 He acknowledged, “[T]hat might strengthen the case for an expectation of privacy.” But the very fact that the technology was so common and inexpensive meant that “employees who might need cell phones or similar devices for personal matters can purchase and pay for their own.”634 Employer policies, in turn, would shape the reasonableness of any expectations of privacy. The SWAT officer, whose messages had been read, had been told that he did not have any privacy rights in the pager system provided by the City of Ontario, California.635 The Court did not address whether the content of text messages was protected.

At least one state supreme court has come to the conclusion that text messages do not trigger Fourth Amendment protections. In 2012, a lower Rhode Island state court held in *State v. Patino* that the defendant did have a reasonable expectation of privacy in the text messages sent and received.636 In June 2014, the Rhode Island Supreme Court reversed the lower court’s opinion.637

In *Patino*, police responded to a 911 call for a child who had stopped breathing.638 Once the child was in the ambulance on the way to the hospital, the police looked through the mother’s cell phone, which was laying on a kitchen countertop, and found texts

631. *Id.*
633. *Id.* at 760.
634. *Id.*
635. *Id.* at 762 (“Even if he could assume some level of privacy would inhere in his messages, it would not have been reasonable for Quon to conclude that his messages were in all circumstances immune from scrutiny. Quon was told that his messages were subject to auditing.”).
638. *Id.* at 43.
that incriminated the mother’s boyfriend, Michael Patino.\footnote{Id. at 45.} The question before the court was whether individuals have a reasonable expectation of privacy in texts stored on others’ cell phones.\footnote{Id. at 55.}

The court found that the reasonableness prong turned on whose phone was accessed.\footnote{Id.} Control mattered. “[W]hen the recipient receives the message,” the court explained, “the sender relinquishes control over what becomes of that message on the recipient’s phone.”\footnote{Id.} Once the content of the message was revealed to another person, the sender lost any reasonable expectation of privacy. In this case, the police had accessed the owner’s phone without her consent, although she had later signed a form allowing the police to search the device.\footnote{Patino, 93 A.3d at 56.} But for the Court, the sender had already relinquished any privacy interest and thus lacked standing to challenge the search and seizure of his messages.\footnote{Id. at 57.}

The Supreme Court has not affirmatively identified a Fourth Amendment interest in e-mail or text messages—to say nothing of instant messaging, or the myriad other ways that messages may be conveyed through apps, games, and other digital means.

In the 2014 case of Riley v. California, the Supreme Court was willing to acknowledge that a generalized privacy interest attached to a mobile phone in a search incident to arrest.\footnote{Riley v. California, 134 S. Ct. 2473, 2478 (2014).} The case did not distinguish between the text messages on a phone and other functions, such as emails, address books, social media, or gaming applications.\footnote{Id.} Instead, it made a general argument that an immense amount of private information could be carried on a mobile device.\footnote{Id. (“[M]odern cell phones have an immense storage capacity . . . . [T]hey can store millions of pages of text, thousands of pictures, or hundreds of videos.”)}

Several consequences for individual privacy followed:

First, a cell phone collects in one place many distinct types of information that reveal much more in combination than any isolated record. Second, the phone’s capacity allows even just one type of information to convey far more than previously possible. Third, data on the phone can date back for years. In
addition, an element of pervasiveness characterizes cell phones
but not physical records.\textsuperscript{648}

A generalized interest in cell phones, however, does not clearly establish the privacy interests that reside in the communication of
digital content as transferred through e-mail, text messaging, and
other means.

\textbf{B. Pen Register/Trap and Trace Devices}

Even as Supreme Court jurisprudence has, to date, failed to
protect digital communications that look like traditional content,
the growth of new technologies challenges the definition of certain
types of non-content, because of the amount of content that they
now convey. Perhaps the most ready example of this are pen regist-
ner and trap and trace devices which the Court, in the aftermath of
\textit{Katz}, placed on the non-content side of the dichotomy. With the
advance of technology and new algorithmic analyses, this type of
information increasingly reveals intimate details about individuals’
lives.

The first case directly on point arose in 1977, when the Court
looked at whether a district court could direct a telephone com-
pany to assist in placing a pen register on a telephone line.\textsuperscript{649} The
Southern District of New York had issued an order authorizing the
FBI to direct the telephone company to monitor two telephone
lines, compensating the company for any assistance it was thereby
forced to provide.\textsuperscript{650} In \textit{United States v. New York Telephone Co.}, the
Court noted that the language of Title III did not cover the use of
pen registers.\textsuperscript{651} To the contrary, it was concerned only with orders
“authorizing or approving the \textit{interception} of a wire or oral commu-
nication.”\textsuperscript{652} Pen registers, the Court reasoned, “do not ‘intercept,’
because they do not acquire the ‘contents’ of communications.”\textsuperscript{653}
The Court borrowed its understanding of “contents” from the stat-
ute itself, which understood it to include “any information concern-
ing the identity of the parties to [the] communication or the
existence, substance, purport, or meaning of [the] communica-
tion.”\textsuperscript{654} The Court cited the Senate Report, which explicitly dis-

\begin{footnotesize}
\begin{enumerate}
  \item Id. at 2478–79.
  \item Id.
  \item Id. at 166.
  \item Id. (citing 18 U.S.C. § 2518(1)(1998) (emphasis added)).
  \item Id. at 167.
  \item Id. (citing 18 U.S.C. § 2518(1)(1998)).
\end{enumerate}
\end{footnotesize}
cussed that the law was meant to exclude pen registers.\textsuperscript{655} The action in question was consistent with the All Writs Act.\textsuperscript{656} Justice White, writing for the Court, outlined a number of considerations that made the use of the All Writs Act acceptable under the circumstances. First, the telephone company was not “a third party so far removed from the underlying controversy that its assistance could not be permissibly compelled.”\textsuperscript{657} Second, the Court had found probable cause that the facilities were being used to facilitate criminal activity on an ongoing basis.\textsuperscript{658} Third, the assistance requested was “meager.”\textsuperscript{659} Fourth, the company was already “a highly regulated public utility with a duty to serve the public.”\textsuperscript{660} Fifth, “the use of pen registers” was “by no means offensive” to the telephone company.\textsuperscript{661} Sixth, the company itself regularly used pen registers to check its billing operations, detect fraud, and prevent illegal activities.\textsuperscript{662} Seventh, the order was not in any way burdensome, as it “provided that the Company be fully reimbursed at prevailing rates, and compliance with it required minimal effort on the part of the company and no disruption to its operations.”\textsuperscript{663} Eighth, without the company’s assistance, the FBI could not have carried out its wishes.\textsuperscript{664}

Justices Stevens, Brennan, Marshall, and Stewart all dissented in part from the Court’s opinion.\textsuperscript{665} Justice Stevens raised particular concern about jumping from the omission of pen registers and trap and trace devices in Title III to the conclusion that they were consti-

\begin{enumerate}
\item \textsuperscript{655} N.Y. Tel. Co., 434 U.S. at 167–68 (quoting S. Rep. No. 90-1097, 90th Cong., 2d Sess. (1968) (“Paragraph 4 defines ‘intercept’ to include the aural acquisition of the contents of any wire or oral communication by any electronic, mechanical, or other device. Other forms of surveillance are not within the proposed legislation. . . . The proposed legislation is not designed to prevent the tracing of phone calls. The use of a ‘pen register,’ for example, would be permissible. But see United States v. Dote, 371 F.3d 176 (7th 1966). The proposed legislation is intended to protect the privacy of the communication itself, and not the means of communication.”)).
\item \textsuperscript{656} Id. at 172 (“The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.”) (quoting the All Writs Act, 28 U.S.C. § 1651(a) (2012)).
\item \textsuperscript{657} Id. at 174.
\item \textsuperscript{658} Id.
\item \textsuperscript{659} Id.
\item \textsuperscript{660} Id.
\item \textsuperscript{661} N.Y. Tel. Co., 434 U.S. at 174.
\item \textsuperscript{662} Id. at 174–75.
\item \textsuperscript{663} Id. at 175.
\item \textsuperscript{664} Id. at 174–75.
\item \textsuperscript{665} Id. at 178.
titionally authorized. He pointed to dicta in Katz, which underscored that Rule 41 was not tied to tangible property.

The content/non-content distinction highlighted in New York Telephone Co. persisted. The following year, in Smith v. Maryland, the Court returned to the function of pen registers as representing non-content, quoting New York Telephone Co. in support:

[A] law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.

Pen registers, and by inference trap and trace devices, represented non-content.

In an age of metadata and social network analytics, however, it simply is not true that data obtained via pen registers or trap and trace devices do not represent content. A tremendous amount of information can be gleaned just from the numbers dialed and received by one’s telephone. At the most obvious level, the numbers one dials reveal hobbies, interests, relationships, and beliefs. Contacting a drone manufacturer, or a 3D printer sales line shows an interest in drones and 3D printing. Calling a local political representative and members of the planning commission may show concern about development plans in the works. Repeated calls to a priest, rabbi, or imam—or to a church, synagogue, or mosque—may suggest religious conviction.

Communication patterns also reveal degrees of intimacy. Frequent contact with an individual denotes a closer relationship than those with whom one rarely interacts. Mapping the strength of these relationships, in turn, help to elucidate broader social net-

666. Id. at 179.
669. Professor Orin Kerr has argued that while “the contents of online communications . . . should receive Fourth Amendment protection . . . non-content information should not be protected.” Orin S. Kerr, Applying the Fourth Amendment to the Internet: A General Approach, 62 Stan. L. Rev. 1005, 1007–08 (2010). The author disagrees with this argument on the grounds that the line between content and non-content, in a digital age, is often indiscernible. See, e.g., Laura K. Donohue, The Dawn of Social Intelligence (SOCINT), 63 Drake L. Rev.1061, 1065 (2015).
works and an individual’s relationship to others in the network.\footnote{670} From this, leaders can be identified. By mapping social networks, critical connections between different groups also can be identified.\footnote{671}

In June 2013, an associate professor of sociology at Duke University posted a provocative article, Using Metadata to Find Paul Revere, to illustrate the power of social network analytics.\footnote{672} Basing his analysis on the organizations to which the American Revolutionists belonged, Professor Kieran Healy identified shared membership of key organizations, in this manner uncovering the strength of relationships between key revolutionary groups. Breaking down his analysis further into the strength of individuals within and among organizations, Paul Revere emerges as the linchpin.\footnote{673} And Healy went further, calculating the eigenvector centrality number to evaluate the power of the various revolutionists, composing a short list of individuals who would be “persons of interest” to the Crown.\footnote{674} It neatly captured the most important members of the Revolution.

Numerous studies similarly highlight that metadata reveals a tremendous amount of content, making Fourth Amendment doctrine appear almost quaint in a digital age.\footnote{675}

\textit{C. Envelope Information}

Envelope information historically has not been considered within the gamut of the Fourth Amendment. Following Katz, the Court reiterated its protection of letters and packages.\footnote{676} Like communications placed inside envelopes, sealed packages provided to private carriers constitute “effects” within the meaning of the

\begin{thebibliography}{99}


\footnote{672}{Kieran Healy, \textit{Using Metadata to Find Paul Revere}, KIERAN HEALY BLOG (June 9, 2013), \url{https://kieranhealy.org/blog/archives/2013/06/09/using-metadata-to-find-paul-revere/}.

\footnote{673}{Id.

\footnote{674}{Id.


\footnote{676}{Walter v. United States, 447 U.S. 649, 654 (1980).}
Fourth Amendment. What is written on the outside of the envelope or the package, though, does not enjoy a reasonable expectation of privacy. Underlying this approach is the basic concept that what one exposes to others who can simply observe the object, person, or behavior in question, does not fall within the Fourth Amendment. It is bolstered by the assumption that the address merely conveys to/from data—not content itself.

In an age of Internet communications, however, the argument that envelope information does not involve content breaks down. E-mail subject lines may carry significant details about the content of the messages themselves. Uniform Resource Locators (URLs) reveal the content of the pages for which one searches—and, therefore, what one reads. URLs reflect both the specific page being read and the website in general. Website IP addresses similarly reveal content. Yet the courts have yet to recognize the content conveyed through these digital resources, leaving electronic data unprotected from private or government intrusion. In the interim, the government is seeking access to Internet browser history without a warrant.

In United States v. Hambrick, the Fourth Circuit concluded that, under Smith, subscriber information conveyed to an ISP to set up an e-mail account was not protected. The Ninth Circuit similarly held that the “to” or “from” addresses on e-mail, IP addresses of websites, or the total volume of file transfers linked to an Internet account, did not fall within the Fourth Amendment. In United States v. Forrester, the Ninth Circuit focused on the distinction in Smith between content and non-content, concluding that the recording of IP addresses functioned as the constitutional equivalent of the pen registers in Smith. The Court did acknowledge that the collection of not just website IP addresses but also URLs of


681. United States v. Forrester, 495 F.3d 1041, 1048–49 (9th Cir. 2007).

682. Id.
pages visited “might be more constitutionally problematic,” but it did not directly address the question.\footnote{683}{Id. at 1049.}

The Seventh Circuit came to a similar conclusion in United States v. Caira, finding that the government was not required to first get a search warrant before obtaining a suspect’s IP address and login history from a third party provider.\footnote{684}{United States v. Caira, 833 F.3d 803, 809 (7th Cir. 2016).} Caira’s efforts to draw a parallel to the GPS chip in Jones fell short: “The government received no information about how he got from home to work, how long he stayed at either place, or where he was when he was not at home or work. On days when he did not log in, the government had no idea where he was.”\footnote{685}{Id. at 808.} The court acknowledged Justice Sotomayor’s Jones concurrence, and her willingness to dispense with Third Party Doctrine altogether, but it also noted that the Supreme Court had yet to embrace her position.\footnote{686}{Id. at 809} Nevertheless, just as the GPS chip in Jones conveyed a significant amount of private information, so, too, do IP addresses and login histories.

One response to the privacy implications of collecting all of this data may be to simply assume that all digital information is content—driving the discussion to whether the information is public or private. Another response might be to say that no digital information is content. But this, too, ignores the deep privacy interests conveyed through bits and bytes. The current approach seeks to sort out the massive gray area between these two extremes. But simply re-entrenching the content/non-content distinction will not address the longer-term concern: how to protect the privacy interests at stake.

VI.
DOMESTIC VERSUS INTERNATIONAL

A final distinction that is breaking down in light of new and emerging technologies centers on the line between domestic and international. Until the mid-20th century, it was generally assumed that the Bill of Rights did not apply outside the United States, even when law enforcement sought to prosecute citizens for criminal activity overseas.\footnote{687}{See, e.g., In re Ross, 140 U.S. 453, 464 (1891) (holding that the Fourth Amendment was limited to domestic bounds); see also Jennifer Daskal, The Un-Territoriality of Data, 125 YALE L. J. 326, 336 (2015); Caitlin T. Street, Note, Streaming the International Silver Platter Doctrine: Coordinating Transnational Law Enforcement in the}
were destined for statehood enjoyed the full protection of the Bill of Rights. Those that would remain unincorporated territories only enjoyed the protection of fundamental rights—understood in 1901 as including those “inherent, although unexpressed, principles which are the basis of all free government.”\footnote{688} In 1957, the Supreme Court shifted its position, suggesting that the Bill of Rights applied to U.S. citizens abroad.\footnote{689}

In the decades after \textit{Katz}, scholars began debating the universal application of the Bill of Rights.\footnote{690} Some lower courts began moving in this direction as well.\footnote{691} But the optimism proved short-lived. In 1990, the Supreme Court issued an opinion limiting the application of the Fourth Amendment overseas.\footnote{692}

There were good reasons for drawing a line. The uncertainties of investigations overseas, the delicacy involved in diplomatic exchanges, the risk of tipping off criminals with political and other ties to foreign governments, questions of jurisdiction, and other concerns suggested that the same standards that marked the domestic realm should not apply outside U.S. bounds. Resultantly, the Court eschewed a warrant requirement, falling back upon the reasonableness standard for U.S. persons abroad. For non-U.S. persons abroad lacking a significant connection to the United States, the

\begin{flushright}
\textit{Age of Global Terrorism and Technology}, 49 \textit{Colum. J. Transnat'l. L.} 411, 429 (2010–2011). Thus, while the Fourth Amendment applied within the United States—regardless of whether the individual targeted was a U.S. citizen or not—it did not apply outside U.S. borders. \textit{See, e.g.}, Sardino v. Fed. Reserve Bank of N.Y., 361 F.2d 106, 111 (2d Cir. 1966) (“The Government’s [argument] that ‘The Constitution of the United States confers no rights on non-resident aliens’ is so patently erroneous in a case involving property in the United States that we are surprised it was made.”), \textit{cited in} Daskal, \textit{supra} at 336 n.22.
\end{flushright}

\footnote{688.} Downes v. Bidwell, 182 U.S. 244, 291 (1901) (White, J., concurring).

\footnote{689.} Reid v. Covert, 354 U.S. 1, 5–6 (1957) (“The United States is entirely a creature of the Constitution. Its power and authority have no other source. It can only act in accordance with all the limitations imposed by the Constitution. When the Government reaches out to punish a citizen who is abroad, the shield which the Bill of Rights and other parts of the Constitution provided to protect his life and liberty should not be stripped away just because he happens to be in another land.”).


\footnote{691.} \textit{See, e.g.}, United States v. Conroy, 589 F.2d 1258, 1264 (5th Cir. 1979); United States v. Rose, 570 F.2d 1358, 1361–62 (9th Cir. 1978).

Fourth Amendment did not apply at all.\textsuperscript{693} This, too, made sense, not just because of practical considerations, but also because a plausible reading of the Fourth Amendment understands “the people” to refer to citizens of the United States (see discussion, \textit{infra}).

In the realm of national security, looser Fourth Amendment standards framed the collection of foreign intelligence within U.S. bounds.\textsuperscript{694} Nevertheless, as in criminal law, the courts drew a line at the border, with no Fourth Amendment protections extended to U.S. persons located overseas.\textsuperscript{695} In 2008, Congress took the first steps to acknowledge citizens’ privacy interests outside the country. However, weaker standards apply than those that mark domestic collection.\textsuperscript{696}

The problem is that persistent reliance on the borders of the country to protect citizens’ constitutional rights fails to recognize that global communications systems run rampant over the domestic/international distinction. Where, previously, individuals would have to physically travel internationally, or deliberately put in telephone calls to other countries, thus entailing some level of knowledge that what one said or did was leaving the United States, today bits and bytes simply follow the most efficient route—without any deliberate action on the part of the individual generating the information. Much of the information generated internationally, moreover, is ultimately held in the United States or by U.S. entities—rather undermining the arguments that it is unpractical to obtain the same information, or that it would somehow alert foreign governments or criminals, by first requiring a warrant. Similarly, the implications for the jurisdictional argument fall away.

Nevertheless, because of the nature of global communications, and where the information is generated, the same types of communications that previously would have been protected are now more vulnerable to monitoring, interception, and collection by the government—simply because we live in a digital age.

\textsuperscript{693} Id. at 271.  
\textsuperscript{695} The 1978 Foreign Intelligence Surveillance Act purely addressed the collection of information on U.S. soil. Collection overseas fell within the broader framing of Executive Order 12,333.  
A. Law Enforcement

In 1990, the Supreme Court decided in *United States v. Verdugo-Urquidez* that non-U.S. citizens, who lack a substantial connection to the United States, do not enjoy the protections of the Fourth Amendment. The DEA had conducted a warrantless search of Mexicali and San Felipe residences of a Mexican citizen. Chief Justice Rehnquist, writing for the Court, suggested that the right of “the people” meant those who made up the political community of the United States—not non-citizens abroad, lacking a “substantial connection” to the country.

Justice Kennedy, in his concurrence, pointed to the 1901 *Insular Cases*, a series of opinions addressing the status of Puerto Rico, the Philippines, and other overseas possessions, in which the Court had held that the Constitution does not apply in all its force to every territory under U.S. control. While searches within the United States fell subject to the Fourth Amendment, practical barriers could prevent the same overseas. Kennedy pointed to “[t]he absence of local judges or magistrates available to issue warrants, the differing and perhaps unascertainable conceptions of reasonableness and privacy that prevail abroad, and the need to cooperate with foreign officials” as reasons why “the warrant requirement should not apply in Mexico as it does in this country.”

Justice Brennan, joined by Justice Marshall, dissented. How could the United States expand its extraterritorial criminal provisions without correspondingly allowing the Fourth Amendment to travel abroad? The fact that a foreign national was being investigated for a violation of U.S. law, for which he could conceivably “spend the rest of his life in a United States prison,” was sufficient

697. *Verdugo-Urquidez*, 494 U.S. at 271, 274–75. See also Reid v. Covert, 354 U.S. 1, 5–6 (1957) (plurality opinion) (stating that the “shield” that the Bill of Rights provides “should not be stripped away just because [a U.S. citizen] happens to be in another land”).


699. *Id.* at 271, 274–75.

700. *Id.* at 277 (Kennedy, J., concurring) (citing Downes v. Bidwell, 182 U.S. 244 (1901); Hawaii v. Mankichi, 190 U.S. 197 (1903); Dorr v. United States, 195 U.S. 138 (1904); Balzac v. Porto Rico, 258 U.S. 298 (1929)) (stating that the cases “stand for the proposition that we must interpret constitutional protections in light of the undoubted power of the United States to take actions to assert its legitimate power and authority abroad”).


702. *Id.*

703. *Id.* at 279 (Brennan, J., dissenting).
to bring the Fourth Amendment to bear.\textsuperscript{704} As soon as U.S. law applied, the foreign national became, "quite literally, one of the governed."\textsuperscript{705} Fundamental fairness required that if individuals were obliged to comply with U.S. law, then the government, in turn, was "obliged to respect certain correlative rights, among them the Fourth Amendment."\textsuperscript{706}

Under Verdugo-Urquidez, non-U.S. citizens based overseas, who lack a significant connection to the country, do not enjoy the protections of the Fourth Amendment.\textsuperscript{707} Lower court decisions appear to come down on different sides of what, precisely, constitutes a "substantial connection."\textsuperscript{708} For U.S. citizens outside the country, the Fourth Amendment \textit{does} apply—albeit under different standards than those extended within the United States.\textsuperscript{709}

The Supreme Court has not spelled out precisely what is required, although some lower courts have considered this question. In \textit{United States v. Barona}, the Ninth Circuit determined that the Fourth Amendment only applies insofar as the search in question meets the reasonableness standard.\textsuperscript{710} It does not demand that officials first obtain a warrant.\textsuperscript{711} That case dealt with a DEA search conducted at the apex of the so-called "war on drugs," 1985–1987.\textsuperscript{712} As the DEA had used electronic intercepts in accordance with Danish law, the court looked to whether the search was reasonable within the context of Denmark’s legal framework, as

\textsuperscript{704} Id. at 283–84.
\textsuperscript{705} Id. at 284.
\textsuperscript{706} Id.
\textsuperscript{707} For discussion of this point and how the courts have subsequently answered the question of what constitutes a sufficient connection to the United States, see Laura K. Donohue, \textit{Section 702 and the Collection of International Telephone and Internet Content}, 38(1) Harv. J. L. & Pub. Pol’y (2015), http://scholarship.law.georgetown.edu/facpub/1355/ [Hereinafter Donohue, \textit{Section 702}].
\textsuperscript{708} \textit{Compare}, e.g., Martinez-Aguero v. Gonzalez, 459 F.3d 618, 625 (5th Cir. 2006) (finding substantial connections on the grounds that "regular and lawful entry . . . and [ ] acquiescence in the U.S. system of immigration constitute [ ] voluntary acceptance of societal obligations"), \textit{with} United States v. Esparza-Mendoza, 265 F.Supp.2d 1254, 1271 (D. Utah 2003), \textit{aff’d}, 386 F.3d 953 (10th Cir. 2004) (holding that "previously deported alien felons [who illegally re-enter the country] are not covered" under the sufficient connections on the grounds that he is "a trespasser in this country."); see also Donohue, \textit{Section 702}, supra note 708; Orin S. Kerr, \textit{The Fourth Amendment and the Global Internet}, 67 Stan. L. Rev. 285, 291–93 (2015).
\textsuperscript{709} See, e.g., United States v. Peterson, 812 F.2d 486, 490 (9th Cir. 1987).
\textsuperscript{710} 56 F.3d 1087 (9th Cir. 1995).
\textsuperscript{711} Id.
\textsuperscript{712} Id. at 1089–90. See also Donohue, \textit{Section 702}, supra note 707, at 231-232.
well as whether U.S. officials had relied in good faith upon the foreign officials’ representations that the wiretapping complied with Danish law.\textsuperscript{713}

B. Foreign Intelligence Collection

Verdugo-Urquidez and Barona addressed ordinary law enforcement activity. For foreign intelligence collection, different standards apply, but they are still premised on a distinction between domestic and international searches. As with many of the authorities and cases addressed in this Article, the framing developed in a post-\textit{Katz} world that no longer reflects the realities of a digital age.

In footnote 23 of \textit{Katz}, the Court went out of its way to note that the decision did \textit{not} reach national security cases.\textsuperscript{714} Nevertheless, three justices took the opportunity to postulate what might be the appropriate standard for foreign intelligence collection. Justice White came down on the side of giving the Executive Branch more leeway.\textsuperscript{715} Justice Douglas, in contrast, with whom Justice Brennan joined, distanced himself from White’s view, which he considered “a wholly unwarranted green light for the Executive Branch to resort to electronic eavesdropping without a warrant in cases which the Executive Branch itself labels ‘national security’ matters.”\textsuperscript{716} Douglas recognized the potential conflict of interest in having the President or the Attorney General ultimately decide the limits of

\textsuperscript{713} \textit{Id.} at 1094. \textit{See also} Donohue, Section 702, supra note 707, at 232. The Second Circuit also found that the search of U.S. citizens overseas is only subject to the reasonableness requirement, and not the warrant clause. \textit{In re Terrorist Bombings of U.S. Embassies in East Africa}, 552 F.3d 157, 171 (2d Cir. 2008). In \textit{In re Terrorist Bombings}, American intelligence agencies had identified five telephone numbers used by individuals suspected of association with al Qaeda. \textit{Id.} at 159 (citing \textit{United States v. Bin Laden}, 126 F. Supp. 2d 264, 269 (S.D.N.Y. 2000). For a year, they monitored the lines, including ones used by an American citizen, El-Hage. In 1997, the Attorney General authorized intelligence officials to target El-Hage, placing his telephone line in his home in Nairobi, as well as his cell phone, under surveillance. U.S. officials later searched his home without a warrant. \textit{Id.} at 160.

\textsuperscript{714} \textit{Katz} v. United States, 389 U.S. 347, 358 n.23 (1967) (“Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case.”).

\textsuperscript{715} \textit{Id.} at 364 (White, J., concurring) (“We should not require the warrant procedure and the magistrate’s judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable.”); \textit{see also} Donohue, Section 702, supra note 708.

\textsuperscript{716} \textit{Katz}, 389 U.S. at 359 (Douglas, J., concurring); Donohue, Section 702, supra note 708.
their own powers. The fact that the crimes in question were the most serious that could be alleged did little to alter his calculus.

Congress responded to Katz by passing Title III of the Omnibus Crime Control and Safe Streets Act of 1968. The legislation originally covered just wire and oral communications, but in 1986 Congress expanded it to include electronic communications. The Electronic Communications Privacy Act of 1986 included two additional titles focused on stored communications, as well as pen register and trap and trace devices. Title III exempted matters involving national security:

Nothing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities.

Congress was careful to draft the law in a way that left the President’s authority in the realm of foreign affairs intact. Foreign in-

---

717. Katz, 389 U.S. at 359–60 (Douglas, J., concurring) (“Neither the President nor the Attorney General is a magistrate. In matters where they believe national security may be involved, they are not detached, disinterested, and neutral as a court or magistrate must be. Under the separation of powers created by the Constitution, the Executive Branch is not supposed to be neutral and disinterested. Rather it should vigorously investigate and prevent breaches of national security and prosecute those who violate the pertinent federal laws. The President and Attorney General are properly interested parties, cast in the role of adversary, in national security cases. They may even be the intended victims of subversive action.”).

718. Id. at 360 (“Since spies and saboteurs are as entitled to the protection of the Fourth Amendment as suspected gamblers like petitioner, I cannot agree that, where spies and saboteurs are involved adequate protection of Fourth Amendment rights is assured when the President and Attorney General assume both the position of ‘adversary and prosecutor’ and disinterested, neutral magistrate.”).


722. 114 Cong. Rec. 14751 (1968) (Senators Holland, McClellan, and Hart stating that the legislation neither expanded nor contracted the President’s foreign affairs powers); S. Rep. No. 90-1097, at 65 (1968) (stating that the power of the president “is not to be deemed disturbed” by the legislation). See also Donohue, Section 702, supra note 708, at 208.
intelligence collection would be subject to different standards. Precisely what had yet to be decided.

In 1972, the Court weighed in on the question. In *United States v. United States District Court for the Eastern District of Michigan*, the Court suggested that in cases of domestic security, while some sort of judicial process was required for domestic interception, the standard could differ from criminal law. The government had conducted a warrantless wiretap on three people suspected of bombing a Central Intelligence Agency office. The Court agreed 8-0 that under the circumstances, the Government first had to obtain a warrant. The Court cited the “inherent vagueness of the domestic security concept” as well as the risk of government abuse of power as reasons why the Fourth Amendment prevailed. While the Government had to use what technological means it had at its disposal to protect citizens, giving the Executive Branch carte blanche undermined citizens’ rights.

Just as Justice Douglas in *Katz* had argued about the conflict of interest that marked giving the Executive the latitude to set the contours of its own power, Powell argued in *Keith* that, “Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch.” Some sort of judicial process was necessary. The precise contours lay in the domain of the legislature. “Different standards,” Powell wrote, “may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens.” In criminal law, probable cause was the standard against which reasonableness was weighed; for foreign intelligence, the probable cause requirements may reflect “other circumstances more appropriate to domestic security

---

725. Id. at 298, 320.
726. Id. at 320; see also Donohue, *Section 702*, supra note 708.
cases.”

The 1978 Foreign Intelligence Surveillance Act (FISA) served as Congress’s riposte. The legislation was to be the only way the Executive branch could engage in domestic electronic surveillance for foreign intelligence purposes. It later expanded FISA to govern physical searches, pen register and trap and trace devices, and tangible goods.

For each of these areas, FISA incorporated standards more lenient than those that mark criminal law. Instead of requiring probable cause that a crime had been, was being, or was about to be committed, for instance, before electronic surveillance could commence, it required only probable cause that an individual was a foreign power or an agent of a foreign power, and probable cause that they would use the facilities to be placed under surveillance, before a special order from the FISC would issue. The courts repeatedly upheld FISA as compatible with the Fourth Amendment.

731. Keith, 407 U.S. at 323; see also Donohue, Section 702, supra note 708, at 210.


734. See generally Donohue, Bulk Metadata, supra note 6, at 776–93 (discussing the historical background, structure, and purpose of the FISA); Donohue, Future, supra note 6, at 11.


FISA stopped at the border of the United States. All foreign intelligence surveillance involving electronic intercepts (and later, physical searches, pen register and trap and trace, or tangible goods), could only be undertaken on domestic soil consistent with the requirements in the statute. Internationally, intelligence collection fell outside the statutory regime and stemmed from the President’s Article II authorities. From 1981 until 2008, such acquisitions only had to comport with the guidelines laid out in Executive Order 12,333.\(^{738}\) In 2008, Congress passed the Foreign Intelligence Surveillance Amendments Act (FAA), bringing electronic surveillance of U.S. persons overseas within the contours of FISA.\(^{739}\)

Prior to enactment of the FAA, the Southern District of New York (S.D.N.Y.) considered in a counter-terrorism context whether a U.S. citizen placed under surveillance overseas was entitled to the full protections of the Fourth Amendment and determined that he was not.\(^{740}\) In *United States v. Bin Laden*, the Court rejected the necessity of law enforcement first obtaining a warrant before placing either a landline or a mobile telephone under surveillance.\(^{741}\) The Court concluded that because of the undue burden that it would place on the Executive Branch, foreign intelligence collection overseas fell into the “special needs” exception.\(^{742}\) Because of the “intricacies” involved, courts were “ill-suited to the task of overseeing foreign intelligence collection.”\(^{743}\) It was difficult to predict the international consequences of wiretapping on foreign soil; other countries might not want to be seen as complicit with actions taken by the United States, and enemies might be alerted to investigations underway—not least by foreign officials sympathetic to their cause.\(^{744}\) The potential for security breaches to occur was significant.\(^{745}\)

---


\(^{741}\) *Bin Laden*, F. Supp. 2d at 275–76.

\(^{742}\) Id. at 274. See also Donohue, *Section 702*, supra note 707, at 233.

\(^{743}\) *Bin Laden*, F. Supp. 2d at 274.

\(^{744}\) Id. at 275. See also Donohue, *Section 702*, supra note 708.

\(^{745}\) *Bin Laden*, F. Supp. 2d at 275.
The S.D.N.Y. was careful to note the absence of any legislative framing.\textsuperscript{746} The political branches, which were responsible for foreign affairs, had yet to create a warrant requirement for collection of intelligence abroad, making any judicial effort to do so somewhat suspect.\textsuperscript{747} It was therefore up to the other two branches to work out the extent to which a warrant would be required and the specific procedures that would have to be followed for overseas collection. Deference, however, extended only insofar as collection centered on foreign intelligence.\textsuperscript{748} As soon as the primary purpose of the search shifted to criminal law, ordinary Fourth Amendment standards for searches conducted overseas applied.\textsuperscript{749}

In 2008, the Foreign Intelligence Surveillance Court of Review (FISCR) also considered whether a foreign intelligence exception to the warrant requirement existed for intelligence collected abroad.\textsuperscript{750} FISCR pointed to its earlier opinion, which had assumed that regardless of whether a foreign intelligence exception to the warrant requirement existed, FISA met the Fourth Amendment standard of reasonableness.\textsuperscript{751} It then turned to the question of whether, by a special needs analogy, there was a foreign intelligence exception to the warrant requirement.

FISCR emphasized the exceptional nature of national security, stating that the purpose behind foreign intelligence collection "goes well beyond any garden-variety law enforcement objective. It involves the acquisition from overseas foreign agents of foreign intelligence to help protect national security."\textsuperscript{752} The court nevertheless rejected the proposition that the primary purpose of the investigation had to be related to foreign intelligence for the special needs exception to apply:

[I]n our view the more appropriate consideration is the programmatic purpose of the surveillances and whether – as in

\textsuperscript{746} Bin Laden, F. Supp. 2d at 275–77. See also Donohue, Section 702, supra note 708, at 233-234.
\textsuperscript{747} Id.
\textsuperscript{748} Id. at 277.
\textsuperscript{749} Id. See also Donohue, Section 702, supra note 708, at 234.
\textsuperscript{750} In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 , 1012 (FISA Ct. Rev. Aug. 22, 2008); see also Donohue, Section 702, supra note 708, at 234-235.
\textsuperscript{751} In re Directives, 551 F.3d at 1011; In re Sealed Case, 310 F.3d 717, 744 (FISA Ct. Rev. 2002). See also Donohue, Section 702, supra note 708, at 235.
\textsuperscript{752} In re Directives, 551 F.3d at 1011. See also Donohue, Section 702, supra note 708, at 235.
the special needs cases – that programmatic purpose involves some legitimate objective beyond ordinary crime control.\footnote{753. In re Directives, 551 F.3d at 1011. See also Donohue, Section 702, supra note 708, at 236.}

Forcing the government to obtain a warrant would hurt its ability “to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake.”\footnote{754. In re Directives, 551 F.3d at 1011. See also Donohue, Section 702, supra note 708, at 237.} For foreign intelligence collection, then, a different standard marks searches conducted overseas than those within domestic bounds.

The problem, as with criminal law, is that the distinction between domestic and international communications breaks down in light of new technologies.\footnote{755. Although I focus on the physical characteristics (or lack thereof) of digital technologies, commentators also have focused on other ways in which technology has undermined Fourth Amendment doctrine as applied to searches outside the United States. See, e.g., Street, supra note 688, at 429 n.72 (arguing that in the 21st century, “technology and the pervasive transnational terrorist threat have broadened the scope of the international silver platter doctrine, reduced the impact of its joint venture exception, and consequently rendered the Fourth Amendment, in practice, virtually inapplicable to most transnational terrorism investigations.” The result is that more evidence obtained in unreasonable searches can be used in U.S. federal court.).}

C. Technological Challenges to the Domestic/International Distinction

Global communications are, well, just that: global. They do not recognize terrestrial borders. Why conform Fourth Amendment requirements to geographic borders, when packets of information freely flow across them, and, for the most part, outside the control of users? The same information that would be protected under one framing falls subject to lesser protections under the other, despite the fact that the same communications are at stake—making Constitutional rights not so dependent on actual privacy needs, but on an accident of how the Internet works at any given time.

Consider, for instance, electronic mail communications. If I e-mail a colleague in the office next to mine, it may—or may not—be routed to a server in Singapore, where it awaits retrieval. \textit{Pari passu,} foreign to foreign communications may be brought within the United States simply by being sent by the Internet across a U.S. frontier. In days of old, when telephone communications were carried on wires draped across land and water, one could intercept conversations entirely outside U.S. borders. But today, one scholar sitting in Dublin could e-mail a colleague in Bonn. And just as my e-
mail to a domestic colleague could go to Singapore, the e-mail from Dublin may be routed through Palo Alto, California. Does that mean that those communications now fall subject to higher levels of protection—either in the criminal law realm or in the foreign intelligence arena?

In 2008, Congress addressed the second part of the concern by enacting the FAA. The government argued against extending higher Fourth Amendment protections to non-U.S. persons abroad simply because they chose to use a U.S. Internet service provider. It was a sound argument. For one, it made little sense to have constitutional protections rest on the particular ISP involved, and not the status of the individual or the nature of the communication at stake. For another, if by simply using an American ISP, a foreign terrorist could gain greater protections, it would allow individuals to game U.S. law to evade detection.

The problem that global communications present to Fourth Amendment law, however, works both ways. Even as communications overseas might be routed through the U.S., entirely domestic communications might now be routed overseas. If I email or text my colleague at Georgetown, the message may be routed through a server in Singapore before my colleague receives it. Through no action of my own, an entirely domestic message has traveled abroad. Yet it may be precisely the same message that, historically, if sent through regular mail, would have received full Fourth Amendment protections. So drawing a line at the border of the country, and extending fewer protections to the international communications, results in greater surveillance of U.S. citizens than has traditionally occurred.

The intense controversy surrounding Section 702.


758. See also Donohue, Section 702, supra note 708 (arguing that this was the strongest point put forward by the government in support of the FAA).

759. For discussion of this point, see Donohue, Section 702, supra note 708; see also Spencer Ackerman, FBI Quietly Changes its Privacy Rules for Accessing NSA Data on Americans, THE GUARDIAN (Mar. 8, 2016) (reporting PCLOB’s confirmation that
702 of the FISA Amendments Act centered in no small measure on the government’s inability to actually calculate the number of Americans whose privacy interests had been compromised even through upstream collection, directed at non-U.S. citizens abroad, and subsequent query of the database.\footnote{See generally Donohue, Future, supra note 6.}


There are increasingly difficult questions that center on whether and under what conditions the U.S. government can demand access to information held outside the United States. The Second Circuit confronted this question in regard to information linked to a Microsoft user’s web-based e-mail account located in a data center in Dublin, Ireland.\footnote{In re Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014).} A District Court determined that because the information could be obtained from Microsoft employees inside the United States, the warrant was not extraterritorial and thus valid.\footnote{Microsoft, 15 F. Supp. 3d at 476; see also Jennifer Daskal, The Un-Territoriality of Data, 125 Yale L.J. 326 (2016).} The Second Circuit Court of Appeals, however, overruled this decision, stating that “to require a service provider to retrieve material from beyond the borders of the United States—would require us to disregard the presumption against extraterritoriality that the Supreme Court emphasized in “the FBI is allowed direct access to the NSA’s massive collections of international emails, texts and phone calls – which often include Americans on one end of the conversation”;}
As Professor Jennifer Daskal, who has written thoughtfully about digital (un)territoriality, observed, “The dispute lays bare the extent to which modern technology challenges basic assumptions about what is ‘here’ and ‘there.’”

The problem with Fourth Amendment jurisprudence is that it assumes that one can draw a line at the border, and that the drawing of this line can be used in some meaningful way to determine the extent of constitutional protections. But, as Daskal notes, two aspects of the digital world make this impossible: first, data flows across borders at the speed of light and in unpredictable ways. Second, there is no necessary connection between where the data is located and where the individual that either “owns” the data, or to whom the data relates, is located, undermining the significance of where the data is at any moment in time. Whether the individual to whom the data relates is a U.S. person, or a non-U.S. person lacking a significant connection to the United States (as framed in Verdugo-Urquidez), may be impossible to ascertain. No clearer is such a connection between bits and bytes flowing over the Internet and the citizenship or location of the foreign power at issue in FISA—even as amended.

Even if one had the IP address of a particular user, it is not at all clear from that information where a user is located—or even whether it is accurate. IP addresses are numerical sequences that can identify specific computers when they go online. They are used to route information to and from websites. But web anonymizers can hide IP addresses by creating a proxy, contacting the website on your behalf and forwarding the relevant information to you, so that no direct connection between your computer and the website is ever formed.

With global communications, and the lack of digital technologies’ territorial tie in mind, the concern is that the end result will be one in which the weaker standards previously adopted in regard to information obtained outside the United States become applied to an increasing amount of citizens’ private data that happens to either flow across international borders, or to be held in foreign countries. This is the de facto standard already applied to foreign

---

764. Microsoft Corp. v. United States (In re Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp.), 829 F.3d 97, 201 (2d Cir. 2016).
765. The Un-Territoriality of Data, supra note 764.
766. Id.
intelligence collection and raises concerns about how the information is being used in a criminal law context—to say nothing about how the courts should consider criminal investigations when international data is involved.

VII. CONFRONTING THE DIGITAL WORLD

The time is ripe to revisit the post-\textit{Katz} distinctions—private vs. public; personal information vs. third party data; content vs. non-content; and domestic vs. international. They fail to capture the privacy interests affected by the digital sphere.

As this Article has argued, the ubiquitous nature of tracking technologies undermines the claim that what one does in public does not generate insight into private lives. Similarly, the rule that individuals lose their right to protect data when it is entrusted to others ignores the extent to which, as a society, we have become dependent on commercial entities to conduct our daily lives. If all information entrusted to third parties loses its constitutional protections, then the right to privacy itself will gradually cease to exist. Individuals cannot live in the modern world without creating a digital doppelganger that yields insight into our most intimate affairs. Denying the substantive interests involved in e-mail, texting, instant messages, and other forms of communication, moreover, subverts the purpose of distinguishing between content and non-content—even as technology has transmuted traditional areas of non-content to content. Global communications and cloud computing, in turn, collapse the line between what occurs inside the United States and that which transpires abroad.

The Court’s continued reliance on these distinctions is leading to a narrowing of rights, with detrimental consequences for individual liberty.

There are a number of possible responses that the Court could make to the current situation in which we find ourselves. Prior to \textit{Katz}, for instance, judicial doctrine reflected a textual approach, protecting “houses” and “papers” from the intrusive eyes of the government.

Accordingly, some scholars have suggested that digital information similarly should be considered “papers” and within the protection of the home, such that the type of information that would have been located behind closed doors falls within the ambit of the Fourth Amendment. The analogy runs: in a digital world, we no longer keep our papers in the den. Instead, we place them on the
cloud, encrypted. Whether the data is physical or digital should have little bearing on whether or not it is considered private. Either way, it is the same information in question.

A parallel approach centers on whether digital data ought to be considered within the domain of “effects.” As Professor Maureen Brady points out, compared to “houses” and “papers,” “effects” has captured rather less of the Supreme Court’s attention. When it has, property considerations loom large. In crafting a deeper understanding, Brady proposes that the Court look to the context, considering whether the subject of the inquiry is personal property, and whether the individual in question retains possession over it, rendering the property “presumptively entitled to Fourth Amendment protection.” This means looking beyond the actual location of the item—be it in a filing cabinet or on the cloud—and considering, instead, the nature of the item, its relationship to other items, and whether the owner has taken steps to shield the information from public scrutiny.

A similar response centers on the Court’s understanding of “persons.” Much has been written about the “digital self”—doppelgangers that exist as a byproduct of living in the modern world. As an extension of personhood, the digital self provides insight into one’s intimate sphere. Under this approach, the collection of uniquely identifiable information, i.e., data that relates, and could be traced back, to unique individuals, may constitute a search per se, requiring a warrant for collection.

768. See Bagley, supra note 534, at 158 (looking at “the evolution of papers and effects increasingly stored by third party Internet giants”).


770. Id. at 981.

771. Id. at 951.

772. Id. at 952.

The problem with these approaches is twofold: first, they do not directly confront the problems raised by the *Katz* reasonableness standard, discussed, at length, above. Second, more profoundly, they neither confront the theoretical framing of the Fourth Amendment, which presupposes a pre-political self, nor do they question the contemporary assumption that the purpose of the Fourth Amendment is to protect privacy.

In 2013, Professor Julie Cohen attacked the concept of a liberal self.\textsuperscript{774} She argued that the real object of privacy law is a socially-constructed being, "emerging gradually from a preexisting cultural and relational substrate."\textsuperscript{775} For Cohen, liberal political theory’s commitment to definitions of absolute rights and core principles is the problem. It fails to acknowledge the types of privacy expectations that mark the real world.\textsuperscript{776} "The self," Cohen writes, "has no autonomous, precultural core, nor could it, because we are born and remain situated within social and cultural contexts."\textsuperscript{777} *Pari passu,* "privacy is not a fixed condition, nor could it be, because the individual’s relationship to social and cultural contexts is dynamic."\textsuperscript{778}

Cohen’s insight illuminates Professor Anita Allen’s observation that society’s expectation of privacy appears to be changing.\textsuperscript{779} “Neither individuals, institutions, nor government consistently demand or respect physical, informational, and proprietary privacy,” Allen writes.\textsuperscript{780} Thus, while polling data may show high levels of concern about privacy, “Certain legal and policy trends; certain modes of market, consumer, and political behavior; and certain dimensions of popular culture . . . suggest low levels of concern.”\textsuperscript{781} Allen cites to the “avalanche of technologies” that make information available to industry and the government.\textsuperscript{782} She concludes, “Liberals may need to rethink the claims they have always made about the value of privacy.”\textsuperscript{783}

Cohen’s approach offers a way out of Allen’s conundrum. Instead of beginning from the point of political theory or philosophy,

\begin{footnotesize}
\begin{enumerate}
\item *Id.* at 1905.
\item *Id.* at 1907.
\item *Id.* at 1908.
\item *Id.*
\item *Id.* at 728.
\item *Id.* at 729.
\item *Id.* at 730.
\item *Id.* at 728.
\end{enumerate}
\end{footnotesize}
Cohen proposes that one must look to cognitive science, sociology, and social psychology to find the empirical foundations for understanding socially-constructed subjectivity.\footnote{784. Cohen, supra note 774, at 1908.} In this framing, privacy plays a critical role, incubating subjectivity and independence, and wrenching individuals and communities from the clutches of governments and commercial actors that would relegate them to fixed, transparent, and predictable beings.\footnote{785. Id. at 1905.} Perceived in this way, privacy “protects the situated practices of boundary management through which the capacity for self-determination develops.”\footnote{786. Id. at 1916. (“In the contemporary information economy, private-sector firms like Google, Facebook, and data broker Acxiom use flows of information about consumer behavior to target advertisements, search results, and other content. . . . Information from and about consumers feeds into sophisticated systems of predictive analytics so that surveillant attention can be personalized more precisely and seamlessly. Government is an important secondary beneficiary of informational capitalism, routinely accessing and using flows of behavioral and communications data for its own purposes. . . . In the modulated society, surveillance is not heavy-handed; it is ordinary, and its ordinariness lends it extraordinary power.”).} The problem with a digitized, networked world, as it is currently constructed, is that it allows constant access to the boundary and therefore prevents the evolution of the socially-constructed self, outside of external influence.\footnote{787. Id. at 1916.}

Cohen’s conception of social construction as a theory of subjectivity differs in subtle but important way from other scholars who see privacy as socially constructed.\footnote{788. Professor Valerie Steeves highlights privacy as a social value, emphasizing its role in identity, dignity, autonomy, social freedom, and democracy. She considers the relationship between privacy and social equality, with particular emphasis on online social behavior. See, e.g., Ian Kerr & Valerie Steeves, Virtual Playgrounds and Buddybots: A Data-Minefield for Tinsys and Tweeneys, PANOPTICON, COMPUTERS, FREEDOM AND PRIVACY CONFERENCE (Apr. 12, 2005), http://idtrail.org/content/view/128/42/index.html.} Professors Joshua Fairfield and Christoph Engel, for instance, try to turn the lens away from individuals in measuring harm. Instead, they draw attention to the negative externalities on non-consenting outsiders that are caused by the revelation of personal data.\footnote{789. Joshua A.T. Fairfield & Christoph Engel, Privacy as a Public Good, 65 DUKE L.J. 385 (2015).} Eschewing individualism, they argue, “it makes sense to examine privacy as a social construct, subject to the problems of social production.”\footnote{790. Id. at 423.} They continue, “without measured intervention, individuals’ fully informed privacy

\textit{...}
decisions tend to reduce overall privacy, even if everyone cherishes privacy equally and intensely.”791 Applying a law and economics model, the scholars map the social and systemic harms that result from “the collection, aggregation, and exploitation of data.”792 Unlike Courts, which “tend to focus on specific harm to specific complaining individuals, not undivided losses to social welfare,” economists conceive of harm differently.793 A critical question is whether group harms “can be sufficiently theorized to be legally cognizable.”794

If the approach to the liberal self that is built into Fourth Amendment doctrine is at least assailable, the object of the amendment is even more vulnerable to question, with profound implications for evolution of the doctrine.

Specifically, some scholars argue that the underlying value of the Fourth Amendment rests not on the right to privacy (either a liberal incarnation or one premised on social construction), but on liberty from undue government power.795 Looked at in light of the history of the Fourth Amendment at the time of the Founding, this approach is extremely persuasive.796 There is little question that Coke, Hale, and Hawkins, and other prominent English jurists and Parliamentarians, worried about limiting the power of the Crown.797 It was to avoid the assumption and concentration of power that the common law came to restrict powers of search and seizure.798 To place a limit on such powers, outside of hot pursuit of a known felon, the Crown could not enter into any home without a

791. Id.
792. Id.
793. Id. at 425.
794. Id. Other scholars similarly consider group privacy. See, e.g., GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGIES (Luciano Floridi, Linnet Taylor & Blair van der Sloot, eds. 2017). These theories, much like those posited by the Court in Katz, recognize that some aspect of privacy is socially constructed.
796. See Donohue, Original, supra note 14.
797. Id.
798. Id.
warrant.\textsuperscript{799} Neither a general warrant, nor one lacking the requisite particularity, would suffice.\textsuperscript{800} The common law standard, of great importance to the founding generation, became codified in the U.S. Constitution.

In light of this history, it is perhaps unsurprising that in 2008, Professor Jed Rubenfeld observed an “oddity” in the Fourth Amendment: that privacy, “the ‘touchstone’ of modern Fourth Amendment law[,] fails to touch one of the paradigmatic abuses—arrests lacking probable cause made under a general warrant—that the Fourth Amendment was enacted to forbid.”\textsuperscript{801} The doctrine should simply give up “trying to protect privacy.”\textsuperscript{802} Instead, it should turn to what the real purpose was behind the amendment, which is a right of security.\textsuperscript{803}

Rubenfeld’s approach turns a cold shoulder to privacy as the determinant of Fourth Amendment protections. Other scholars take a similar line but are not quite as willing to throw the proverbial baby out with the bath water. Professor Paul Ohm, for instance, has argued that just as privacy replaced property, the Court should now consider power as the “constitutional lodestar” of the Fourth Amendment.\textsuperscript{804} It is not that privacy is irrelevant to the Fourth Amendment enterprise—but rather that power ought to become a new interpretative lens for giving substance to privacy guarantees.\textsuperscript{805}

Ohm is right to the extent that power ought to be considered the constitutional lodestar of the Fourth Amendment. But he is wrong in suggesting that it is a new interpretive lens. It is, instead, a return to the original values of the Fourth Amendment. And it offers a promising way forward for the Court to confront the significant threats posed by digitization, which carries with it the ability to record vast amounts of information, to combine information to

\textsuperscript{799} Id.

\textsuperscript{800} Id.

\textsuperscript{801} Jed Rubenfeld, \textit{The End of Privacy}, 61 STAN. L. REV. 101, 104 (2008); see also Donohue, \textit{Original}, supra note 14, at 1188–93 (discussing the original prohibition on general warrants).

\textsuperscript{802} Rubenfeld, \textit{supra} note 802, at 104.

\textsuperscript{803} Id. at 104–05.

\textsuperscript{804} Ohm, \textit{supra} note 456, at 1338.

\textsuperscript{805} Various efforts have been made to put alternative approaches into practice. See generally, e.g., Kerr, \textit{supra} note 35 (arguing that the rules ought to create a level playing field between criminals and law enforcement in light of technological advancement); Ohm, \textit{supra} note 796 (building on Kerr by considering dual-assistance technologies that help both law breakers and law enforcement).
generate new knowledge, and to do so for many people over extensive periods of time, with minimal resource constraints.

In Riley, the Court alluded to these concerns.\textsuperscript{806} It acknowledged four consequences that flowed from the government’s collection of data, which helped to clarify why the search of a mobile phone was more invasive than finding a packet of cigarettes in someone’s pocket. The former had “several interrelated privacy consequences.”\textsuperscript{807}

First, a cell phone collects in one place many distinct types of information that reveal much more in combination than any isolated record. Second, the phone’s capacity allows even just one type of information to convey far more than previously possible. Third, data on the phone can date back for years. In addition, an element of pervasiveness characterizes cell phones but not physical records. A decade ago officers might have occasionally stumbled across a highly personal item such as a diary, but today many in the more than 90% of American adults who own cell phones keep on their person a digital record of nearly every aspect of their lives.\textsuperscript{808}

Similar issues haunted the shadow majority in Jones. Justice Alito recognized, “longer term GPS monitoring in investigation of most offenses impinges on expectation of privacy.”\textsuperscript{809}

Justice Sotomayor explained, “In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the Katz analysis will require particular attention.”\textsuperscript{810} That it was precise and reflected a “wealth of detail about” one’s “familial, political, professional, religious, and sexual associations,” was relevant.\textsuperscript{811}

Sotomayor went on to note that the length of time the records could be kept, and mined, for more information, raised further concerns: “And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds sur-

\textsuperscript{806} See also Susan Friewald, \textit{A First Principles Approach to Communications’ Privacy}, \textit{Stan. Tech. L. Rev.} (2007) (arguing electronic surveillance that is intrusive continuous, indiscriminate, and hidden should be subject to Fourth Amendment restrictions). Friewald’s principles align with the direction the Court took in Riley and Jones.

\textsuperscript{807} \textit{Riley}, 134 S. Ct. at 2478.

\textsuperscript{808} \textit{Id}.


\textsuperscript{810} \textit{Id}. at 955 (Sotomayor, J., concurring).

\textsuperscript{811} \textit{Id}. 
reptitiously, it evades the ordinary checks that constrain abusive law enforcement practices.”

Justice Sotomayor tried to fold her broader concerns into the *Katz* framework: “I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.” But in relying on *Katz*, Sotomayor’s approach fell short of challenging the dichotomies and bringing attention to the underlying issue, which is the steady expansion of government power over the people. By acknowledging that the purpose of the Fourth Amendment was to protect against the accumulation of power, the Court will be better equipped to confront the dangers of the digital age.

812. *Id.* at 956.
813. *Id.*
Panel VII:

The Arctic: National Security and Oceans Law for the New Maritime Frontier

Moderator:
RADM Kevin E. Lunday

Discussants:
Julie Gascon
Bronwyn Douglass
John Norton Moore

INTRODUCTION 380
I. BREAKING THE ICE: GETTING TO KNOW THE CURRENT INTERNATIONAL LEGAL FRAMEWORK FOR ARCTIC NAVIGATION 383
   A. Relevant Nations: The Arctic States 383
   B. The International Legal Framework: UNCLOS and the Polar Code 387
II. INCONSISTENT NATIONAL APPLICATION OF THE INTERNATIONAL FRAMEWORK: ANALYSIS OF THREE CASE STUDIES 396
   A. Russia and Arctic Navigation 397
   B. Canada and Arctic Navigation 400
   C. The United States and Arctic Navigation 402
   D. But Why Do These Inconsistencies Matter? 403
III. TOWARD A UNIFORM FRAMEWORK: ENABLING INNOCENT PASSAGE AND THE POLAR CODE AS DELINEATION OF “DUE REGARD” FOR NAVIGATION 405
CONCLUSION 410

*380 INTRODUCTION

With the continued melting of sea ice in the Arctic, previously inaccessible stretches of Arctic waters have become navigable. 1 With that increased navigability comes the possible opening of more efficient shipping routes through the Arctic Circle. 2 While the question of who gets to determine navigational laws in the Arctic Ocean has long been an intellectual exercise, the persistence of thick sea ice throughout much of the year kept that question strictly in the realm of the hypothetical. 3 Now, however, that thick sea ice is melting and potentially creating a shortcut across the Arctic Ocean that would shave thousands of miles off of currently frequented shipping routes. 4 The potential for increased ship traffic through the Arctic via those once inaccessible routes has given the question of who determines the “rules of the road” for the Arctic Ocean--and what those rules should look like--new urgency. Arctic environmental and navigational schemes are crucial to answering these questions because the discussions surrounding the two concepts are frequently intertwined. 5 A primary reason for this is that the amount of ice in Arctic waters, which is necessarily dependent on temperature and climate, dictates the extent of navigation that can occur. 6 Additionally, the introduction of hitherto unknown volumes of traffic brings the possibility for hitherto unknown volumes of pollution to one of the most unusual,
pristine environments remaining on Earth. Indeed, due to the isolation and extreme nature of the Arctic Circle's environment, accidental spills of oil or other pollutants would be extremely difficult to mitigate and remediate.

*381 Given these concerns, ensuring safety of navigation and protection of the environment are closely linked, and the conversation surrounding Arctic navigation and shipping routes necessarily requires some discussion of environmental impact. Unsurprisingly, the existing international legal framework regarding protection of the maritime environment, which includes the United Nations Convention on the Law of the Sea and the Polar Code, is frequently cited in discussions regarding Arctic navigational laws. The United Nations Convention on the Law of the Sea ("UNCLOS") is an international agreement that created a vague “due regard” standard for Arctic environmental and navigational laws, and the Polar Code is a very recently promulgated instrument that aims to provide a comprehensive set of Arctic shipping and environmental protection guidelines. However, due to UNCLOS's use of poorly defined phrases such as “due regard,” Arctic navigation laws passed by the Arctic Coastal States (Canada, Denmark, Norway, Russia, and the United States) are arguably inconsistent with the framework's intent, not to mention inconsistent with other nations' laws passed in response to the same framework.

This Note argues that to remedy those inconsistencies, the UNCLOS standard requiring that Arctic environmental laws have “due regard” for navigation should be interpreted in light of the Voyage Planning Requirements found in the Polar Code. Specifically, this Note examines the Arctic navigation policies of three Arctic Coastal States (Russia, Canada, and the United States), the inconsistencies between those policies and the international legal framework, and how those inconsistencies can be easily resolved by understanding “due regard” in Article 234 of UNCLOS to incorporate the Arctic navigational requirements found in the Polar Code. Part I provides an overview of the existing international framework for Arctic navigation. Part II analyzes how well (or poorly) the Russian, Canadian, and American Arctic navigational policies fit into the current international scheme created by UNCLOS and the Polar Code, and examines how inconsistent approaches to Arctic navigation could have far-reaching negative impacts. Part III posits that to avoid those dangers and tensions, “due regard” in UNCLOS Article 234 should be interpreted using the Voyage Planning requirements listed in the Polar Code's Voyage Planning chapter. Additionally, Part III proposes that reshaping Arctic navigational laws according to this interpretation of “due regard” would increase clarity among countries and increase efficiency in protecting the safety of the ships and crews navigating through the region. Lastly, this Note concludes that such an interpretation would help Arctic Coastal States protect the environment and the safety of individuals navigating the Arctic, as well as allow those States to maintain some level of autonomy and sovereignty.

I. BREAKING THE ICE: GETTING TO KNOW THE CURRENT INTERNATIONAL LEGAL FRAMEWORK FOR ARCTIC NAVIGATION

A. Relevant Nations: The Arctic States

The primary nations in the discussion surrounding Arctic navigation laws are those geographically closest to the Arctic Ocean. While the Arctic Ocean is capped with a thick layer of sea ice that has historically limited navigation, the extent of that sea ice has been steadily declining since 1979. In 1996, representatives from Canada, Denmark, Finland, Iceland, Norway, Russia, Sweden, and the United States—the eight nations with the nearest geographic proximity to the Arctic Circle—met in Ottawa, Canada, to draw up the Declaration on the Establishment of the Arctic Council, also known as the “Ottawa Declaration.”
The Ottawa Declaration established the Arctic Council as an intergovernmental forum to promote discussion of and cooperation on Arctic issues and named the eight nations participating in the Arctic Council the “Arctic States.” The Ottawa Declaration does not specifically mention adhering to UNCLOS. However, all of the Arctic Council nations have ratified UNCLOS except for the United States. Additionally, all eight nations were previously part of a 1991 nonbinding environmental protection agreement called the Arctic Environmental Protection Strategy (“AEPS”) that specifically emphasized the need for environmental protection measures consistent with UNCLOS. Given that background, the principles of UNCLOS were very likely a foundational principle in the coming together of these eight Arctic States.

Of the eight Arctic States, five physically border the Arctic Ocean. Those five states are Canada, Denmark, Norway, Russia, and the United States. Although all five are part of the greater Arctic Council, they regard themselves as a separate subset within the Arctic Council due to the “unique position” to handle Arctic issues their proximity to the Arctic Ocean provides. This sentiment is most clearly demonstrated by the 2008 issuance of the Ilulissat Declaration, which came about in response to Russia’s planting of a Russian flag on the ocean floor at the North Pole. Many news sources, countries, and politicians interpreted Russia's gesture as a power grab. In response, Canada, Denmark, Norway, Russia, and the United States came together in May 2008 at the Arctic Ocean Conference in Ilulissat, Greenland, to negotiate what became the Ilulissat Declaration. Finland, Iceland, and Sweden, the three Arctic States that do not physically border the Arctic Ocean, were not included in the Ilulissat conference, and the Ilulissat Declaration explicitly states that the “five Coastal States” are “in a unique position to address [Arctic] possibilities and challenges.” In addition to distinguishing the five Coastal Arctic States, the Ilulissat Declaration stated that the Coastal States have a continued commitment to UNCLOS, will work together within the bounds of current laws to protect and preserve the marine environment, and “see no need to develop a new comprehensive international legal regime to govern the Arctic Ocean.”

This public declaration that the five Arctic Coastal States see themselves as a separate entity within the Arctic Council drew criticism from Iceland, Finland, and Sweden--the three members of the Arctic Council excluded from the Arctic Ocean Conference and Ilulissat Declaration. The excluded non-Coastal States have criticized the Ilulissat Declaration's implied distinction between the “unique[ly] position[ed]” Coastal States and the non-Coastal States. The Swedish government, for example, has stated that the Arctic Council as a whole should discuss Arctic issues to ensure that the concerns of the non-Coastal States and indigenous peoples are not overlooked. Nevertheless, the overall goals, viewpoint, and emphasis on compliance with UNCLOS articulated in the Ilulissat Declaration by the five Arctic Coastal States do not appear to have any drastic differences from the stances articulated by the three non-Coastal Arctic States. This implies that despite the apparent fractioning of the Arctic States into Coastal and non-Coastal States, the Arctic States as a group have similar priorities and goals for the Arctic region and a willingness--at least on paper--to work within the existing international legal framework.

B. The International Legal Framework: UNCLOS and the Polar Code

The international legal framework governing international maritime law, safety, and environmental protection consists of UNCLOS and the Polar Code, the two main international agreements that touch on international Arctic navigational laws. UNCLOS, adopted in 1982, represents an evolution of the historical understanding of maritime jurisdiction and navigational rights. Historically, jurisdiction over the ocean was defined by the freedom-of-the-seas doctrine, a
principle that limited each nation's territorial ocean rights to a swath of sea extending a few miles past its shore. As time passed, however, nations became more interested in expanding their territory and exploiting the seas: coastal states wanted access to the ocean's natural resources, and naval states wanted freedom of the seas and the ability to navigate as they pleased. By the mid-twentieth century, many nations had greatly expanded their territorial claims. That expansion created tension and exacerbated rivalries as nations strove to capture as much territory and as many resources as possible, resulting in inconsistent national laws regarding navigation and disposition of resources. In an attempt to create a standardized law to replace the patchwork of national offshore territorial claims, the United Nations held its first United Nations Conference on the Law of the Sea in 1956.  

That first conference of United Nations members resulted in four separate conventions, or “formal multilateral treaties with a broad number of parties.” Those four conventions were finalized in 1958 but did not mark the end of international maritime law's evolution. A second United Nations Conference on the Law of the Sea in 1960 failed to result in any new conventions or a compilation of the conventions from the first conference. The third and final United Nations Conference on the Law of the Sea, convened in 1973, was more successful and ended in 1982 with the adoption of the United Nations Convention on the Law of the Sea (“UNCLOS”). UNCLOS entered into effect in 1994 and contained provisions regarding navigational rights, territorial sea limits, economic jurisdiction, conservation of marine resources, protection of the marine environment, and a binding dispute settlement procedure, among others. UNCLOS has been signed by each of the Arctic Council nations and ratified by all the Arctic Council nations except for the United States. 

UNCLOS was intended to create a standard framework for international maritime law that would result in a consistent global law of the sea and relatively uniform national maritime laws. In addition to prescribing universal international laws for such diverse bodies of water as the high seas, straits, and enclosed or semi-enclosed seas, UNCLOS gives the Arctic Coastal States sovereignty in their “territorial seas,” the band of ocean extending up to twelve nautical miles from the country's shore. UNCLOS also gives the Arctic Coastal States jurisdiction to prescribe and enforce environmental laws in their exclusive economic zone (“EEZ”), the stretch of ocean extending up to 200 nautical miles beyond the end of the territorial sea. Specifically, UNCLOS Article 234 provides Arctic Coastal States with the sovereignty to craft laws regarding the “prevention, reduction and control of marine pollution from vessels in ice-covered areas within the limits of the exclusive economic zone” provided that the laws crafted by Coastal States give “due regard” to navigation. “Due regard” is not clearly defined anywhere in UNCLOS, and that ambiguity makes Article 234 open to interpretation. This lack of clarity has resulted in a patchwork of conflicting Arctic navigational and environmental laws, and there is no clear way to determine whether a national law is consistent with the international legal framework. Although Article 234 of UNCLOS relates to the adoption and enforcement of marine environment protection laws for ice-covered areas, it is frequently mentioned in discussions of Arctic navigation as a result of the connection between increased navigation and increased potential for pollution and accidental spills. Specifically, UNCLOS Article 234 gives Coastal States the right to adopt and enforce non-discriminatory laws and regulations for the prevention, reduction and control of marine pollution from vessels in ice-covered areas within the limits of the exclusive economic
Such laws and regulations shall have due regard to navigation and the protection and preservation of the marine environment based on the best available scientific evidence.\footnote{57}

\footnote{390} Focusing on that “due regard” requirement, “due regard” is not specifically defined elsewhere in UNCLOS but can be interpreted as a requirement that Coastal States avoid limiting or curtailing navigation that occurs within the boundaries of their EEZs barring an overriding environmental concern.\footnote{58} This makes sense given the unique nature of the Arctic environment (e.g., extreme cold temperatures, animal life found nowhere else on earth) and the unique concerns affecting the Arctic environment (e.g., climate change leading to melting sea ice, level of difficulty involved in remediating environmental contamination in extreme temperatures).\footnote{59} For example, “due regard” acting as an instruction for nations to respect the navigational needs of ships proceeding through their EEZs is compatible with the sections in UNCLOS regarding innocent passage, which give foreign ships the right to proceed through the waters of other states so long as their passage is expeditious and does not threaten the Coastal State's national security.\footnote{60} The consistency that such an interpretation of “due regard” lends to UNCLOS is also desirable, especially when the goal is a legal framework to guide national Arctic navigation laws.

Additionally, UNCLOS gives all nations the right of innocent passage through territorial seas,\footnote{61} which means that ships may cross a territorial sea so long as their passage is “continuous and expeditious,” they do not enter internal waters or call at a port outside internal waters, and they do not threaten the security of the nation through whose territorial sea they are passing.\footnote{62} Coastal States have the freedom to adopt several different types of laws in their territorial seas.\footnote{63} Such laws include safety and maritime traffic laws; laws protecting any facilities, installations, pipelines, or cables in their territorial sea; environmental protection and conservation laws; and marine scientific laws, among others.\footnote{64} However, Coastal States cannot \footnote{391} hamper the innocent passage of foreign ships through their territorial sea; impose requirements that essentially deny or impair innocent passage; or discriminate against ships based on whose ships they are, whose cargo they are carrying, and where they are going.\footnote{65} Once a ship is in a nation's EEZ, as opposed to its territorial sea, the ship enjoys even more freedom: UNCLOS Articles 58 and 87 grant ships freedom of navigation through both the EEZ and the high sea, which is the zone beyond the EEZ.\footnote{66}

Beyond establishing innocent passage and other navigational rights, UNCLOS also provided for resolution of disputes between member states by establishing the International Tribunal for the Law of the Sea (“ITLOS”),\footnote{67} which is an independent judicial body that arbitrates disputes springing from the interpretation and application of UNCLOS.\footnote{68} Suits regarding the consistency of national maritime laws stemming from UNCLOS are properly heard and arbitrated by ITLOS.\footnote{69}

Another important component of the international Arctic navigation law framework is the Polar Code, which is a more recent addition to the international legal framework. The Polar Code grew out of the International Maritime Organization's ["IMO’s"] 2009 safety guidelines for polar waters, and came into force on January 1, 2017.\footnote{70} The IMO is a specialized agency of the United Nations that sets global standards for safety and security of shipping as well as environmental protection.\footnote{71} There are 171 member states in the IMO, and all eight of the Arctic States are members.\footnote{72} The IMO intended the Polar Code to provide a comprehensive set of mandatory guidelines for all shipping \footnote{392} and environmental matters in the Arctic and included guidelines in the Polar Code to ensure the protection of ships, sailors, and the environment in the Arctic.\footnote{73}
Navigating in Arctic waters is exceptionally dangerous, and hazards include collisions with ice, adverse environmental conditions such as low temperature, snow, and high winds, and accumulation of ice on vessels. Because of the extreme nature of the Arctic environment and the hazards associated with Arctic navigation, the IMO followed their 2009 safety guidelines with a push to create a code containing a set of mandatory guidelines. The resulting Polar Code consists of safety and environmental provisions. These provisions were incorporated by amendment into two preexisting conventions that were already legally binding on their parties, namely the International Convention for the Safety of Life at Sea (“SOLAS”) and the International Convention for the Prevention of Pollution from Ships (“MARPOL”). Despite a drawn-out development process and delayed adoption, the safety provisions of the Polar Code and the amendments to SOLAS required to make them legally binding were passed on November 21, 2014. The environmental provisions of the Polar Code and the amendments to MARPOL required to make them legally binding were passed on May 15, 2015. The Polar Code went into effect on January 1, 2017, and is legally binding on all nations that are bound by MARPOL and SOLAS, including all of the Arctic States.

Included in the safety provisions section of the Polar Code is a section regarding voyage planning (i.e., considerations that the shipmaster should have in mind when planning a polar voyage). The list of voyage planning requirements contained in Chapter 11 of the Polar Code was intended to “ensure that the Company, master and crew are provided with sufficient information to enable operations to be conducted with due consideration to safety of ship and persons on board and, as appropriate, environmental protection.” The “due consideration” language, which echoes UNCLOS Article 234’s “due regard” language, indicates that the Polar Code’s voyage planning requirements are a list of the considerations that the IMO believes must be taken into account in order to adequately protect the safety of the ship, the sailors, and the environment when navigating through Arctic waters. The list itself consists of nine considerations the shipmaster must take into account when planning a voyage through polar waters:

1. the procedures required by the [Polar Water Operational Manual];

2. any limitations of the hydrographic information and aids to navigation available;

3. current information on the extent and type of ice and icebergs in the vicinity of the intended route;

4. statistical information in ice and temperatures from former years;

5. places of refuge;

6. current information and measures to be taken when marine mammals are encountered relating to known areas with densities of marine mammals, including seasonal migration areas;
7. current information on relevant ships' routing systems, speed recommendations and vessel traffic services relating to known areas with densities of marine mammals, including seasonal migration areas;

8. national and international designated protected areas along the route; and

9. operation in areas remote from search and rescue (SAR) capabilities. 85

Further guidance on the voyage planning requirements provided in Part I-B of the Polar Code notes that in the development and execution of a ship's voyage plan, “any existing best practices” to minimize disturbance of marine mammals should be considered, and if the ship's route will be near an area of “cultural heritage or cultural significance,” the voyage plan should be constructed to minimize the ship's impact on those areas. 86 Together, the list of voyage planning requirements and additional guidance provided in Part I-B contemplate safety protocols, 87 presence of ice and icebergs, statistical information regarding temperature and presence or absence of ice, and places of refuge on the journey. The voyage planning requirements include all of the factors a shipmaster needs to weigh in order to pick a safe navigational route for an Arctic expedition and arguably encompass *395 environmental concerns as well. 88 Critically, the Polar Code includes environmental considerations on the list of voyage planning requirements and in the accompanying guidance. Rather than using vague terms to describe the outlines of what national Arctic environmental laws should look like, the Polar Code sets out an Arctic navigation planning process that actually contemplates environmental concerns.

The Polar Code is a legally binding piece of international law that represents a step toward a uniform approach to international shipping laws. 89 However, the Polar Code is not without issues: it has been critiqued by scholars, activist groups, the media, and even the Secretary-General of the IMO for being “weak” and relying on flag states to monitor their own compliance rather than providing active enforcement mechanisms. 90 Given its recent adoption and entry into force, it remains to be seen whether the Polar Code will be adequately enforced. 91 Between UNCLOS’s lack of definitions for critical phrases like “due regard” and the Polar Code’s reliance on flag states to enforce *396 its provisions, the current international scheme for Arctic navigation is at best poorly defined and at worst ineffective at creating a uniform navigational scheme in the region.

II. INCONSISTENT NATIONAL APPLICATION OF THE INTERNATIONAL FRAMEWORK: ANALYSIS OF THREE CASE STUDIES

As it stands, the framework of international Arctic navigation is hampered by vague language and reliance on member nations to enforce its laws. To deal with the day-to-day business of handling Arctic navigation, the Arctic Coastal States have promulgated their own individual Arctic navigational laws. 92 This Note focuses specifically on the laws of Russia, Canada, and the United States not only because of their roles as Arctic Coastal States, but also because they are the three countries primarily responsible for negotiating Article 234 of UNCLOS. 93 However, although Russia, Canada, and the United States have all ratified (or at least recognized) UNCLOS, 94 and are the nations responsible for the final
form of UNCLOS Article 234, their Arctic navigational laws and policies do not necessarily provide “due regard to navigation” in “ice-covered areas” as required by UNCLOS Article 234.

*397 The main difficulty with defining “due regard” is delineating what acceptable and unacceptable limits on navigation look like. Requiring environmental regulations to have “due regard to navigation” seems to indicate that Coastal States must consider navigational rights when crafting environmental protection laws, but stops short of using language requiring environmental laws to comply strictly with all navigational laws. If Russia, Canada, and the United States had intended to draft UNCLOS Article 234 to bar environmental regulations from limiting the freedom of navigation, they could have simply done so by inserting language to that effect—for example, a phrase like “environmental protection laws may not impair navigation.” However, they chose to use the phrase “due regard,” which implies that those three nations contemplated situations where environmental regulations could at least partially limit navigational rights. For example, such regulations could potentially include a measure requiring ships to give icebergs or animal breeding grounds a wider berth than usual, while still allowing them innocent passage elsewhere without requiring permission.

On the other hand, though the “due regard” language suggests that environmental regulations may be able to limit navigation in certain circumstances, it also indicates that environmental regulations cannot create a situation in which a nation effectively bans innocent passage through its waters under the guise of protecting the Arctic environment. That “due regard” requirement implies that navigational rights cannot be completely curtailed in favor of environmental protection laws and regulations. Using this understanding of “due regard” and the limitations that phrase places on environmental and navigational laws, the current Arctic navigational laws and policies of Russia and Canada arguably go too far in limiting innocent passage through their respective waters.

A. Russia and Arctic Navigation

Russia has been an aggressive participant in what the media has portrayed as a “race to control the Arctic Circle.” One motivation for Russia's proactive stance regarding the Arctic is the fact that two of the shipping shortcuts that could open up if Arctic sea ice continues to melt run along its coastline. The first route is the Bering Strait, a portion of the Northwest Passage that cuts between Russia and Alaska. The second is the Northern Sea Route, which runs along the northern coast of Russia and which Russia considers to be at least partly made up of internal waters. Both routes are currently too icy to be of much practical use, but should those routes become ice-free enough to be safely navigable, they could provide a shortcut across the Arctic Ocean that would shave thousands of miles off of shipping routes frequented by many nations today.

The current Russian scheme for navigation through the Northern Sea Route was approved by Russia's Ministry of Transport and came into force on January 17, 2013. The official protocol requires all ships passing through Russian waters to submit an application to the Ministry of Transport at least 120 days in advance of the planned voyage. The Ministry of Transport may refuse permission, but should it grant permission for passage through the Northern Sea Route, the applicant will then be informed of both the period of time during which they may traverse the route and the type of icebreaker escort they must have. Furthermore, ships passing through the Northern Sea Route are charged a fee for the mandatory icebreaker escort, and they must periodically report their location to the Ministry of
Transport. The government of Russia reserves the right to turn away ships it thinks are not appropriately equipped for the sea voyage.

Arguably, Russia's government has been exercising that right inappropriately, giving rise to concerns about Russia's adherence to the guiding principles of international navigation law as laid out by UNCLOS. One relatively recent incident that has led to the accusation of inconsistent, discriminatory application of Russian Arctic navigation laws was the arrest of thirty Greenpeace activists. After a peaceful September 2013 demonstration at a Gazprom oil rig to protest against Russia's oil drilling policy, the thirty activists were arrested, detained, and charged with piracy, while their Netherlands-flagged ship was towed to a port 500 miles away. The ship was not released until June 2014, and in August 2015, the Permanent Court of Arbitration, an intergovernmental body dedicated to facilitating international alternative dispute resolution, ordered Russia to pay damages for having seized the ship outside its territorial sea. Arousing further skepticism regarding Russia's willingness to adhere to the principles of UNCLOS was Russia's reaction to the subsequent suit the Netherlands brought in ITLOS alleging conduct in violation of UNCLOS. When ITLOS found that Russia violated UNCLOS by seizing the Greenpeace ship in international waters, and assessed a financial penalty in addition to the penalty imposed by the PCA, Russia responded by issuing a statement that they would not abide by the ruling. This incident gives rise to grave concerns regarding the compatibility of current Russian Arctic navigation laws with UNCLOS and the right to innocent passage, as well as Russia's willingness to work with other nations in the absence of clear definitions of what “due regard” means.

B. Canada and Arctic Navigation

Canada's framework governing navigation through Canadian Arctic waters consists of the Northern Canada Vessel Traffic Services Zone Regulations (“NORDREG”), and the Arctic Waters Pollution Prevention Act (“AWPPA”). Initially implemented in 1977 as a voluntary set of shipping guidelines, NORDREG became mandatory on July 1, 2010. Like Russia's Arctic navigation scheme, NORDREG requires ships to submit requests for clearance and allows the Canadian government to refuse ships the right of passage through either the territorial sea or the EEZ. While passing through Canadian waters, NORDREG requires ships to submit four different types of reports. Failure to comply with NORDREG reporting requirements triggers AWPPA, which provides that ships may be prevented from entering Canadian waters if they do not comply with all Canadian regulations. Furthermore, the penalties under AWPPA are severe in the event a ship enters Canadian waters after being denied or failing to request permission: the ship could be escorted out of Canadian waters and be subject to both civil and criminal liability, as well as be “liable on summary conviction” to fines.

The main objections lodged against the Canadian regulatory scheme come from the United States Secretary of State, which complains that the Canadian government is able to refuse permission to enter the Canadian EEZ or territorial seas and that NORDREG contains no exceptions for sovereign immune vessels. Sovereign immune vessels are defined by UNCLOS Article 236 as “any warship, naval auxiliary, other vessels or aircraft owned or operated by a State and used, for the time being, only on government non-commercial service,” and they are exempted from the UNCLOS Articles relating to the protection and preservation of the marine environment. Those objections have led to concerns that Canadian laws regarding Arctic navigation, while ostensibly promulgated in accordance with UNCLOS, in fact violate the right of innocent passage and the “due regard” requirements of UNCLOS by allowing Canada to
cite environmental concerns and refuse ships passage through Canadian waters. Additionally, the United States disagrees with Canada on how to classify the portion of the Northwest Passage that runs along the top of the North American continent. Canada maintains that the Northwest Passage is a part of the internal waters of Canada, thus giving it sovereignty over and the ability to restrict access to those waters. The United States, on the other hand, maintains that the Northwest Passage is not part of the internal waters of Canada at all, but rather is a strait used for international navigation, thereby giving any nation the right of passage. Together, Canada's ability to use AWPPA to deny ships innocent passage through Canadian waters and the contentious definition of the Northwest Passage waters create a national Arctic navigational scheme that is at best questionably aligned with UNCLOS.

C. The United States and Arctic Navigation

While the United States is an Arctic Coastal State, it has relatively little Arctic coastline compared to Canada and Russia. Since the United States is also the only Arctic Coastal State or Arctic Council member that has not ratified UNCLOS, it is the only member not technically bound by the terms of UNCLOS. Furthermore, the United States has a less-developed stance on the Arctic than Russia and Canada and relies more on general policy than actual legislation to govern its approach to the Arctic region. Nevertheless, the United States has expressed serious interest in maintaining its Arctic territorial rights as well as protecting the Arctic environment. The most recent articulation of the United States' Arctic policy is the May 2013 National Strategy for the Arctic Region. Promulgated by President Barack Obama, the National Strategy emphasizes the United States' goals of safeguarding national security, protecting the Arctic environment, and strengthening international cooperation.

The United States' diplomatic interactions with Russia and Canada regarding Arctic navigation have attempted to encourage both countries to bring their policies more in line with the United States' interpretation of UNCLOS—that is, to make their EEZs and territorial seas more easily accessible and to recognize the Northern Sea Route and Northwest Passage as noninternal waters. As mentioned above, in its interactions with Canada, the United States has maintained that the Northwest Passage is a strait used for international navigation and should therefore be open to transit passage by any ship. The United States has also accused Canada of promulgating navigational laws that violate the UNCLOS principles of innocent passage and “due regard” for navigation. And while Russia considers the Northern Sea Route to be internal waters, the United States argues that since the Northern Sea Route is an international strait, not an internal body of water, ships should be allowed innocent passage and should not have to request permission. The arguments put forward by the United States seem reasonable on their face and look like they would go far towards creating a uniform navigation scheme in the Arctic; however, the United States' refusal to ratify UNCLOS makes its attempts to force its favored interpretation on other countries ring hollow.

D. But Why Do These Inconsistencies Matter?

The regulations promulgated by Arctic Coastal States requiring that ships seek and receive permission before crossing their waters seem to be simply an inconvenience for those wishing to navigate through Arctic waters. In theory, careful planning and communication with the various Coastal States would make satisfying those requirements relatively straightforward. However, Arctic Coastal States having such laws complicates the logistics of Arctic voyages, has the potential to greatly increase the costs of such voyages, and undermines the existing international navigational framework negotiated and agreed to by the Arctic Council nations, the United Nations, and the IMO.
One of the main problems with Arctic navigation laws that require ships to seek permission before crossing the waters of Coastal States (e.g., the laws of Russia and Canada) is that they are inconsistent with the internationally accepted principles of UNCLOS. There is simply no basis in UNCLOS for Coastal States to promulgate laws restricting access to their EEZs in the ordinary course of events. UNCLOS allows nations to promulgate and enforce laws in the territorial sea to ensure safety of navigation, regulation of traffic, conservation of resources, and environmental preservation, and UNCLOS Article 234 allows nations to adopt and enforce laws and regulations for the prevention, reduction, and control of marine pollution in ice-covered areas within the bounds of their EEZs. Those sections, however, do not give Coastal States the right to issue blanket requirements forcing all ships seeking innocent passage to request permission to enter the Coastal State's waters or the right to issue blanket denials of entry to ships of other nations. Furthermore, despite Article 234's expansion of the authority granted to Coastal States regarding the promulgation and enforcement of marine environmental protection laws, there is still a specific requirement that navigational policies have “due regard” for navigation. There is no language that can logically be construed as permitting Coastal States to abridge the right of navigation enjoyed by foreign ships.

*405 III. TOWARD A UNIFORM FRAMEWORK: ENABLING INNOCENT PASSAGE AND THE POLAR CODE AS DELINEATION OF “DUE REGARD” FOR NAVIGATION

Actual application of “due regard” in the real world would likely prohibit Coastal States from denying entry to foreign ships. In order to navigate through the Arctic Ocean in accordance with the impending Polar Code, a shipmaster must take into account safety protocols, current weather conditions, current ice coverage, historical weather conditions and ice conditions, presence of marine mammals, migration paths of mammals, and contingency plans should an accident or foul weather occur. Plotting and navigating the ship's journey is essentially an attempt to create the best balance among safety, weather, and environmental concerns. The right to freedom of passage in the EEZ granted by UNCLOS allows shipmasters to create the best possible balance of all those concerns, rather than the balance that best suits the Coastal State's desire to have the same jurisdictional rights in the EEZ that they do in the territorial sea. While Article 234 of UNCLOS does allow Coastal States to promulgate and enforce navigational laws in the EEZ, the language requiring “due regard for navigation” implies that Coastal States must still allow ships some opportunity for navigation and that they may not bar ships from passing through either their own territorial waters or their EEZs.

Indeed, Arctic navigation laws and policies that require shipmasters to seek permission from the government before attempting passage, like those of Russia and Canada, do not give “due regard” to navigation because they preclude shipmasters from pursuing routes that may be necessitated by the voyage planning requirements of the legally binding Polar Code. This places shipmasters in an unenviable position: if they are denied permission to enter a Coastal State's EEZ, but the best route according to the requirements listed in the Polar Code requires passage through that zone, they will have to make a choice--do they calculate a new route and potentially leave themselves vulnerable to liability under the Polar Code, or do they enter the Coastal State's EEZ and potentially leave themselves vulnerable to enforcement actions by the Coastal State? For example, if an American shipmaster determines that their ship should follow a specific path through the Northern Sea Route based on the current state of Arctic sea ice and historical data, but is denied access by the Russian Ministry of Transport, they will be subjected to liability no matter their choice. Following the Polar Code and proceeding through the Northern Sea Route means there is a high probability that the ship will be seized and its crew taken into custody. Choosing a different route that does not follow the Polar Code's voyage planning requirements means that the ship's flag state--here the United States--could impose financial penalties or legal
liability should anything go wrong, which, given the unpredictable nature of the Arctic environment, makes this option a significant gamble. Without further clarification on the definition of “due regard” or integration between UNCLOS and the Polar Code, both choices mean potential liability.

Setting aside the difficulties of diplomacy and international negotiation, the stance of the Arctic Coastal States as expressed in the Ilulissat Declaration indicates a strong preference for Coastal State sovereignty and distaste for additional sweeping international measures. Indeed, the terms of the Ilulissat Declaration arguably show that the development of a further comprehensive legal regime regarding Arctic navigation would be anathema to the Coastal States. This indicates that the problem of inconsistency with the principles of UNCLOS is best solved by negotiation and mutual understanding rather than conferences, conventions, and more legally binding instruments beyond the existing legal framework.

An efficient approach to deciding the authorship and content of Arctic navigational laws would be to use the voyage planning section of the Polar Code as an interpretive lens for the “due regard” requirement in UNCLOS Article 234. This would mean that if an Arctic Coastal State is promulgating new Arctic environmental protection laws pursuant to Article 234, or if an Arctic Coastal State's Arctic environmental protection law is challenged, the law would be deemed appropriate if it gave ship captains the latitude to comply with all of the Polar Code's voyage planning requirements, and inappropriate if it did not. Using a preexisting list of legally binding requirements that the IMO has decided are mandatory for safe navigation and by which the Arctic Coastal States have already agreed to be bound eliminates the need for further negotiation regarding requirements or definitions.

Interpreting “due regard” in UNCLOS through the lens of the Polar Code is arguably the exact kind of interpretation that UNCLOS itself suggests: requiring “due regard” for navigational interests could easily be understood to incorporate by reference other binding instruments that deal with navigational issues, such as the Polar Code. Furthermore, other international rules of treaty interpretation support such an interpretation of “due regard.” For example, the Vienna Convention on the Law of Treaties, a treaty concerning the international law on treaties that entered into force in 1980, states in Article 31 that treaties should be interpreted in light of subsequent agreements and practices of the member states. Here, since all of the relevant Arctic Coastal States are party to both UNCLOS and the Polar Code, “due regard” in UNCLOS Article 234 ought to be interpreted in light of the Polar Code.

In international law, the parties to treaties are the primary interpreters of what various terms mean. If all Arctic Coastal States were party only to UNCLOS and not the Polar Code, laws such as those passed by Canada and Russia would not be obviously flawed interpretations of Article 234's “due regard” requirement. The entire setup of UNCLOS (i.e., using a standard instead of a rule in a legal framework with only very weak third party adjudication and interpretation) is designed to allow party states to interpret the laws themselves, which inevitably leads to self-interested interpretation. However, as the Arctic Coastal States have also made themselves party to the legally binding Polar Code, the national laws promulgated pursuant to UNCLOS are no longer constrained only by each nation's individual interpretation of what “due regard” should mean. Instead, each nation's interpretation of “due regard” should now be bound by the Polar Code's constraints. While negotiating the Polar Code, nations had the opportunity to explicate an appropriate understanding of what responsible voyage planning looks like, which necessarily delineates the bounds of what giving “due regard” to navigational concerns entails. Because international law generally seeks to give effect to negotiations between parties through interpretive rules such as Article 31 of the Vienna Convention on the Law of Treaties, national laws encompassing the self-interested interpretations of “due regard”--while not obviously
violative of UNCLOS at the time of promulgation--are no longer appropriate applications of the international legal framework given the entry into force of the legally binding Polar Code.

Using an interpretation of the UNCLOS “due regard” standard that contemplates the Polar Code's voyage planning requirements means that Coastal States would still be allowed to promulgate their own Arctic laws within the bounds of the new understanding of “due *409 regard.” Moreover, the international Arctic navigational scheme would be far more uniform than the international system currently in place today. This fine tuning of the international understanding of “due regard” would still allow nations to maintain control over their territorial seas and would only require modification of laws regarding the EEZ. Such a shift in understanding, while it would not necessarily resolve disputes such as that over the Northwest Passage, would still assist individuals navigating the Arctic by providing a more uniform set of navigational laws by which to abide. Having a more uniform set of Arctic navigational laws set in place as soon as possible can only be a positive change for the region, especially if the Arctic sea ice continues to melt rapidly and the Northern Sea Route and Northwest Passage become more viable options for shipping routes.

Indeed, tweaking the current understanding of “due regard” in Article 234 of UNCLOS in light of the Polar Code may provide a simple, realistic path to a uniform international Arctic navigation scheme. Such an updated understanding of “due regard” would protect not only the safety of ships and individuals navigating through Arctic waters, but also the Arctic environment, and would do so without creating an additional legal regime or unduly complicating the existing framework. While UNCLOS certainly contemplates the relationship between navigational laws and protection of marine environments, Article 234's attempt to create a framework that allows for promulgation of national laws protecting the marine environment while still allowing for navigation falls short. As discussed in Part II, the laws promulgated by various Arctic nations in response to Article 234 have resulted in a legal patchwork that may actually leave the marine environment more vulnerable: the laws promulgated by Canada and Russia require advance planning and approval of ships' routes, leaving ship captains very little flexibility should environmental concerns arise (e.g., encountering a pod of whales but not being able to deviate from the set course to avoid it). However, while UNCLOS Article 234's attempt to create a framework protecting both environmental and navigational concerns falls short, the Polar Code does a far better job of integrating environmental and navigational concerns. Rather than using vague terms to describe the outlines of what national Arctic environmental laws should look like, the Polar Code rolls environmental concerns into the Arctic navigation planning process. In terms of environmental protection, this approach is superior because, in addition to providing a concrete list of environmental concerns that must be taken into account, the Polar Code provides a more explicit outline of responsible navigation through Arctic waters than UNCLOS. As a result, the Polar Code minimizes confusion and makes it more likely that the Arctic navigation and environmental laws of different Arctic States will be consistent with one another.

CONCLUSION

The melting sea ice in the Arctic Circle has triggered much discussion among nations and in the media on the potential accessibility of northern shipping routes, which makes the state of navigational law in the Arctic a pressing consideration. The international legal framework regarding navigation in the Arctic, consisting of UNCLOS and the Polar Code, recognizes the interplay between freedom of navigation and the environment. That existing framework attempts to provide for the protection of the Arctic environment and create uniformity in navigational laws that allows for freedom of navigation while still giving Arctic Coastal States some measure of sovereignty. Despite the best efforts of its creators, however, that current international framework lacks clarity and has led to a collection of Arctic navigational laws promulgated by Coastal States that are inconsistent with UNCLOS and undermine the Polar Code. International use of the Voyage Planning requirements in the Polar Code to determine whether a particular Arctic
environmental protection law has “due regard” for navigation consistent with UNCLOS Article 234 would help clarify the international law framework in a way that is easier to conceptualize and enforce.

This definitional scheme would enable more consistent interpretation of the existing innocent passage and EEZ sections of UNCLOS. This could allow standardized Arctic navigation law among all the Arctic States and more efficient shipping, should the northern shipping routes become ice-free enough to allow for navigation. Furthermore, UNCLOS and the Polar Code would together provide an efficient, better-delineated guideline for what polar navigation codes should look like, as well as shape an international legal regime that allows for the protection of the unique--and uniquely fragile--Arctic environment. This would allow Arctic Coastal States the sovereignty to promulgate their own Arctic navigation and environmental protection laws within the bounds of UNCLOS without jeopardizing the uniformity of the Arctic navigational scheme, thereby making Arctic navigation laws not only consistent among nations but also more mindful of the unique navigational hazards and environmental concerns inherent to the Arctic region.

Footnotes

a

J.D. Candidate, 2017, Vanderbilt University Law School; B.A., 2012, Duke University. I would like to thank Professor Timothy Meyer for his thoughtful comments and suggestions; the editors and staff of the Vanderbilt Law Review for their excellent work; and my parents, Bob Williams and Lisa Boccetti, for their unwavering support and encouragement and their willingness to discuss obscure points of Arctic navigation law frequently and at length. I could not have done it without you.


See, e.g., Valur Ingimundarson, Territorial Discourses and Identity Politics: Iceland's Role in the Arctic, in ARCTIC SECURITY IN AN AGE OF CLIMATE CHANGE 174, 177 (James Kraska ed., 2011) (describing the potential for trade routes and navigation through the Arctic as “speculation”); Frédéric Lasserre & Sébastien Pelletier, Polar Super Seaways? Maritime Transport in the Arctic: An Analysis of Shipowners' Intentions, 19 J. TRANSPORT GEOGRAPHY 1465, 1465 (2011) (noting that sea ice melt is “fuelling [sic] many speculative scenarios about the purported renewal of a ‘cold war’, [sic] or even an actual armed conflict, in the Arctic, for the control of ... its sea routes).

Paul Brown, Arctic's Melting Ice Shrinks Shipping Routes, CLIMATE NEWS NETWORK (Aug. 4, 2015), http://climatenewsnetwork.net/arctics-melting-ice-shrinks-shipping-routes/ [https://perma.cc/A2PV-X3YZ] (stating that Arctic ice melt is opening up the Northwest Passage, but noting that the Northern Sea Route will likely not be feasible for winter passage until approximately 2030).

See, e.g., Int'l Maritime Org. [IMO], International Code for Ships Operating in Polar Waters (Polar Code), at Preamble ¶ 5, MSC.385(94) (Nov. 21, 2014) [hereinafter Polar Code] (“The relationship between the [Polar Code's] additional safety measures and the protection of the environment is acknowledged as any safety measure taken to reduce the probability of an accident, will largely benefit the environment.”); ARCTIC COUNCIL, ARCTIC MARINE SHIPPING ASSESSMENT
2009 REPORT 4 (2009) (providing an analysis of the current state of international Arctic navigational laws as they relate to shipping).

See, e.g., Dawson, supra note 2 (linking the rise in volume of traffic to the decrease in sea ice extent); Haas & Howell, supra note 2 (discussing thick sea ice as a reason why feasible Arctic shipping lanes may be years in the future).

See, e.g., Arctic Shipping Issues, NAT'L OCEANIC & ATMOSPHERIC ADMIN. OFF. OF GEN. COUNS., http://www.gc.noaa.gov/gecil_arctic_shipping.html (last visited Jan. 21, 2016) [https://perma.cc/Z54M-5PHE] (noting the pristine nature of the Arctic environment as well as its vulnerability to potential pollution caused by increased shipping traffic, such as oil spills and potential introduction of alien species via accidental or illegal discharge of bilge water, among other concerns).

See, e.g., Threats to America's Arctic, PEW CHARITABLE TRUSTS, http://www.pewtrusts.org/~media/legacy/oceans_north_legacy/page_attachments/pethreatstoamericasarctic.pdf (last visited Jan. 21, 2016) [https://perma.cc/9GW9-CT3E] (stating that “no technology or infrastructure exists to effectively clean up an oil spill in icy Arctic waters, especially in winter when hazardous conditions could delay a response for weeks. A large spill in the Arctic is likely to linger in the ecosystem for decades with devastating consequences to Arctic peoples and the ecosystems on which they depend”).

See, e.g., Polar Code, supra note 5, at Preamble ¶ 5 (“The relationship between the [Polar Code]’s additional safety measures and the protection of the environment is acknowledged as any safety measure taken to reduce the probability of an accident, will largely benefit the environment.”).


See, e.g., UNCLOS, supra note 10; ARCTIC COUNCIL, supra note 5, at 4 (providing an analysis of the current state of international Arctic navigational laws as they relate to shipping, written by an Arctic Council working group that focuses on the preservation of the Arctic Ocean environment); Aldo Chircop, International Arctic Shipping: Towards Scaling-Up of Marine Environment Protection, in CHANGES IN THE ARCTIC ENVIRONMENT AND THE LAW OF THE SEA (Myron H. Nordquist, John Norton Moore, & Tomas H. Heidar eds. 2010) (examining the maritime regulatory framework and how it works to protect the Arctic marine environment); Ingvild Ulrikke Jakobsen, The Adequacy of the Law of the Sea and International Environmental Law to the Marine Arctic: Integrated Ocean Management and Shipping, 22 MICH. ST. INT'L L. REV. 291 (discussing the state of current international shipping and environmental laws applicable to the Arctic).

UNCLOS, supra note 10.

Polar Code, supra note 5.

UNCLOS, supra note 10, at art. 234.

While Greenland is sometimes listed as a separate Arctic Coastal State, it is an island that was a province of Denmark until 1979 and is now a Danish dependent territory, although one with limited rights of self-government. Greenland Profile, BBC NEWS (Feb. 19, 2015), http://www.bbc.com/news/world-europe-18249474 [https://perma.cc/4K52-FH35]. Many sources group Denmark and Greenland together when referring to the Arctic Coastal States, and that is the convention that will be followed in this Note. See, e.g., The Five Coastal States: Canada, Denmark/Greenland, Norway, Russia, and USA, THE ARCTIC GOVERNANCE PROJECT, http://www.arcticgovernance.org/the-five-coastal-states-canada-denmarkgreenland-norway-russia-and-usa.4612672-137746.html (last visited Jan. 21, 2016) [http://perma.cc/6V8B-PF8T] [hereinafter The Five Coastal States] (referring to “Denmark/Greenland” as one of the five Coastal States).

The Five Coastal States, supra note 15 (listing the Arctic Coastal States).

For the full list of Voyage Planning Requirements, see Polar Code, supra note 5, at pt. I-A ch. 11, pt. I-B ch. 12. Any discussion regarding how to interpret multiple international treaties on the same or similar subjects would be incomplete without at least a mention of fragmentation, or the diversification and expansion of international law over time and the attendant complications. See Martti Koskiniemi (Chairman of the Int'l Law Comm'n Study Grp.), Report of the Study Group on the Fragmentation of
International Law: Difficulties Arising From the Diversification and Expansion of International Law, ¶¶ 5-20, U.N. Doc. A/ CN.4/L.682 (Apr. 13, 2006). The body of literature dealing with how international treaties ought to be interpreted in light of each other is far too broad to be thoroughly explored in this Note; however, the issue this Note addresses is an example of fragmentation, and the proposed solution is a way to resolve tension between two international treaties involving the same or similar subject matter—for example, UNCLOS and the Polar Code. For a more thorough and nuanced introduction to fragmentation as a phenomenon, see id. See also Harlan Grant Cohen, Finding International Law, Part II: Our Fragmenting Legal Community, 44 N.Y.U. J. INT’L L. & POL’Y 1049 (2012).


19 Id.; The Arctic Council: A Backgrounder, ARCTIC COUNCIL (May 20, 2015), http://www.arctic-council.org/index.php/en/about-us [https://perma.cc/NZ4X-FUSK]. The Ottawa Declaration also granted permanent participant status to certain nonprofit organizations representing indigenous Arctic peoples so that the indigenous inhabitants of the Arctic Coastal States would have a voice in the Arctic Council. Id. (listing the organizations of indigenous peoples taking part in the Arctic Council as permanent participants). In addition to providing for participation by indigenous peoples, the Ottawa Declaration allows non-Arctic States to apply for observer status, which allows those non-Arctic States to participate in working groups and contribute to the Council. See Steven Lee Myers, Arctic Council Adds Six Nations as Observer States, Including China, N.Y. TIMES (May 15, 2013), http://www.nytimes.com/2013/05/16/world/europe/arctic-council-adds-six-members-including-china.html [https://perma.cc/T7C5-T93B] (discussing the addition of observer states as an indication of the growing global interest in the Arctic and allowing states outside the Arctic Circle to potentially influence the Council’s decisionmaking process).


22 See Arctic Environmental Protection Strategy, supra note 22, at 33-34 (noting the AEPS’s goal of protecting the Arctic environment and commitment to consistency with UNCLOS); Baker, supra note 22, at 38-39 (discussing the foundation of
the AEPS and the importance AEPS placed on adhering to UNCLOS); Chronological Lists of Ratifications of, Accessions and Successions to the Convention and the Related Agreements, UNITED NATIONS DIVISION FOR OCEAN AFF. & T HE LAW OF THE SEAA (June 23, 2016), http://www.un.org/depts/los/reference_files/chronological_lists_of_ratifications.htm [https://perma.cc/JCP7-XSZK] [hereinafter Chronological Lists] (listing the nations that ratified UNCLOS in the order of ratification).

24 The Five Coastal States, supra note 15.

25 Id.


28 Parfitt, supra note 27 (stating that with the planting of the Russian flag on the seabed of the North Pole, “Russia symbolically staked its claim to billions of dollars worth of oil and gas reserves in the Arctic Ocean,” but also noting the “ridicule and scepticism” the gesture prompted among other Arctic Coastal States such as Canada); Russia Makes Renewed Bid for Contentious Arctic Regions, BBC NEWS (Aug. 4, 2015), http://www.bbc.com/news/world-europe-33777492 [https://perma.cc/H375-DFU6] (noting Russia’s 2007 actions and describing their renewed attempts to stake a similar claim as an attempt to get the United Nations to recognize Russia’s claim to the Arctic continental shelf, a claim which has been rejected by the other Arctic Coastal States).

29 Ilulissat Declaration, supra note 26; Baker, supra note 22, at 38-39 (describing the Ilulissat Declaration as a response to the outcry over Russia's planting of a flag on the ocean floor below the North Pole).

30 Ilulissat Declaration, supra note 26.

31 Id.

32 See, e.g., Greg Poelzer & Gary N. Wilson, Governance in the Arctic: Political Systems and Geopolitics, in ARCTIC HUMAN DEVELOPMENT REPORT: REGIONAL PROCESSES & GLOBAL LINKAGES 185, 206 (Joan Nymand Larsen & Gail Fondahl eds., 2014) (noting that the Arctic Coastal States have “come under criticism from non-coastal Arctic states ... who feel that pan-Arctic issues should be discussed by the wider Arctic Council”).

33 Id.; see also Baker, supra note 22, at 38-39 (describing the negative reaction from Sweden, Finland, and Iceland to news of being excluded from the conference which led to the Ilulissat Declaration). Indigenous populations were not invited to participate in the Arctic Ocean Conference, had no input into the contents of the Ilulissat Declaration, and none have signed on to the Declaration, creating further concerns about representation. Julia Rotondo, Ilulissat Declaration: Legal Regimes to the Rescue?, ICE CASE STUDIES (Dec. 13, 2010), http://www1.american.edu/ted/ice/Ilulissat.html [https://perma.cc/7J4X-GFP4].

34 Id.; Baker, supra note 22, at 38-39 (noting that the backlash from the three excluded States is surprising given the similarities in national Arctic policies between Arctic Coastal States and the rest of the Arctic Council States); Lassi Heininen, Arctic Strategies and Policies: Inventory and Comparative Study 67-76 (2012), http://www.rha.is/static/files/NRF/Publications/arctic_strategies_7th_draft_new_20120428.pdf [https://perma.cc/2WBL-LA8G] (comparing the objectives and priorities listed in the Arctic policies of the eight Arctic Council Nations and concluding “that there are many commonalities between the current list of indicators on the priorities and objectives of national strategies and state policies [in the Arctic]”).

AN OCEAN BETWEEN US: THE IMPLICATIONS OF..., 70 Vand. L. Rev. 379


See The United Nations Convention on the Law of the Sea (A Historical Perspective), UNITED NATIONS DIVISION FOR OCEAN AFFS. & THE LAW OF THE SEA (2012) http://www.un.org/depts/los/convention_agreements/convention_historical_perspective.htm [https://perma.cc/MA76-VTMV] [hereinafter UNCLOS Historical Perspective] (describing how UNCLOS standardized the extent of national jurisdiction and provided overarching regulation for “all aspects of the resources of the sea and uses of the ocean ... [to] bring a stable order” to the laws of the sea); see also ARCTIC COUNCIL, supra note 5, at 4 (stating that “[t]here are no uniform, international standards for ice navigators ... in polar conditions”).

UNCLOS Historical Perspective, supra note 37.

Id.

Id.

Id.

Id.


See Background to UNCLOS, supra note 44.

Id.

Id.

For a discussion of the United States’ reasoning for not ratifying UNCLOS, see supra note 21 and accompanying text. See also Chronological Lists, supra note 23.

UNCLOS Historical Perspective, supra note 37.

UNCLOS, supra note 10, pts. III, VII, IX.

Id. arts. 2-5 (granting nations jurisdiction in their territorial seas and defining the limits of the territorial sea).

Id. arts. 55-57 (defining the jurisdiction and rights of nations in their EEZ and defining the breadth of the EEZ).

Id. art. 234 (emphasis added).

Id.

See infra Sections II.A, II.B, and II.C (discussion of the Arctic policies of Russia, Canada, and the United States, respectively).

See supra Introduction.

UNCLOS, supra note 10, at art. 234 (emphasis added). It is important to note that Article 234 provides a standard rather than a rule for what types of national laws and regulations are appropriate under UNCLOS. One way to conceptualize the difference between the two is the extent to which the law must be interpreted in order to determine if a violation has occurred: standards provide a guideline and therefore require a higher level of interpretation in order to determine whether there has
been a violation, while rules lay out what specifically constitutes a violation and so require little--if any--interpretation. See Louis Kaplow, Rules Versus Standards: An Economic Analysis, 42 DUKE L.J. 557, 560 (1992). Standards tend to save time and transaction costs initially, as they are less specific and therefore require less negotiation than rules, but they create greater transaction costs down the line, as they require interpretation. See id. at 577. Rules, on the other hand, are more expensive to promulgate given their specificity, but enforcement costs are much lower. Id. Given the extensive international negotiations that went into forming UNCLOS, it is unsurprising that it uses standards; however, given the interpretation required by standards, it is also unsurprising that different and potentially inconsistent interpretations exist. See infra Part II.


See, e.g., Ice Navigation in Canadian Waters, CANADIAN COAST GUARD 81-83 (Aug. 2012), http://www.ccg-gcc.gc.ca/folios/00913/docs/ice-navigation-dans-les-galces-eng.pdf [https://perma.cc/2PAH-9JQU] (listing Arctic navigational hazards that include collisions with ice; adverse environmental conditions such as low temperature, snow, and high winds; and accumulation of ice on vessels); Arctic, NAT'L WILDLIFE FED'N, https://www.nwf.org/Wildlife/Wild-Places/Arctic.aspx (last visited Jan. 21, 2016) [https://perma.cc/6CQ8-YJLV] (discussing Arctic wildlife and the unique threats to that wildlife).

UNCLOS, supra note 10, pt. II, § 3.

Id. § 3, subsec. A.

Id. arts. 17-19.

Id. art. 21.

Id. art. 24.

Id. arts. 58, 87. The high seas are “all parts of the sea that are not included in the exclusive economic zone, in the territorial sea or in the internal waters of a State, or in the archipelagic waters of an archipelagic State.” Id. art. 86. However, while both the EEZ and high seas confer freedom of navigation on ships of all states, the rights of the Coastal State differ in the two zones: no State may exercise sovereignty over the high seas and each nation must exercise their freedom of navigation with “due regard for the interests of other States in their exercise of the freedom of the high seas,” while Coastal States may exercise sovereignty in their EEZs regarding the exploring, exploiting, conserving, and managing of natural resources. Id. arts. 56, 87.


Id.

Id.

Adoption of a Polar Code, supra note 36.


Member States, INT'L MAR. ORG. (2016), http://www.imo.org/en/About/Membership/Pages/MemberStates.aspx [https://perma.cc/PQ2W-RR7X] (listing all 171 member states and the year they joined the IMO).

Adoption of a Polar Code, supra note 36 (noting the dates of adoption of the Polar Code and the relevant amendments to the International Convention for the Safety of Life at Sea (SOLAS) and International Convention for the Prevention of Pollution
from Ships (MARPOL) required to make it legally binding; the date the Code is expected to enter into force; and a general summary of the Code's contents).

74 *Ice Navigation in Canadian Waters*, supra note 59, at 81-83 (listing hazards associated with navigation in Arctic waters).

75 Adoption of a Polar Code, *supra* note 36 (discussing the background of the Polar Code, the provisions included in the Polar Code, and the dates the Polar Code was adopted and is expected to enter into force).

76 *Id.*

77 SOLAS and MARPOL are considered among the most comprehensive sets of rules and standards on safety and pollution prevention, and as of March 2014 had been ratified by--and therefore were legally binding on--162 and 152 states, respectively. *See* Koji Sekimizu, Sec'y-Gen., Int'l Mar. Org., *Address on The United Nations Convention on the Law of the Sea and the Int'l Maritime Organization* (Mar. 18, 2014) (listing SOLAS and MARPOL as two of the three "most comprehensive sets of rules and standards on safety, pollution prevention, and training and certification of seafarers"). The Polar Code, because it has been incorporated into the existing legal mechanisms present in SOLAS and MARPOL through amendments, will be legally binding on the parties to SOLAS and MARPOL. *IMO Adopts Mandatory Code for Ships Operating in Polar Waters*, INT'L MAR. ORG. *(Nov. 21, 2014)*, http://www.imo.org/en/MediaCentre/PressBriefings/Pages/38-nmsc94polar.aspx#.Vp6IhpMrK8o [https://perma.cc/2H3H-TTLW].


79 *IMO Adopts Mandatory Code for Ships Operating in Polar Waters*, *supra* note 77 (reporting the November 21, 2014 adoption of the safety provisions of the IMO's Polar Code by the Maritime Safety Committee's 94th session, as well as the amendments to SOLAS required to make those provisions legally binding on signatory parties).


81 Together, those nations represent ninety-nine percent of the gross tonnage of the world's merchant fleet. Sekimizu, *supra* note 77. For a complete list of signatories to MARPOL and SOLAS, see *Status of Multilateral Conventions and Instruments in Respect of Which the International Maritime Organization or its Secretary-General Performs Depositary or Other Functions*, INT'L MAR. ORG. 13-17, 102-07 (Oct. 28, 2016), http://www.imo.org/en/About/Conventions/StatusOfConventions/Documents/Status%20-%202016.docx.pdf [https://perma.cc/9GBW-ZZLD]


83 *Id.* pt. I-A ch. 11.

84 The Polar Water Operational Manual includes a list of the capabilities and limitations of the ship, specific procedures the ship should follow in the course of normal operations, procedures to follow in case the ship meets with an accident, and procedures to be followed should the ship find itself in conditions it is unable to withstand. *Id.* pt. I-A ch. 2, pt. I-B ch. 3.

85 *Id.* pt. I-A ch. 11.

86 *Id.* pt. I-B ch. 12.

87 *See supra* note 84 (discussing the safety protocols included in the Polar Water Operations Manual and incorporated by reference into the Polar Code's voyage planning requirements).
The guidance on the voyage planning requirements in Part I-B of the Polar Code does mention minimizing disturbances to marine mammals, and disruption of marine fauna is one of many concerns scientists have had about the introduction of higher traffic through the Arctic. However, this is also an example of the intertwining of environmental and navigational interests: minimizing disturbance to marine mammals minimizes the risk of animal-induced structural damage, which is a serious concern for ships. See generally NATHANIEL PHILBRICK, IN THE HEART OF THE SEA (2001) (detailing the 1820 tragedy of the whale ship Essex, in which a whale rammed the ship and sank it, stranding the twenty-man crew in the middle of the ocean with little food or fresh water).


See, e.g., Fran Ulmer, Alaska and the Arctic, 31 ALASKA L. REV. 161, 165 (2014) (expressing the feeling that the Polar Code is a step in the right direction regarding the protection of the Arctic, but also that it fails to go far enough in addressing Arctic concerns); Richard Wanerman, Freezing Out Noncompliant Ships: Why the Arctic Council Must Enforce the Polar Code, 47 CASE W. RES. J. INT’L L. 429, 429, 431 (2015) (noting that “neither the existing guidelines nor the final Polar Code will have active enforcement powers,” and instead will rely on self-policing of party states to ensure that parties act in conformity with guidelines); Sekimizu, supra note 77 (noting that enforcement of IMO regulations are limited to the actions taken by flag and Coastal States, and that “[i]n principle, IMO treaties do not regulate the nature and extent of coastal State jurisdiction”); Kate Colwell, Polar Code Too Weak to Properly Protect Polar Environments from Increased Shipping Activity, FRIENDS OF EARTH (Nov. 21, 2014), http://www.foe.org/news/archives/2014-11-polar-code-too-weak-to-properly-protect-polar-environments [https://perma.cc/2X5S-7F3U] (including quotes from policy analysts stating various weaknesses of the Polar Code); Karl Mathieson, Polar Code Agreed to Prevent Arctic Environmental Disasters, THE GUARDIAN (Nov. 21, 2014), https://www.theguardian.com/environment/2014/nov/21/polar-code-agreed-to-prevent-arctic-environmental-disasters [https://perma.cc/YLG7-E3N8] (quoting a source as saying that “[t]he safety net is only as good as the [the Polar Code safety manual], and [that manual] is only as good as how it is enforced by the flag state. There are many [flag states] who have both eyes closed”).

See Wanerman, supra note 90; Sekimizu, supra note 77; Colwell, supra note 90; Mathieson, supra note 90.

See, e.g., Northern Canada Vessel Traffic Services Zone Regulations (NORDREG), SOR/2010-127 (Can.) (stating the law of navigation in Canadian Arctic waters); Rules of Navigation on the Water Area of the Northern Sea Route, approved by the Ministry of Transport of Russia, Jan. 17, 2013, registered by the Ministry of Transport of Russia, Apr. 12, 2013, No. 7 (Russ.); THE WHITE HOUSE, NATIONAL STRATEGY FOR THE ARCTIC REGION 1-11 (2013) (discussing the Arctic strategy and policies of the United States).

4 CTR. FOR OCEANS LAW & POLICY, UNITED NATIONS CONVENTION ON THE LAW OF THE SEA 1982, A COMMENTARY 393 (Myron H. Nordquist et al. eds., 1991) (stating that “Article 234 ... is one of the few provisions in the Convention the terms of which were negotiated directly between the States concerned--in this case Canada, the USSR and the United States of America”).

Chronological Lists, supra note 23. For a discussion of the United States' recognition of and refusal to ratify UNCLOS, see supra note 21 and accompanying text.

CTR. FOR OCEANS LAW & POLICY, supra note 93, at 393 (noting that Canada, the USSR, and the United States directly negotiated UNCLOS Article 234 among themselves).

UNCLOS, supra note 10, art. 234. Russia and Canada have both enacted legislation regarding Arctic environmental protection and navigation pursuant to Article 234, while the United States has done little more than delineate the bounds of the contiguous zone, territorial sea, and EEZ, and instead relies on policy. Proclamation 7219, 64 Fed. Reg. 48,701 (Aug. 2, 1999) (delineating the bounds of the contiguous zone of the United States); Proclamation 5928, 54 Fed. Reg. 777 (Dec. 27, 1988) (delineating the bounds of the territorial sea of the United States); Proclamation 5030, 48 Fed. Reg. 10605 (Mar. 10, 1983) (delineating the bounds of the United States' EEZ); Rules of Navigation on the Water Area of the Northern Sea Route, supra note 92 (Russian legislation regarding navigation in the Arctic); Northern Canada Vessel Traffic Services Zone Regulations, supra
note 92 (Canadian legislation regarding navigation in the Arctic); THE WHITE HOUSE, supra note 92 (outlining the Arctic policy of the United States).

CTR. FOR OCEANS LAW & POLICY, supra note 93 (stating that “Article 234 ... [was] negotiated directly between the States concerned--in this case Canada, the USSR and the United States of America”).

UNCLOS, supra note 10, art. 234.

See, e.g., Parfitt, supra note 27 (stating that with the planting of the Russian flag on the seabed of the North Pole, “Russia symbolically staked its claim to billions of dollars worth of oil and gas reserves in the Arctic Ocean” but also noting the “ridicule and scepticism” the gesture prompted among other Arctic Coastal States such as Canada); Russia Makes Renewed Bid for Contentious Arctic Regions, supra note 28 (describing the gesture as an attempt to get the United Nations to recognize Russia's claim to the Arctic continental shelf, and the rejection of that claim by the other Arctic Coastal States); Ruth Sherlock, America and Russia Locked in Race to Control the Arctic, THE TELEGRAPH (Sept. 2, 2015), http://www.telegraph.co.uk/news/worldnews/northamerica/11840640/America-and-Russia-locked-in-race-control-the-Arctic-Circle.html [https://perma.cc/5FE9-A6MR].

NSR--General Area Description, N. SEA ROUTE INFO. OFF., http://www.arctic-lio.com/NSR_generalareadescription (last visited Jan. 21, 2016) [https://perma.cc/4KVQ-3MKX] (describing the geography of the Northern Sea Route and Russia’s view that the Northern Sea Route is comprised of “the internal sea waters, the territorial sea, the adjacent zone and the exclusive economic zone of [Russia]”); What Is the Northwest Passage?, GEOLOGY.COM, http://geology.com/articles/northwest-passage.shtml (last visited Jan. 21, 2016) [https://perma.cc/5ACJ-GAS4] (showing the location of the Northwest Passage, including the Bering Strait).

What Is the Northwest Passage?, supra note 100.

NSR--General Area Description, supra note 100.

See, e.g., Haas & Howell, supra note 2 (finding that the Arctic ice is, on average, over three meters thick and extremely thick ice formations were common); Brown, supra note 4 (stating that Arctic ice melt is opening up the Northwest passage, but noting that the Northern Sea Route will likely not be feasible for winter passage until approximately 2030).

Brown, supra note 4 (remarking that the opening of northern shipping routes would have the effect of “making the sea routes far shorter” for many countries in the northern hemisphere).

Legislation, N. SEA ROUTE INFO. OFF., http://www.arctic-lio.com/nsr_legislation (last visited Jan. 21, 2016) [https://perma.cc/CP9C-9THZ] (providing background regarding the passage of the most recent Russian Arctic navigation laws relating to the Northern Sea Route).


Id. § 10.6. An icebreaker is a ship that has been specially designed to move efficiently through ice-covered waters, usually by using propulsive power to push the bow of the ship above the ice and then relying on the weight of the ship to break the ice. Lawson W. Brigham, Icebreaker, in ENCYCLOPEDIA OF THE ARCTIC 917, 919 (Mark Nuttall ed., 2012). An icebreaker escort is an icebreaker or group of icebreakers assigned to accompany a ship passing through a nation's Arctic waters in order to assist with breaking up ice, ensure that the ship is following the nation's navigational and environmental laws, and provide assistance should an emergency arise. Id.

The fee for icebreaker escorts varies based on the capacity of the ship, the ice class of the ship, the distance for which an escort will be required, and how long the navigation will take. Rules of Navigation on the Water Area of the Northern Sea Route, supra note 92, § 24.

Id. §§ 14-20.
Id. §§ 11-12.


Russia “Seizes” Greenpeace Ship After Arctic Rig Protest, supra note 111; Vidal, supra note 111.

Russia “Seizes” Greenpeace Ship After Arctic Rig Protest, supra note 111; Vidal, supra note 111.


Russia Loses Case over Greenpeace Ship, supra note 112; Russia Ordered to Pay Compensation for Seizure of Greenpeace Ship, Activists, Including Australian, supra note 112.

Foreign Ministry Says That Russia Will Dismiss Greenpeace Ruling, supra note 112; Russia Loses Case over Greenpeace Ship, supra note 112; Russia Ordered to Pay Compensation for Seizure of Greenpeace Ship, Activists, Including Australian, supra note 112; Russia “Seizes” Greenpeace Ship After Arctic Rig Protest, supra note 111.

Foreign Ministry Says That Russia Will Dismiss Greenpeace Ruling, supra note 112; Russia Loses Case over Greenpeace Ship, supra note 112; Russia Ordered to Pay Compensation for Seizure of Greenpeace Ship, Activists, Including Australian, supra note 112; Russia “Seizes” Greenpeace Ship After Arctic Rig Protest, supra note 111.

Foreign Ministry Says That Russia Will Dismiss Greenpeace Ruling, supra note 112; Russia Loses Case over Greenpeace Ship, supra note 112; Russia Ordered to Pay Compensation for Seizure of Greenpeace Ship, Activists, Including Australian, supra note 112; Russia “Seizes” Greenpeace Ship After Arctic Rig Protest, supra note 111.

Arctic Waters Pollution Prevention Act (AWPPA), §§ 18-19, R.S.C. 1985, c A-12; Northern Canada Vessel Traffic Services Zone Regulations, supra note 92.

Northern Canada Vessel Traffic Services Zone Regulations, supra note 92.

Id.

The four different types are a sailing plan report, to be submitted when the ship is about to enter the NORDREG zone; a position report, to be submitted immediately upon entrance into Canadian waters and daily for each day the vessel is in Canadian waters; an additional position report, to be submitted as soon as the shipmaster learns of obstructions to navigation, other ships in distress, malfunctioning or missing navigation aids, ice or poor weather conditions, or pollutants in the water; and final reports, to be provided when the ship berths in Canadian waters and immediately before the ship leaves Canadian waters. Id. Should the ship’s intended route change, the ship is required to submit an additional deviation report. Id.

Arctic Waters Pollution Prevention Act (AWPPA), § 15, R.S.C. 1985, c A-12.

Arctic Waters Pollution Prevention Act (AWPPA), §§ 18-19, R.S.C. 1985, c A-12; Northern Canada Vessel Traffic Services Zone Regulations, supra note 92.

UNCLOS, supra note 10, art. 236; Diplomatic Note, supra note 126.

Canada's ability to refuse ships passage arguably does not provide “due regard” to the navigation of those ships and denies innocent passage to ships, while the lack of exceptions for sovereign immune vessels also refuses those vessels both “due regard for navigation” and innocent passage. UNCLOS, supra note 10, art. 236; Diplomatic Note, supra note 126.

Diplomatic Note, supra note 126.


UNCLOS, supra note 10, arts. 38, 236; Byers & Lalonde, supra note 130, at 1156-58.

Arctic Ocean Map and Bathymetric Chart, supra note 22.

Chronological Lists, supra note 23.


THE WHITE HOUSE, supra note 92.

Id.

In addition to mentioning general promotion of international cooperation in the Arctic, the 2013 National Strategy for the Arctic Region specifically mentions “work[ing] toward U.S. accession to the United Nations Convention on the Law of the Sea.” Id. at 2.

See, e.g., Diplomatic Note, supra note 126 (lauding Canada for environmental Arctic policies while stating that the United States believes Canada should recognize the Northwest Passage as a strait used for international navigation).

UNCLOS, supra note 10, art. 38; Diplomatic Note, supra note 126.

UNCLOS, supra note 10, art. 38; Diplomatic Note, supra note 126.

See, e.g., HEATHER A. CONLEY, ARCTIC ECONOMICS IN THE 21ST CENTURY: THE BENEFITS AND COSTS OF COLD 33 (2013) (stating that “[t]he United States and many other countries assert that the Northern Sea Route is an international strait, granting foreign vessels the right of passage without seeking the permission of the coastal state”).

Shetty, supra note 134 (noting skeptically that the United States is attempting to police other nations' Arctic policies using a treaty that it has not ratified).

For example, the fees ships are charged for the mandatory icebreaker escort required to pass through Russian waters increase depending on the weather conditions, number of icebreakers needed, type of ship being escorted, etc. Rules of Navigation on the Water Area of the Northern Sea Route, supra note 92, § 24.

See supra Sections II.A, II.B.

UNCLOS, supra note 10, arts. 56, 234 (stating the rights of the Coastal State to promulgate laws in the EEZ).

Id. arts. 21, 56, 234.
147 See id. arts. 21, 56 (stating the rights of innocent passage through the territorial sea and the rights of the Coastal State in the EEZ). As discussed in Part II, the language of Article 234 implies that conservation of the Arctic environment could potentially provide a basis for nations limiting the right of innocent passage through portions of their waters, but that language does not suggest that nations may use Article 234 to essentially ban all innocent passage.

148 Compare UNCLOS, supra note 10, art. 234 (allowing countries to promulgate and enforce laws in their EEZs that pertain to protection of the marine environment), with id. art. 56 (giving Coastal States the right to exploit the resources of their EEZs and conduct research, but not to prescribe and enforce navigational laws).

149 UNCLOS, supra note 10, art. 234.

150 Id.


152 UNCLOS, supra note 10, at 115-16. For example, a Coastal State could conceivably enact laws requiring ships passing through to avoid specific areas that are especially environmentally fragile, or areas where the presence or passage of a ship could conceivably have a negative impact on indigenous peoples or their culture so long as those laws did not unduly hamper the passage of foreign ships.

153 See supra notes 95-97 and accompanying text (discussing whether Arctic navigational laws provide “due regard to navigation”). The implication in the juxtaposition of Article 234 and the other UNCLOS articles regarding the EEZ is that the right of Coastal States to proscribe and enforce navigational laws in the EEZ is limited to environmental laws for the protection of the marine environment. The limitation of Coastal State rights in UNCLOS Part V--the part regarding the EEZ--to the rights of exploring, exploiting, conserving, and managing resources implies that those rights delineate the boundary of Coastal State EEZ rights. This means that Article 234 is an exception, and indicates that navigational laws promulgated by a Coastal State that do not have to do with environmental protection are incompatible with the principles of UNCLOS.


155 Because the Polar Code has no enforcement provisions, it is left to the flag states to determine what liability should be assessed for Polar Code violations. As discussed in notes 89-91 and accompanying text, it remains to be seen what exactly that liability will look like.

156 See supra notes 113-119 and accompanying text (discussing seizure of ships by Russia).

157 See supra notes 59, 90-92 and accompanying text (discussing the unique dangers of the Arctic environment and the Polar Code's enforcement mechanism, respectively).

158 Ilulissat Declaration, supra note 26.

159 The statement in the Ilulissat Declaration that the Arctic Coastal States “see no need to develop a new comprehensive international legal regime to govern the Arctic Ocean” is a very clear statement about how the Arctic Coastal States view the prospect of the imposition of further international Arctic navigation law, and suggests that further international law regimes would likely struggle to gain traction. Ilulissat Declaration, supra note 26. Granted, the Ilulissat Declaration was released in 2008, before the promulgation of the Polar Code, but because the Polar Code itself was based on preexisting shipping guidelines and because of the perceived or actual weakness of the Code, it may not be perceived by the Arctic Coastal States as an unduly restrictive international Arctic navigational scheme. See supra notes 75-77, 90-92 and accompanying text (discussing adoption and enforcement of the Polar Code).

160 Vienna Convention on the Law of Treaties art. 31, May 23, 1969, 1155 U.N.T.S. 331, 340 (entered into force Jan. 27, 1980). The relevant article states that when interpreting international treaties, “any subsequent agreement between the parties regarding the interpretation of the treaty or the application of its provisions ... [and] any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation” should be taken into account. Id. It
should be noted that much like with UNCLOS, the United States is a signatory but not a party to the Vienna Convention on the Law of Treaties, although the United States still “considers many of the [Convention’s] provisions ... to constitute customary international law on the law of treaties.” Vienna Convention on the Law of Treaties, U.S. DEP’T OF STATE, http://www.state.gov/s/ll/treaty/faqs/70139.htm (last visited June 19, 2016) [https://perma.cc/2DBC-3K5N].


Vienna Convention on the Law of Treaties, supra note 160, at 340 (stating that “[a] treaty shall be interpreted in good faith” by the parties, taking ordinary meaning and context into consideration).

For a brief discussion of the differences between rules and standards, see supra note 57.

Stephanie Altman, International Maritime Organization Adopts Polar Code, TRENDS (ABA Section of Env’t, Energy, and Res., Chi., Ill.), Jan./Feb. 2016, at 13 (noting the “nearly five years of work and negotiation” that went into creating the Polar Code).


See, e.g., UNCLOS, supra note 10, art. 234 (requiring nations to have “due regard” for navigation when promulgating environmental laws).

See, e.g., Dawson, supra note 2 (discussing the rising shipping volume in the Arctic); Plumer, supra note 2 (discussing new shipping routes). But see generally Haas & Howell, supra note 2 (disputing the feasibility of northern shipping routes due to ice thickness).

Polar Code, supra note 5, at 5; UNCLOS, supra note 10, art. 34.

See supra Part II (analyzing case studies).

Introduction
A. Relying on Russia 57
B. Proactive Strategy 59
I. Background 61
A. Reluctant American Arctic Engagement 62
B. Importance of the American Arctic 67
C. Filling the Arctic Breach? 68
II. Analysis 72
A. Article 234 72
B. U.S. Position on Article 234 74
C. Canadian Interpretation and Leadership 77
D. Russian Interpretation and Leadership 80
E. Canadian and Russian Legal Regimes and Article 234 Seven-Factors Analysis 86
G. Article 234 Within UNCLOS 94
H. Summary 103
Conclusion 105
A. The Way Ahead 105
B. Benefits of Planning and Investment 106
C. Risks in Current Strategy 107
D. Conclusion 108
Appendix A.
Diplomatic Note from the U.S. Embassy to the Canadian Department of Foreign Affairs and International Trade 110
Appendix B.
Letter from U.S. Minister for Economic Energy and Environment Affairs to Canadian Manager of Navigation Safety and Radiocommunications, Operations, & Environmental Programs 113
Appendix C.
Canadian Coast Guard, Vessel Traffic Reporting Arctic Canada Traffic Zone (NORDREG) 116
Appendix D.
Charts Depicting Russia's Icebreaker Escort Fees 119
Appendix E.
Northern Canada Vessel Traffic Services Zone Regulations (NORDREG), SOR/2010-127 (Excerpt) 123

*57 I am concerned that we as a nation are setting ourselves up for another 'Sputnik Moment,' but this time falling behind more than any other country with even non-Arctic nations like China and India investing in icebreakers and acknowledging the value of the region.
--U.S. Senator Lisa Murkowski

**Introduction**

**A. Relying on Russia**

“Without active heavy icebreakers, ‘the control of the Arctic is in the hands of Russia.’” A vivid example of Russia's control of the Arctic, including the U.S. Arctic, is the response to the fuel shortage in Nome, Alaska, during 2012. With the onset of an early freeze that closed the Port of Nome that year, the normal method of using a barge to bring fuel into the City of Nome could not be employed. There was no infrastructure, such as roadways, to get fuel to Nome, and airlifts would have been exorbitantly expensive. Winter was approaching, and winter on the doorstep of the Arctic Circle is a different kind of threat than in other parts of the U.S. The average temperature in January ranges from a high of 13.1 degrees to a low of -2.8 degrees Fahrenheit, which is almost 30 degrees colder than New York City. Fortunately for the citizens of Nome, there was a Russian ice tanker that could transport the fuel, but using it would require a Jones Act waiver from the Secretary of Homeland Security. The Secretary granted the waiver, and the Russian ice tanker, with assistance from U.S. Coast Guard Cutter HEALY (WAGB-20), delivered fuel to the citizens of Nome, thereby avoiding a potential humanitarian crisis. Unfortunately, at the time of this writing, it is questionable whether the Russians would be as motivated to assist the U.S. citizens residing in Alaska if a similar situation arose today due to situations in Eastern Europe and Syria. In light of increasing human activity in the U.S. Arctic, it is equally unfortunate that the U.S. Government has failed to develop any substantive strategy addressing this situation.

It is hard to believe that the U.S. Government would be unable to assist its own citizens in a potentially life-threatening situation anywhere else in the United States. By way of example, it is difficult to imagine the citizens of New York City being in need of emergency federal waivers and action from other nations to ensure they have fuel to heat their homes in the winter. This disparity is just one example that the Arctic, and the U.S. citizens residing there, appear to be an afterthought to the U.S. Government. This must change. The U.S. Government cannot simply abdicate its sovereign responsibilities in the U.S. Arctic. The people living there need and deserve at least the minimum level of protection and services provided to people living elsewhere in the United States.

Article 234 of the United Nations Convention on the Law of the Sea (UNCLOS) provides the authority and opportunity for the U.S. to establish and sustain its sovereignty in the Arctic. Unfortunately, the current U.S. interpretation of Article 234 inhibits the U.S. from exercising its authority in its own Arctic territory. This paper will examine the U.S. interpretation of Article 234, and how the current interpretation is incorrect and counterproductive to U.S. interests in the Arctic. The Canadian and Russian interpretations of Article 234 will be examined and contrasted to the U.S. interpretation. This article argues that the Canadian and Russian interpretations better allow these foreign nations to address the increasing potential of environmental and humanitarian disaster in the Arctic. Furthermore, the rest of the world is substantially complying with the Article 234-based legal regimes of Canada and Russia. This review ultimately concludes that customary international law has developed, or is developing right now, with respect to Article 234, and that the U.S. position regarding Article 234 deviates from the emerging norm being established in the Arctic.

**B. Proactive Strategy**
Canada and Russia have used international legal regimes to strengthen their sovereign presence in the Arctic regions. Both nations have placed particular emphasis on Article 234 of UNCLOS, which focuses on waters that are ice-covered for a majority of the year. Article 234 of UNCLOS states:

SECTION 8. ICE-COVERED AREAS

Coastal States have the right to adopt and enforce nondiscriminatory laws and regulations for the prevention, reduction and control of marine pollution from vessels in ice-covered areas within the limits of the exclusive economic zone, where particularly severe climatic conditions and the presence of ice covering such areas for most of the year create obstructions or exceptional hazards to navigation, and pollution of the marine environment could cause major harm to or irreversible disturbance of the ecological balance. Such laws and regulations shall have due regard to navigation and the protection and preservation of the marine environment based on the best available scientific evidence.

Canada and Russia have specifically referenced this Article as the basis for their unilateral implementation of additional environmental safety regulations and, in the case of Russia, icebreaker escort fees to ensure safety of the environment and seafarers in their respective Arctic Exclusive Economic Zones (EEZ). The U.S. has historically been opposed to reliance on Article 234 for additional regulation of activities on ice-covered waters due to possible impacts on freedom of navigation. Changing the U.S. approach would allow implementation of a regulatory framework, similar to that of Russia and Canada, to enhance environmental protection, safety of life at sea, security, and maritime domain awareness in the U.S. Arctic. Moreover, this revamped approach to Article 234 would likely ensure additional attention and funding for surface assets, a deepwater port, and attached military infrastructure for Arctic operations that would achieve a functional end-state of enhanced safety and security in the U.S. Arctic.

II. Background

“The United States is an Arctic Nation with broad and fundamental interests in the Arctic Region, where we seek to meet our national security needs, protect the environment, responsibly manage resources, account for indigenous communities, support scientific research, and strengthen international cooperation on a wide range of issues.” The official policy of the White House acknowledges that the United States is an Arctic nation, and that this region is home to U.S. citizens and natural resources. Moreover, this policy acknowledges there are national security risk needs. Nonetheless, the U.S. has failed to make any meaningful progress securing and protecting this part of the nation.

Fig. 1: Arctic Shipping Routes

TABULAR OR GRAPHIC MATERIAL SET FORTH AT THIS POINT IS NOT DISPLAYABLE

*62 A. Reluctant American Arctic Engagement

Without question, it is the primary duty of a national government to ensure the safety and security of its citizens. Unfortunately, the United States has taken a “reluctant” approach to executing its sovereign duty to citizens living in its...
Only Arctic region—Alaska. The Federal Government's failure to invest meaningfully in the U.S. Arctic has left this region of the United States without an adequate federal presence or emergency response capabilities. Even when there is a vessel on patrol in the Bering Sea, it can take at least three days to respond to a maritime incident. No other region of the U.S. is faced with such a lack of Federal Government presence and protection. This is a significant issue in an area where the population is subsistence based. Furthermore, vessel traffic has generally continued to intensify due to decreases in multi-year ice that has encouraged additional shipping traffic, adventure cruises, natural resource exploration, and research activity. 

Vessel traffic through the Bering Strait, the unofficial gateway for the Arctic, more than doubled from 220 transits in 2008 to more than 480 in 2012, and then dipped to approximately 440 and 340 in 2013 and 2014, respectively. In addition, vessel traffic along the Northern Sea Route (NSR) has generally been increasing, with approximately 4 vessels sailing the route in 2010, increasing to 34 in 2011, 46 in 2012, and 71 in 2013. In 2014, 53 vessels sailed along the NSR. In comparison, vessel traffic on the Northwest Passage (NWP) has generally decreased over the past three years, with 31 vessels sailing the route in 2012, 22 in 2013, and approximately 16 in 2014. Notably, however, 2014 marked the first time that a shipping vessel traversed the NWP without an icebreaker escort.

The U.S. Government, while citing financial constraints as a roadblock to establishing prevention and response capabilities in the Arctic, has collected billions of dollars from offshore lease sales alone in the U.S. Arctic, and has secured sizeable royalties for any future petroleum extraction. Given the lack of federal funding for efforts in the Arctic, it appears the Federal Government perceives the Arctic as little more than a revenue stream that is undeserving of investment. One thing that petroleum companies, environmental organizations, and citizens residing in and near the Arctic should agree upon is that the U.S. should be using those public proceeds to establish prevention and response capabilities in the U.S. Arctic region. The U.S. Government has chosen a contradictory path by arguing it has no authority to exercise unilateral jurisdiction in its own Arctic territory, and that it is unable to return some of those funds to the Arctic because they appear to have been put to use in other regions of the U.S.

The two primary reasons for the U.S. position is a fear that allowing Article 234 to be applied as written would create a precedent for coastal states to assert jurisdiction in EEZ's elsewhere in the world (i.e., non-polar regions), and that jurisdiction could be asserted upon U.S. vessels. These fears are not completely without rationale, but they do lack a legal basis. With respect to coastal states asserting jurisdiction in non-polar regions not specifically included within Article 234, no nation has asserted such authority under Article 234. Furthermore, the language of Article 234 limits application specifically to areas within polar regions. With regard to areas where Article 234 is applicable, state vessels are specifically precluded from Article 234, and U.S. merchant vessels are already generally complying with the Article 234 jurisdiction by Russia and Canada.

The U.S. Government's failure to ensure enforcement and response capabilities in the face of a changing Arctic environment is tantamount to an abdication of its sovereign duty. A marine casualty that results in a significant discharge of oil or other pollutants in the U.S. Arctic could have a devastating cascading effect on the environment, negatively affecting whale and seal populations, thereby having disastrous impacts on local populations that depend on these animals for their food and livelihood. The devastating effects would be compounded as it would take days, or even weeks, for the United States to mount any type of response.

A change in how the United States interprets Article 234 of UNCLOS could generate fundamental change in how it views and prioritizes its own Arctic interests. This change will allow the country to empower itself with respect to the
Arctic, just like Canada and Russia have done. Notably, Canada and Russia are far from being close allies, yet they consistently interpret Article 234 to provide coastal states with unilateral authority to adopt and enforce legal regimes in areas subject to Article 234 regulation. While the American position generally recognizes the vast majority of UNCLOS as customary international law, the U.S. interpretation of Article 234 deviates from the interpretation of its geographically closest and largest Arctic neighbors.

This discussion regarding the U.S. approach to the Arctic is not simply academic. U.S. interpretation of Article 234 has the potential to affect how the U.S. cares for its Arctic territory and the U.S. citizens residing in and around the Arctic.

B. Importance of the American Arctic

Many U.S. legislators, particularly those from Alaska and the state of Washington, are raising the alarm about the continued decline of U.S. presence and ability to influence Arctic affairs and governance. Nevertheless, these warnings appear to be falling on deaf ears.

Senator Mark Begich, from Alaska, stated that “[i]t's like they've never heard of it .... With the Obama administration we've had to push back pretty hard to convince them and show them why they need to invest in not only icebreakers, but forward operating bases for the Arctic.” Consistent with the Alaskan legislator, Representative Rick Larsen, from Washington, indicated that “[i]t's no surprise' that the Russians are investing heavily in the Arctic. 'They recognize the potential and opportunity there' .... The U.S. continues to lag behind []. The Canadians are working on a new navy base and are far ahead of the U.S. when it comes to icebreakers.”

Likewise, Senator Lisa Murkowski, also of Alaska:

While Russia's investment in military infrastructure is not necessarily a precursor to future hostility, it is more evidence that the United States is not appropriately stepping up its activities in the Arctic and investing in a region where commercial and international activities are increasing ... I am concerned that we as a nation are setting ourselves up for another ‘Sputnik Moment,’ ... but this time falling behind more than any other country with even non-Arctic nations like China and India investing in icebreakers and acknowledging the value of the region.

* The U.S. is the chair of the Arctic Council in 2015 and U.S. citizens, particularly those in Alaska, can only hope that it will add some focus and inspiration to the Federal Government's apathetic approach to addressing the needs of its Arctic territory and American citizens residing there. However, some congressional representatives are apparently apprehensive about the ability of the U.S. to affect Arctic policy, even as the chair of the Arctic Council, because the U.S. has failed to demonstrate a sincere interest in establishing a presence or demonstrating a resolve to ensure U.S. Arctic interests are protected. As U.S. Representative Don Young, R-Alaska, stated, “[u]nfortunately, when our nation takes over the chair of the Arctic Council in 2015, we will be leading from behind.”

As explained above, this region is home to U.S. citizens. Additionally, this area is home to wildlife populations that U.S. native populations rely upon for food. The dearth of prevention and response capabilities in the Arctic means a vastly increased response time to any pollution event or emergent situation. Consequently, in a region that hosts numerous endangered or threatened species, there is a significant chance for harm to the ecosystem if a significant pollution discharge occurs, especially in light of the lack of prevention and response capabilities.
C. Filling the Arctic Breach?

In the face of the U.S. Government's overall indifference to the Arctic, the U.S. Coast Guard has taken the lead in performing many Arctic missions and attempting to provide some degree of Arctic domain awareness. As succinctly stated by the Vice Commandant of the U.S. Coast Guard, “[w]here there are humans on the water, there is a demand for us to keep them safe and secure and ensure environmental responsibility.” The U.S. Coast Guard, as a military service, law enforcement agency, and regulatory agency, executes the following statutory missions throughout the U.S. and around the world: (1) ports, waterways, and coastal security; (2) drug interdiction; (3) aids to navigation; (4) search and rescue; (5) living marine resources; (6) marine safety; (7) defense readiness; (8) migrant interdiction; (9) marine environmental protection; (10) ice operations; and (11) other law enforcement missions.

While all of these duties may be performed with varying degrees of effort based upon the needs at different locations throughout the United States and globally, when it comes to the U.S. homeland, only the Arctic portions of the nation experience a severe dearth of all of these government services. The lack of services is primarily due to a lack of assets and personnel stationed in the Arctic. Since the U.S. Coast Guard is the federal agency primarily tasked with performing both domestic and international ice-breaking operations for the United States, it stands to reason that it would be at the forefront of any effort to establish safety and security in the U.S. Arctic and efforts to obtain adequate resources and assets to perform ice operations in the Arctic.

With respect to assets, the well-known threats presented by polar ice require vessels operating in this environment to have hulls that can break through ice in order to offer safe transit and support to people living and working here. Financial considerations are cited as the primary reason the U.S. Government is unable to fund an Arctic deepwater port or icebreakers that could provide the requisite services, thereby creating what has been described as “an unfunded requirement” for the U.S. Coast Guard. However, international law may provide a basis for recouping a small portion of the costs spent for services rendered to those plying through the U.S. Arctic waters. The combination of any fees charged for services rendered, the billions of dollars from offshore oil lease sales, and any royalties from future extraction can provide a significant opportunity to offset the costs of establishing infrastructure and obtaining assets needed in the U.S. Arctic. As it stands, however, the U.S. Coast Guard is not equipped to meet all of its statutory missions in the Arctic and is valiantly fighting to fill the gaps created by its unfunded mandates.

III. Analysis

A. Article 234

The EEZ is an area measured from the baseline, or mean low-tide mark, seaward to 200 nautical miles. The text of Article 234 provides for unilateral governance by the coastal state in the EEZ in order to protect the environment from major harm. Both Canada and Russia have interpreted and applied Article 234 in this manner. However, there are seven specific requirements that must be satisfied before a legal regime can be adopted and enforced pursuant to Article 234:

1. The legal regime must be non-discriminatory;

2. The legal regime must be focused on the prevention, reduction, and control of marine pollution from vessels;
3. The area regulated must be covered by ice for more than six months of the year;

4. The ice must present obstructions or exceptional hazards to navigation;

5. The legal regime must apply to an area where pollution could cause major harm to or irreversible disturbance to the environment;

6. The legal regime must have due regard for navigation; and

7. The legal regime must be based on the best available scientific evidence.

These requirements make it quite clear that Article 234 is only applicable under very specific and very limited circumstances.

Additionally, Article 234 was placed in its own section within UNCLOS, indicating that it functions in concert with other sections of UNCLOS, such as those sections that institute both innocent passage and transit passage regimes, so long as Article 234 is applicable. Consequently, it is axiomatic that the application and interpretation of Article 234 must be consistent with other applicable Articles. In addition to examining the plain language of Article 234, any apparent contradiction between Articles should be assessed using *lex specialis derogate legi generali*: the rule of legal interpretation that when two legal provisions appear applicable, but contrary to one another, the more specific legal provision will supersede the more general.

An additional point of consideration is how the international community, including U.S. flagged commercial vessels, has responded to the implementation of the unilateral authority exercised by both Canada and Russia pursuant to Article 234. In general, the seafaring public has substantially complied with Canadian and Russian requirements under Article 234. Consequently, the plain language of Article 234 and international *status quo* both establish that Article 234 provides coastal states with the authority to unilaterally exercise jurisdiction pursuant to Article 234 when all of the conditions specified within that Article are satisfied.

**B. U.S. Position on Article 234**

The U.S. position with respect to Article 234, which has been described as inconsistent and ambiguous, generally asserts that Article 234 is wholly subservient to the principle of freedom of navigation. U.S. commentators recognize that Article 234 provides coastal states with authority to implement and enforce regulatory regimes within the very limited parameters set forth in the text of the Article. However, some commentators suggest that the coastal state can only do so under the permission or auspices of multilateral action by the International Maritime Organization.
Additionally, the United States asserts that a coastal state's Article 234 regulatory regime cannot include the possibility of denying passage through its Arctic EEZ, territorial seas, or an international strait, even if a non-state vessel is non-compliant with the coastal state's requirements, because doing so would violate the rights to freedom of navigation, innocent passage, and the *transit passage regime,* respectively. Upon review, however, these latter two averments suffer from significant practical and interpretive shortcomings.

The U.S. position essentially posits an invincible international straits regime that would eviscerate any meaningful interpretation of Article 234. The practical effect under the U.S. position is that coastal states cannot interfere with a vessel's transit, but are instead required to undertake responsive action to clean up any environmental damage, attempt to recoup costs, and impose sanctions after the events occur. In contrast, under the Canadian and Russian position, coastal states could take preemptive action pursuant to Article 234, by precluding non-state vessels that pose a threat to the environment from transiting through waters regulated pursuant to Article 234. It is almost certain that any U.S. citizen on the Alaskan coast would prefer something more proactive than hoping to adequately respond to the environmental damage after their food supply and livelihood have been destroyed. While this illustration might appear “unbelievable,” the EXXON VALDEZ incident indicates it is not outside of the realm of possibility. As will be discussed in greater detail below, only in cases of severe violations, such as instances where the violations are “almost unbelievable,” and threatened to cause “major harm to or irreversible disturbance of the ecological balance” could freedom of navigation be hampered pursuant to “non-discriminatory laws and regulations” adopted and enforced pursuant to Article 234. Furthermore, these preclusions could only be enforced with respect to non-state vessels.

Beyond the problems of practicality, interpreting Article 234 such that it has no impact on freedom of navigation regimes is problematic because it renders Article 234 nonsensical by failing to account for the plain language of the Article itself, together with the rest of UNCLOS. For instance, Article 24, innocent passage, is subject to exceptions implemented “[i]n accordance with this Convention,” which, by its very own language, includes the specific exceptions provided in Article 234. Furthermore, the language of Article 38, which states “[t]ransit passage means the exercise in accordance with this Part,” makes clear that it is subject to Article 34, Legal Status of Waters Forming Straits Used for International Navigation. Article 34 states that Part III—which, as established, includes Article 38—“shall not in other respects affect the ... exercise by the States bordering the straits of their sovereignty or jurisdiction over such waters and their air space, bed and subsoil.” This provides further evidence that the transit passage regime should be interpreted in concert with Article 234.

However, Article 34 also states that “[t]he sovereignty or jurisdiction of the States bordering the straits is exercised subject to this Part and to other rules of international law.” This latter clause is implicitly restrictive and provides the basis for an alternative argument; one that supports the U.S. position that transit passage is an “invincible” right. However, this position requires interpreting the phrase “coastal states have the right to adopt and enforce” in Article 234 to either be devoid of the common meaning of the words constituting the phrase, or to have no substantive effect whatsoever. In short, such an interpretation means Article 234 has no functional application, which seems unlikely since this Article was adopted simultaneous with the rest of the competing Articles comprised in UNCLOS.

The U.S. position fails to recognize that Article 234 carves out a very narrow and very specific exception to the generally applicable principles of freedom of navigation in the EEZ, innocent passage, and transit passage based upon the unique dangers presented in areas where ice covers water for a majority of the year. The plain language and specific, limited application of Article 234 weigh in favor of the Canadian and Russian position.
Finally, it is worth noting that the U.S. interpretation of Article 234 constrains its own ability to assert its sovereign authority and inhibits the U.S. Government's ability to execute its own responsibilities to its citizens in and near the Arctic. While maintaining and justifying a laissez faire approach to the Arctic, the U.S. allows the elements and other nations to dictate development in this region.

C. Canadian Interpretation and Leadership

Canada implemented the current version of its Arctic Waters Pollution Prevention Act (AWPPA) pursuant to the authority provided by Article 234. However, the original version of AWPPA was adopted in 1970, prior to the implementation of UNCLOS, which included Article 234, in 1982. The events that precipitated Canada’s adoption of AWPPA in 1970 are helpful to understand the subsequent adoption of Article 234 in 1982 because the motivation for adopting both AWPPA in 1970 and Article 234 in 1982 stem from the same events.

In 1969, a U.S. flagged oil tanker, MANHATTAN, made a transit through the NWP, although the transit was made without petroleum products. MANHATTAN repeatedly got stuck in ice and required the assistance of U.S. and Canadian icebreakers in order to be set free from the ice. At the end of the transit, it was discovered that MANHATTAN had sustained serious hull damage. Needless to say, the government and citizenry of Canada were alarmed at the prospect of having oil tankers plowing through ice-laden waters on its coastline. Consequently, Canada adopted AWPPA to place restrictions on vessels operating along its Arctic coast. At the time, there were legitimate questions regarding the legality of AWPPA, and even Canada itself appeared to question the legal basis of its own legislation. UNCLOS was later adopted in 1982, which provided an international legal basis for Canada's AWPPA.

AWPPA was amended in 1985, after Article 234 was implemented, and established certain engineering, navigation, and safety standards:

12. (1) The Governor in Council may make regulations applicable to ships of any class specified therein, prohibiting any ship of that class from navigating within any shipping safety control zone specified therein

(a) unless the ship complies with standards prescribed by the regulations relating to

(i) hull and fuel tank construction, including the strength of materials used therein, the use of double hulls and the subdivision thereof into watertight compartments,

(ii) the construction of machinery and equipment, the electronic and other navigational aids and equipment and telecommunications equipment to be carried and the manner and frequency of maintenance thereof,

(iii) the nature and construction of propelling power and appliances and fittings for steering and stabilizing,

(iv) the manning of the ship, including the number of navigating and look-out personnel to be carried who are qualified in a manner prescribed by the regulations,

(v) with respect to any type of cargo to be carried, the maximum quantity thereof that may be carried, the method of stowage thereof and the nature or type and quantity of supplies and equipment to be carried for use in repairing or remedying any condition that may result from the deposit of any such cargo in the arctic waters,

(vi) the free-board to be allowed and the marking of load lines,

(vii) quantities of fuel, water and other supplies to be carried, and
*79 (viii) the maps, charts, tide tables and any other documents or publications relating to navigation in the arctic waters to be carried;

(b) without the aid of a pilot, or of an ice navigator who is qualified in a manner prescribed by the regulations, at any time or during one or more periods of the year, if any, specified in the regulations, or without icebreaker assistance of a kind prescribed by the regulations; and

(c) during one or more periods of the year, if any, specified in the regulations or when ice conditions of a kind specified in the regulations exist in that zone.

Subsequently, Canada implemented the mandatory Northern Canada Vessel Traffic Services Zone Regulations (“NORDREGS”) regime, which require certain reporting and communications standards before vessels can operate in Canadian waters classified as subject to coastal state regulation pursuant to Article 234. To summarize, the Canadian regulatory regime imposes specific hull construction, marine machinery, inspection, and communications requirements for vessels sailing through its Arctic territory. The Canadians also monitor vessel traffic and ice conditions in the NWP by requiring mandatory reporting before, during, and after a vessel enters “waters of Arctic Canada.” The focus of AWPPA is squarely on the enhancement of vessel safety for vessels traversing through ice-covered waters. In this context, it is axiomatic that vessel safety equates to environmental safety because it reduces the likelihood of hull breeches and vessel casualties that would discharge pollution into the environment.

It is worth noting that Canada has not only implemented legal regimes consistent with its interpretation of Article 234, but has also undertaken substantive actions to ensure the safety of vessels and the environment in its Arctic territory. Canada currently has plans to establish a port in its Arctic territory and add another icebreaker to the six Arctic-capable icebreakers already in service. These substantive actions, consistent with the legal regime established under Article 234, provide Canada with the capability to respond to incidents that may threaten vessel safety and the environment.

D. Russian Interpretation and Leadership

Russian interpretation and application of Article 234 is largely consistent with that of Canada, and specifically employs the language of Article 234 to establish the basis for these laws. However, Russia has placed the Arctic as a major focal point of its economy and its expressions of sovereignty. Russia adopted, inter alia, its 1990 Northern Sea Route Regulations, to exert specific authorities over the NSR. Subsequently, Russia has implemented additional national statutes and regulations governing the NSR. The statutory and regulatory framework establishes specific engineering and notification requirements for vessels and crewmembers transiting through Russia's NSR. Similar to Canada, Russia specifically imposes technical and operational standards:
1.4. Vessel--any ship, or other craft regardless of her nationality.

1.5. Special requirements--technical and operational rates and standards as set forth in publications issued by the Administration in addition to the Regulations, including the Guide to Navigation through the Northern Sea Route and the Requirements for the Design, equipment, and Supply of Vessels Navigating the Northern Sea Route.

4. Requirements to vessels and their commanding personnel--A vessel intending to navigate the Northern Sea Route shall satisfy special requirements and her Master, or a person replacing him, shall be experienced in operating a vessel in ice. In situations where these persons have no such experience, or when Master requests so, the Administration (Marine Operations Headquarters) may assign a State Pilot to the vessel to assist in guiding her through the Northern Sea Route.

These regulations also establish mandatory notification guidelines and require vessels to request “guiding” though the NSR, which are sometimes referred to as the “icebreaker escort” fee regulations. The guiding requirements, or icebreaker escort fee regulations, establish fees for services rendered in the context of Article 234. These fees appear to be based upon the precedent established by Article 26.

The general concept of a fee schedule for services rendered is likely consistent with international law. Article 26 of UNCLOS, while specifically applicable to the territorial sea, provides a conceptual legal basis for charging fees when actual services are rendered to assist vessels traveling through Article 234 Arctic waters. As noted, however, Article 26 expressly establishes coastal state authority to charge vessels for services rendered in the coastal state's territorial seas only. This concept is an extrapolation of Article 26 authority to the EEZ, and is presented because it provides an example of where UNCLOS has authorized service fees to be charged, and because the Russian fees could be premised upon this precedent. Article 26 simply illustrates that interpreting the authority granted by Article 234 to similarly allow fees for actual services rendered is not a novel idea or one inconsistent with UNCLOS.

Russia's icebreaker escort fee regulations require icebreaker escort for vessels with particular ice classifications when particular ice conditions are present. The text of Russia's icebreaker fee framework indicates that it is EEZ. The stated objective of Russia's overall regulatory framework is to provide for the safe passage of vessels along the NSR, and the requirements that vessels with lesser ice classifications use icebreaker escorts when certain ice conditions are expected in certain areas along the NSR reasonably pursues that objective. Textually, the regulation and escort fees appear reasonably tailored, and are based upon ice conditions, the size of the vessel, distance of escort, and the
type of cargo being transported. In the context of Article 234, the regulation protects the environment from possible pollution discharges due to marine casualties caused by ice in areas where water is covered by ice most of the year.

Furthermore, the author is unaware of any substantive analysis of the regulations that finds them unreasonable with regard to the services actually rendered. The more unreasonable the escort fees, the less likely shipping companies will be persuaded to use the NSR, which is contrary to Russia's stated intent to increase vessel traffic along the NSR. Consequently, logic lends support to the presumption that Russia's icebreaker escort fee regulations are focused on simply offsetting costs incurred to ensure safe navigation by vessels through its ice-covered areas, in accordance with the authorities provided in Article 234. Whether those regulations are operationally implemented in a manner consistent with the text of the regulations and Article 234 is another question, one that is beyond the scope of this review.

Similar to Canada, Russia has implemented mandatory notification reporting requirements. Vessels are required to report when and where vessels intend to enter the NSR, basic information about the vessel and its crew, and malfunctions of machinery during the transit. Russia also imposes technical engineering and safety equipment standards, together with reporting requirements, in its ice-covered waters to ensure the safety of vessels, life, and the environment.

Russia has not only implemented legislation, but has also taken substantive actions to ensure the safety of the environment and the vessels transiting through its Arctic territory. It has already established deepwater ports and military bases along its Arctic coast, and has already started construction on the largest and most powerful icebreakers in history to add to the twenty Arctic-capable icebreakers it already has. Russia has by far established a greater ability than any other nation to protect the environment and the vessels transiting through its Arctic territory. Moreover, these laws and capabilities have served to help Russia develop its economy and protect Russian citizens in its Arctic territory.

Furthermore, some scholars that have examined the Russian legal regime have concluded that it is generally sound when analyzed in the framework of Article 234 and customary international law. Given the relative consistency of the unilateral and assertive authority being exercised by Canada and Russia, it appears customary international law is developing right now. The rest of the world is substantially complying with the Russian legal regime. Even the primary Classification Society used by the U.S. provides guidance to U.S. flagged commercial vessels to aid compliance with the Russian legal requirements for transiting through the Russian EEZ along the NSR.

E. Canadian and Russian Legal Regimes and Article 234 Seven-Factors Analysis

This review is intended to provide a general overview of the Canadian and Russian legal regimes in the context of Article 234 requirements. An in-depth, line-by-line analysis of the laws adopted and enforced by Canada and Russia is outside the purview of this general review. Analysis of the actual operational practices employed by Canada and Russia to implement their respective regulatory regimes is similarly omitted.

Both the Canadian and Russian legal regimes are generally consistent with Article 234 requirements. An overview of these legal regimes is presented below in the context of the seven-factor analysis introduced above, supra Section III.A, for examining the application of Article 234. Subsequent to reviewing the Canadian and Russian legal regimes in the context of the seven-factor analysis, UNCLOS Articles that might have concurrent application will be examined to assess interactions with Article 234 during the rare occasions that Article 234 is applicable.
1. Non-Discriminatory

The first factor requires examining whether the legal regime is discriminatory. Article 234 requires AWPPA, NORDREGS, and Russia's 1990 environmental regulations and icebreaker escort regulations to apply to all vessels transiting through the EEZ, regardless of nationality. The text of these laws focus on vessel standards, such as ice classification, and qualifications of crewmembers. As written, the laws do not discriminate with regard to nationality, and the substance is reasonably related to safe navigation through hazardous waters covered by ice the majority of the year. There is no appearance of arbitrary discrimination. To the extent that these legal regimes may be applied in a manner that is inconsistent with their plain language is another matter; a fact-specific inquiry that is beyond the scope of this basic analysis. The legal regimes are non-discriminatory on their face.

2. Prevention, Reduction, and Control of Marine Pollution from Vessels

The legal regime must focus on prevention, reduction, and control of marine pollution from vessels. Canada's AWPPA and NORDREGS, and Russia’s 1990 environmental regulations and icebreaker escort regulations, are geared toward vessel safety, and, therefore, they are designed for the protection of the environment. Ensuring vessel safety equates to environmental safety because it reduces the likelihood of hull breeches and vessel casualties that could yield the discharge of pollution into the environment. This is especially true where vessels ply through waters covered with ice for most of the year. Article 234 does not simply provide authority for the prevention of marine pollution, but also for the “reduction and control of marine pollution.” This provides a greater breadth of authority, because it includes both preventative and responsive measures. Coastal states can require response capabilities on Arctic vessels, such as tracking, safety and oil spill response equipment, communications, and escort requirements if those measures are primarily focused on ensuring the protection of the environment. These measures promote vessel safety by requiring enhanced prevention and response capabilities, which improves environmental protection.

3. Covered by Ice for More Than Six Months of the Year

Arctic portions of the Russian, Canadian, and U.S. EEZ's are covered with ice the majority of the year. Even during the best months to navigate through the Arctic, there is usually some ice present. These areas meet the “ice-covered” test for most of the year.

4. Obstructions or Exceptional Hazards to Navigation

Fourth, the climatic conditions and sea-ice must present obstructions or exceptional hazards to the safety of vessels. “Exceptional” navigational hazards are those outside the norm. The norm in Arctic waters covered with ice for most of the year is certainly not the norm for most of the oceans. Although submerged rocks and tidal fluctuations can be experienced in all of the world's oceans, the threat of thick sea ice damaging the hull of a tanker and possibly sinking the vessel is uncommon.

The MANHATTAN example exemplifies the obstructions and hazards facing Arctic vessels. The vessel was specifically fitted to sail through ice-covered Arctic waters and was escorted by multiple icebreakers, but nevertheless became repeatedly stuck in the ice and sustained hull damage. Even during the summer months sea ice presents
risks and vessels can become stuck, requiring assistance from icebreakers. Since such obstructions and hazards are not normal types of hazards encountered in a majority of the world's oceans, they are by definition “exceptional.” Consequently, the significant threat presented by sea ice that can trap a vessel and damage its hull is “exceptional” for the purposes of Article 234.

5. Major Harm or Irreversible Environmental Disturbance by Pollution

The Arctic area landward of the Canadian, Russian, and U.S. EEZ boundaries is home to a large number of threatened or endangered species, such as the polar bear, spectacled eider, and bowhead whale, among many others, and has been described as one of the most environmentally sensitive regions in the world. The harsh Arctic marine environment is one of the most specialized and fragile environments on earth. It is home to wildlife populations that native populations rely upon for food, such as seals, walrus, and bowhead whales. Pollution, particularly oil pollution, remains in the Arctic environment longer than in warmer climates because oil degrades at a slower rate in the Arctic. Furthermore, the dearth of prevention and response capabilities in the Arctic means a vastly increased response time to any pollution event or emergent situation. There is a much greater chance for major harm or irreversible damage to very sensitive environmental region that hosts numerous endangered or threatened species if a significant pollution discharge occurs, especially in light of the lack of prevention and response capabilities.

6. Due Regard For Navigation and the Protection and Preservation of the Marine Environment

Legal regimes must have due regard for both navigation and protection of the environment. AWPPA, NORDREGS, and Russia's 1990 environmental and icebreaker escort regulations allow any vessel to transit through areas subject to Article 234 regulation so long as they comply with the legal regimes adopted and enforced in accordance with Article 234. State vessels, such as warships, are specifically exempted from Article 234. The first portion of this requirement, due regard to navigation, is the one primarily relied upon by the U.S. to challenge the aforementioned legal regimes. The requirement for due regard to navigation is directly linked to “due regard to [ ] protection and preservation of the marine environment.”

The most reasonable interpretation is that there is a balancing requirement for determining whether it is appropriate to “hamper” the right to freedom of navigation for the sake of “protect[ing] and preserv[ing] [ ] the marine environment.” The U.S. has asserted that any requirement under Article 234 that might foreclose the sailing of a vessel through another nation's EEZ, including international straits that provide passage through the territorial seas and EEZ, violates freedom of navigation regimes. This across-the-board, no-exceptions position has fundamental flaws when examined under the narrow exception carved out by Article 234. Applying these legal regimes to state owned or operated vessels would clearly be outside the scope of authority provided by Article 234.

7. Based on the Best Available Scientific Evidence

The author is unaware of any scientific studies that specifically assess the bases of the regulatory regimes of Canada and Russia. The legal regimes are primarily based upon engineering and design standards for vessels operating in polar environments. Some reviewers imply that the requirement for the legal regime to be based upon the best available scientific evidence compels coastal states to undertake studies or investigations that directly test and support the legal regime being implemented under Article 234. However, such an interpretation would be a stretch. The plain language does not require additional studies to be done, only that the legal regime be based on the best scientific data available at the time the regulations are adopted.
The coastal state bears the burden under Article 234 to explain the scientific bases for the requirements, but a failure to clearly explain the scientific basis for each and every requirement does not foreclose analysis under this factor. Analyzing each requirement and its scientific basis is outside this paper's scope. In brief, Canadian and Russian requirements appear logically related to vessel safety.

Strengthened hulls and icebreaker escorts during periods of heavy ice conditions reduce the likelihood that the vessel will experience a casualty due to striking ice or being trapped in ice. Vessel tracking in Arctic waters, and requiring escorts when there are heavy ice conditions, enhances response capability in the event there is a pollution event, search and rescue incident, or commission of a transnational crime--such as weapons of mass destruction proliferation--all of which can negatively impact the environment. The requirements generally appear consistent with international industry standards for vessels operating in ice-covered waters. Consequently, the Canadian and Russian regulations generally satisfy this test.

*94 **G. Article 234 Within UNCLOS**

The following section assesses the authority of Article 234 in the context of other applicable Articles of UNCLOS.

**Article 24: Duties of the Coastal State (Innocent Passage)**

1. The coastal State shall not hamper the innocent passage of foreign ships through the territorial sea except in accordance with this Convention. In particular, in the application of this Convention or of any laws or regulations adopted in conformity with this Convention, the coastal State shall not:

(a) impose requirements on foreign ships which have the practical effect of denying or impairing the right of innocent passage; or

(b) discriminate in form or in fact against the ships of any State or against ships carrying cargoes to, from or on behalf of any State.

2. The coastal State shall give appropriate publicity to any danger to navigation, of which it has knowledge, within its territorial sea.

States may regulate and “hamper” innocent passage in accordance with UNCLOS. Article 234 provides coastal states with unilateral authority to regulate activities within their EEZ, so long as the requirements of Article 234 are satisfied. Article 24 applies to territorial seas. Since a coastal state's authority is greater in its territorial sea than in its EEZ, it would be illogical for Article 234 to provide greater authority in the EEZ than the territorial sea. Article 234 provides coastal state authority in concert with Article 24 where the conditions of Article 234 are satisfied, and the practical effect does not foreclose innocent passage or discriminate against foreign ships.
**Article 26: Charges Which May Be Levied Upon Foreign Ships**

1. No charge may be levied upon foreign ships by reason only of their passage through the territorial sea.

2. Charges may be levied upon a foreign ship passing through the territorial sea as payment only for specific services rendered to the ship. These charges shall be levied without discrimination. 175

Article 26 generally precludes imposing fees upon foreign ships for passing through the territorial sea of a coastal state, 176 but it also allows charges to be levied upon foreign ships sailing through territorial seas where “specific services [are] rendered to the ship,” and the charges are levied without discrimination. 177 Icebreaker fees charged by Russia in the territorial sea portion of the NSR are consistent with UNCLOS if they satisfy the Article 26 requirements in practice. There is no express provision that allows for charging fees for services rendered in the EEZ, so states must rely on the more general authority granted under Article 234, together with the precedent set by Article 26 to charge for services rendered in the Arctic EEZ.

The ambiguity provides ample opportunity for competing arguments about whether such application is consistent with international law. Article 234 provides a broad grant of authority under a very specific set of circumstances. So long as all factors of Article 234 are satisfied by a particular legal regime, that defines the services provided and the fees for those services, it is consistent with the purposes of UNCLOS. Ensuring the safety of vessels traversing these areas equates to protecting the environment. 178 Freedom of navigation is effectively enhanced, not degraded or hampered, by ensuring vessels do not suffer a casualty and are not trapped in ice as they sail through a coastal state's Arctic EEZ. This is especially the case given the regulatory regimes are only applicable to private or commercial vessels, not state vessels which would be expected to have greater capability and responsibility as a national asset.

**Article 38: Right of Transit Passage**

1. In straits referred to in article 37, all ships and aircraft enjoy the right of transit passage, which shall not be impeded; except that, if the strait is formed by an island of a State bordering the strait and its mainland, transit passage shall not apply if there exists seaward of the island a route through the high seas or through an exclusive economic zone of similar convenience with respect to navigational and hydrographical characteristics.

2. Transit passage means the exercise in accordance with this Part of the freedom of navigation and overflight solely for the purpose of continuous and expeditious transit of the strait between one part of the high seas or an exclusive economic zone and another part of the high seas or an exclusive economic zone. However, the requirement of continuous and expeditious transit does not preclude passage through the strait for the purpose of entering, leaving or returning from a State bordering the strait, subject to the conditions of entry to that State.
3. Any activity which is not an exercise of the right of transit passage through a strait remains subject to the other applicable provisions of this Convention. 179

Article 38 is drafted somewhat awkwardly, and can reasonably be interpreted to offer support for both the Canadian/Russian position and the U.S. position. The language of Article 38 states, “[t]ransit passage means the exercise in accordance with this Part,” 180 which makes clear that transit passage is also subject to Articles 34 and 42, which are both in the same Part as Article 38.

Article 34 states that the Articles in that Part of UNCLOS “shall not in other respects affect the ... exercise by the States bordering the straits of their sovereignty or jurisdiction over such waters and their air space, bed and *97 subsoil.” 181 This can be read to mean that transit passage can be limited by coastal states when expressly provided for in UNCLOS.

A later clause in Article 34 also states, “[t]he sovereignty or jurisdiction of the States bordering the straits is exercised subject to this Part and to other rules of international law.” 182 This portion could be read to restrict coastal states from exercising any “sovereignty or jurisdiction” that limits transit passage. Alternatively, it could be read to allow some degree of regulation pursuant to Article 234 because the jurisdiction of the coastal state is being exercised subject to the authority of Article 234 as an “other rule of international law.” The latter interpretation stretches the language beyond its clear meaning because the use of the language “subject to” implies a limitation on coastal state sovereignty and jurisdiction. 183 The later clause in Article 34 appears to weigh in favor of limiting the affect of coastal state legal regimes on the exercise of transit passage.

Article 42: Laws and Regulations of State Bordering Straits Relating to Transit Passage

1. Subject to the provisions of this section, States bordering straits may adopt laws and regulations relating to transit passage through straits, in respect of all or any of the following:

(a) the safety of navigation and the regulation of maritime traffic, as provided in article 41;

(b) the prevention, reduction and control of pollution, by giving effect to applicable international regulations regarding the discharge of oil, oily wastes and other noxious substances in the strait;

(c) with respect to fishing vessels, the prevention of fishing, including the stowage of fishing gear;

(d) the loading or unloading of any commodity, currency or person in contravention of the customs, fiscal, immigration or sanitary laws and regulations of States bordering straits.
2. Such laws and regulations shall not discriminate in form or in fact among foreign ships or in their application have the practical effect of denying, hampering or impairing the right of transit passage as defined in this section.

*98 3. States bordering straits shall give due publicity to all such laws and regulations.

4. Foreign ships exercising the right of transit passage shall comply with such laws and regulations.

5. The flag State of a ship or the State of registry of an aircraft entitled to sovereign immunity which acts in a manner contrary to such laws and regulations or other provisions of this Part shall bear international responsibility for any loss or damage which results to States bordering straits. 184

The right of transit passage is also expressly subject to regulation pursuant to Article 42. Article 42 states that “[s]tates bordering straits may adopt laws and regulations relating to transit passage through straits []. [] Foreign ships exercising the right of transit passage shall comply with such laws and regulations.” 185 There is an exception for state owned or operated vessels and aircraft that limits the application of such laws and regulations: 186 any legal framework imposed pursuant to Article 234 would only be applicable to state owned vessels after the fact, where a state owned or operated vessel acted contrary to such laws and the coastal state experienced an ensuing “loss or damage.” 187 Article 42 offers support for the Canadian and Russian position with respect to non-state owned or operated vessels, because Article 42 expressly requires vessels transiting through an international strait to comply with the laws and regulations that the coastal state requires for transiting through the strait.

However, Article 42 also requires that the laws imposed by the coastal state “shall not discriminate in form or in fact among foreign ships or in their application have the practical effect of denying, hampering or impairing the right of transit passage as defined in this section.” 188 The requirements imposed by the laws of the coastal state cannot hamper the right of transit passage by imposing unreasonable requirements that “have the practical effect of denying, hampering or impairing the right of transit passage.” 189 Imposing generally accepted prevention and response requirements that directly and reasonably relate to enhancing safety of the environment in accordance with Article 234 would not have the “practical effect of denying, hampering or impairing the right of transit passage.” 190 This is especially the case in instances where the coastal state is implementing generally accepted international standards 191 and exercising sui generis authority under the very limited and narrow exception established via Article 234. In contrast, if requirements were so onerous so as to preclude the transit of a significant portion of vessels that the international community considered safe to operate under the conditions described in Article 234, then those regulations would clearly run afoul of the rights secured under Article 42.

AWPPA, NORDREGS, and Russia's 1990 environmental and icebreaker escort regulations allow vessels to transit through the areas regulated pursuant to Article 234, so long as they comply with the regulations. 192 Simply adopting and enforcing regulations pursuant to Article 234 does not provide de facto evidence that the right of transit passage has been violated because Article 42 prohibitions focus on laws and regulations that “have the practical effect of denying,
To show a violation, there must be some modicum of evidence that the legal regime precludes the transit of vessels that the international community considers safe to operate in “severe climatic conditions [where] the presence of ice covering such areas for most of the year create obstructions or exceptional hazards to navigation, and pollution of the marine environment could cause major harm to or irreversible disturbance of the ecological balance.”

The Canadian and Russian regulatory regimes do not “discriminate in form [] among foreign ships [so as to] have the practical effect of denying, hampering or impairing the right of transit passage,” and are generally consistent with internationally recognized norms for vessels operating in polar environments.

**Article 58: Rights and Duties of Other States in the Exclusive Economic Zone**

1. In the exclusive economic zone, all States, whether coastal or land-locked, enjoy, subject to the relevant provisions of this Convention, the freedoms referred to in article 87 of navigation and overflight and of the laying of submarine cables and pipelines, and other internationally lawful uses of the sea related to these freedoms, such as those associated with the operation of ships, aircraft and submarine cables and pipelines, and compatible with the other provisions of this Convention.

2. Articles 88 to 115 and other pertinent rules of international law apply to the exclusive economic zone in so far as they are not incompatible with this Part.

3. In exercising their rights and performing their duties under this Convention in the exclusive economic zone, States shall have due regard to the rights and duties of the coastal State and shall comply with the laws and regulations adopted by the coastal State in accordance with the provisions of this Convention and other rules of international law in so far as they are not incompatible with this Part.

Article 58 secures the right of freedom of navigation in the EEZ, but that right is limited. Article 58 provides that vessels exercising their rights to navigate through the EEZ “shall comply with the laws and regulations adopted by the coastal State in accordance with the provisions of this Convention and other rules of international law in so far as they are not incompatible with this Part.” The plain language tends to support the U.S. position that freedom of navigation is paramount. However, it also provides for the application of other provisions of UNCLOS. The hierarchy of various Articles in an apparent conflict is unclear.

It is reasonable to interpret the compatibility requirement of Article 58 consistent with the requirement in Article 42 on transit passage. The mere possibility that a vessel may be prohibited from transiting through an area regulated pursuant to Article 234 due to the threat the vessel presents to the environment, does not equate to “discriminat[ing] in form or in fact among foreign ships or hav[ing] the practical effect of denying, hampering or impairing the right” of freedom of navigation in the EEZ.

**Article 233: Safeguards With Respect to Straits Used for International Navigation**
Nothing in sections 5, 6 and 7 affects the legal regime of straits used for international navigation. However, if a foreign ship other than those referred to in section 10 has committed a violation of the laws and regulations referred to in article 42, paragraph 1(a) and (b), causing or threatening major damage to the marine environment of the straits, the States bordering the straits may take appropriate enforcement measures and if so shall respect mutatis mutandis the provisions of this section.202

Sections 5, 6, and 7 do not impact transit passage,203 and UNCLOS expressly identifies when a specific legal authority established under UNCLOS will not be interpreted to displace “the legal regime of straits used for international navigation.” 204 Article 234 is in section 8, and was not similarly precluded from displacing the transit passage regime. 205 This is evidence that the drafters of UNCLOS knew very well how to make clear that specific authority provisions would not affect transit passage.

Consequently, Article 233 offers strong support to the proposition that Article 234 can “affect[] the legal regime of straits used for international navigation,” 206 because the drafters could have clearly indicated that Article 234 should be subservient to transit passage had that been their intent.

Article 234: Ice-Covered Areas

Coastal States have the right to adopt and enforce nondiscriminatory laws and regulations for the prevention, *102 reduction and control of marine pollution from vessels in ice-covered areas within the limits of the exclusive economic zone, where particularly severe climatic conditions and the presence of ice covering such areas for most of the year create obstructions or exceptional hazards to navigation, and pollution of the marine environment could cause major harm to or irreversible disturbance of the ecological balance. Such laws and regulations shall have due regard to navigation and the protection and preservation of the marine environment based on the best available scientific evidence.207

The plain language of Article 234 provides coastal states with the exceptional authority to adopt and enforce laws to protect the environment in their EEZs due to the unique dangers presented in areas where ice covers water for most of the year. Article 234 requires balancing between navigation and environmental protection.208 The language itself establishes that, in instances where risk to the environment outweighs the right of navigation, Article 234 provides an exception to the right of transit passage when all seven Article 234 requirements are satisfied.209

Article 236: Sovereign Immunity

The provisions of this Convention regarding the protection and preservation of the marine environment do not apply to any warship, naval auxiliary, other vessels or aircraft owned or operated by a State and used, for the time being, only on government non-commercial service. However, each State shall ensure, by the adoption of appropriate measures not impairing operations or operational capabilities of such vessels *103 or aircraft owned or operated by it, that such vessels or aircraft act in a manner consistent, so far as is reasonable and practicable, with this Convention.210
Article 234 clarifies that Article 234 “do[es] not apply to any warship, naval auxiliary, other vessels or aircraft owned or operated by a State and used, for the time being, only on government non-commercial service.”\textsuperscript{211} To the extent either the Canadian or Russian regulatory regimes under Article 236 are applied to any state vessel or any vessel operated by a state, then that portion of the regulatory regime, or application thereof, is clearly in violation of Article 236.\textsuperscript{212} This specifically places the portion of the Canadian AWPPA that pertains to application of state vessels clearly outside the authority bestowed by Article 234 since that portion of AWPPA implies state owned vessels are subject to AWPPA jurisdiction.\textsuperscript{213}

This Article clarifies that Article 234 has little, if any, impact on current U.S. maritime activity. State vessels are explicitly excluded from application, and, as discussed above, commercial vessels are substantially complying with Article 234.\textsuperscript{214}

H. \textbf{Summary}

There are approximately 436 Articles that comprise UNCLOS and its Annexes, and sometimes many competing Articles can be applicable to certain factual scenarios.\textsuperscript{215} When there is a question of which competing Article has primacy in a given scenario, it is best to interpret the provisions \textsuperscript{104} such that each Article has meaning and ensures effect based on the plain meaning of the Articles.\textsuperscript{216} If Article 234 is always subject to freedom of navigation in the EEZ, to transit passage, and to innocent passage regimes, Article 234 is essentially meaningless because it will never have any consequential application in the Arctic. Such an interpretation precludes application of the Article throughout the NWP and NSR, which pass through vast portions of Arctic coastal states’ EEZ.\textsuperscript{217} The result is a legal oxymoron because the Arctic EEZ will be completely unaffected by a provision \textit{specifically} tailored to address the unique threats and risks presented in that environment. The overall weight of the plain language of the applicable Articles, the fact that the U.S. interpretation renders Article 234 ineffective, and that Article 234 has very specific application to polar environments, tend to support the Canadian and Russian position for unilateral adoption and enforcement.

It seems most appropriate to interpret the interrelation between Article 234 and the rights of freedom of navigation in the EEZ, transit passage, and innocent passage to establish a rebuttable presumption that these navigational rights can only be overcome by demonstrated non-compliance with lawful Article 234 requirements. Specifically, non-compliance would have to be severe enough to present significant risk of pollution to the marine environment that “could cause major harm to or irreversible disturbance of the ecological balance.”\textsuperscript{218} This provides “due regard” for navigation, but also provides a reasonable interpretation of Article 234, which requires balancing of navigational rights with “due regard to ... the protection and preservation of the marine environment ....”\textsuperscript{219} As required by the plain language of Article 234, there must be a balancing of these two important coastal state responsibilities, protecting freedom of navigation and protecting the environment.\textsuperscript{220}

Accordingly, when operating in the Arctic, coastal states have the responsibility to ensure that navigation is not only “free,” but that it is executed in a manner that is safe and protects the environment,\textsuperscript{221} especially in \textsuperscript{105} light of the unique threats presented by an ice-laden navigational area.\textsuperscript{222} Coastal states owe this obligation to everyone plying their ice-laden waters. Moreover, the coastal states also owe this obligation to their own citizens who rely on the government to protect them from environmental disasters that can threaten life and livelihood if major environmental damage occurred because the coastal state failed to establish appropriate prevention and response capabilities. Nevertheless, under this line of reasoning, it would be incumbent upon the coastal state to demonstrate balancing these two important interests and finding non-compliance that threatened to cause “major harm to or irreversible disturbance of the ecological balance.”\textsuperscript{223}
before denying entry to a vessel pursuant to Article 234 authority. Consequently, only under the most extreme set of circumstances would a coastal state be able to actually “hamper” a vessel's right to freedom of navigation, transit passage, or innocent passage.

IV. Conclusion

A. The Way Ahead

1. U.S. Recalcitrance is Deviant and Counterproductive Internationally and Domestically

Given the relative consistency of the unilateral authority being exercised by Canada and Russia, it appears customary international law has developed, or is developing right now, with respect to coastal state authority on ice-covered areas within the EEZ. The rest of the world is substantially complying with the Canadian and Russian regimes that rely upon Article 234 as a legal basis. The U.S. position regarding Article 234 deviates from the norm that is now being established in the Arctic.

*106 2. U.S. Assertiveness in Arctic Territory

U.S. citizens would benefit from the U.S. government asserting its authority in the Arctic consistent with other Arctic nations. The United States would have to recognize and respect the assertion of other nations' rights pursuant to Article 234. Doing so would enhance sovereignty and stability in the Arctic by augmenting consistency in Arctic legal authorities, and protecting the environment and interests of all people living in the Arctic.

Recognizing the authority granted by Article 234 would allow the U.S. to focus and apply its authority to the region in a manner consistent with Canada and Russia. This would provide additional opportunities to enhance funding to address U.S. shortcomings in the Arctic, and would allow for the recoupment of actual expenses for services rendered to vessels transiting through U.S. Arctic waters.

B. Benefits of Planning and Investment

The differences in the interpretation of Article 234 are not without substantive effects. Imagine, for a moment, a deepwater port in the U.S. Arctic, perhaps Barrow, with four U.S. Arctic-capable icebreakers that regularly patrol and resupply the port. At the port would be equipment stockpiled for responding to an environmental threat, and an air station housing aviation assets to respond to emergency situations. These assets would also provide enhanced maritime domain awareness, which delivers the capability to track the development of dangerous situations. This capability would enable responders to engage in preventative action to stave off the development of an emergency situation or catastrophe.

There is a large shipping vessel coming through the Northwest Passage or the Northern Sea Route, and it manages to get stuck in ice just north of the Bering Strait. If the vessel tries ramming through the ice to free itself, it could damage its hull, releasing petroleum products northward of the bottleneck created by the Bering Strait. The potential loss of life and damage to the environment could be catastrophic, especially during the bowhead whale migration through the Strait. The catastrophe is averted because the United States has an icebreaker that can respond that same day. The vessel is safely freed from the ice and continues on its journey south without further incident. Success!

The United States would have the ability to charge the shipping company costs for services rendered to free the vessel and avert the potential crisis. A small price to pay for avoiding a potential disaster that would likely have been
more costly in terms of environmental damage, possible loss of human life, loss of the vessel, and the financial costs associated with mitigating a significant pollution event. Any fees the U.S. Government charges for services rendered, with the billions of dollars in revenue the obtained from offshore oil leases in the Arctic, could make it financially feasible to invest in the region.

C. Risks in Current Strategy

Unfortunately, the response and capability assets described in the scenario above are not in place, and there is no plan to ensure such measures in the future. Without these measures, American response capability would be extremely limited, as Congress and the Congressional Research Service recognize. The results could be catastrophic to life and the environment as days or even weeks passed as assets “rush” to the area in an attempt to simply begin mounting a response to an incident. There could be loss of the vessel, human life, and a pollution event that could destroy wildlife populations such as bowhead whales, walruses, ringed seals, and eiders, among other at-risk species. There would also be the possibility of a resulting humanitarian crisis because local populations would no longer have their primary food supply. The United States has accepted these risks through its inaction.

D. Conclusion

While the United States sits idly by, Russia, Canada, China, and a host of other nations are building icebreakers and asserting their sovereign interests in the Arctic to protect and secure their environment and citizens in the Arctic. Meanwhile, the U.S. cannot, without help from other nations, ensure that its own citizens have heating fuel and that their food supply can be protected in the event of an environmental disaster, such as a significant oil spill or other maritime casualty in the Arctic. America has largely failed in its sovereign responsibilities to the citizens of Alaska, who still rely upon subsistence activities for survival and livelihood.

The United States is overdue in tackling its sovereign responsibilities in the Arctic. It should acknowledge the unique authority provided by Article 234 to address these challenges, and use its sovereign authority to protect its territory and citizens in the Arctic. The U.S. is an Arctic nation—it is well past time it acts like it. Instead of arguing with its Arctic neighbors, the U.S. should applaud their efforts and coordinate similar efforts to ensure safety and security throughout the Arctic.

*110 Appendix A. Diplomatic Note from the U.S. Embassy to the Canadian Department of Foreign Affairs and International Trade

No. 625

The Embassy of the United States of America presents its compliments to the Department of Foreign Affairs and International Trade and has the honor to refer to the Northern Canada Vessel Traffic Services Zone Regulations (NORDREGs) which entered into effect on July 1, 2010.

The United States notes its support for the navigational safety and environmental protection objectives of NORDREGs and commends the Government of Canada for its efforts to promote the protection of the marine environment in the Arctic. As conditions in the Arctic continue to change and the volume of shipping traffic increases, Arctic coastal States need to consider ways to best protect and preserve this sensitive region.
The Government of the United States of America advises, however, that it continues to be concerned that the NORDREGs are inconsistent with important law of the sea principles related to navigational rights and freedoms and recommends that the Government of Canada submit its vessel traffic services and mandatory ship reporting system to the IMO for adoption.

Among our concerns, the NORDREGs purport to require Canadian permission for foreign flagged vessels to enter and transit certain areas that are within Canada's claimed exclusive economic zone and territorial sea and that enforcement action could include prosecution. In the view of the United States, this is not consistent with navigational rights and freedoms within the exclusive economic zone, the right of innocent passage within the territorial sea, and the right of transit passage through straits used for international navigation, all of which are bedrock principles of the law of the sea.

DIPLOMATIC NOTE

*111 While Article 234 of the Law of the Sea Convention (the Convention) allows coastal states to adopt and enforce certain laws and regulations in ice-covered areas within the limits of their exclusive economic zones, these laws and regulations must be for the prevention, reduction and control of marine pollution from vessels and have “due regard to navigation.” The United States does not believe that requiring permission to transit these areas meets the condition set forth in Article 234 of having due regard to navigation.

Additionally, the NORDREGs do not provide express exemptions for sovereign immune vessels from the applicability and enforcement of the final regulations. While the NORDREGs note that enforcement action would be consistent with international law, the United States wishes to note that, by virtue of Article 236 of the Convention, sovereign immune vessels are immune not only from enforcement of NORDREGs but also their applicability. The United States expects that this is a matter upon which our governments agree.

Finally, from a safety of navigation perspective, the United States has concerns about whether the NORDREGs vessel traffic services system is consistent with IMO guidance on the establishment of vessel traffic services.

In our view, measures like those contained in NORDREGs should be proposed to and adopted by the IMO to provide a solid legal foundation and broad international acceptance. The United States would welcome the opportunity to work with Canada and with others at the IMO on this matter.

The United States also reiterates its long-standing view that the Northwest Passage constitutes a strait used for international navigation. At a minimum, a measure such as the NORDREGs for an international strait would need to be proposed at and adopted by the IMO.

*112 The United States noted with concern the references to “sovereignty” in the statements accompanying the announcement of the regulations. The United States wishes to note that the NORDREGs do not, and cannot as a matter of law, increase the “sovereignty” of Canada over any territory or marine area.

The Embassy of the United States of America avails itself of this opportunity to renew to the Department of Foreign Affairs and International Trade the assurances of its highest consideration.

Embassy of the United States of America.
Ottawa, August 18, 2010.
Appendix B. Letter from U.S. Minister for Economic Energy and Environment Affairs to Canadian Manager of Navigation Safety and Radiocommunications, Operations, & Environmental Programs

Embassy of the United States of America
Ottawa, Canada

March 19, 2010

Robert Turner, Manager,

Navigation Safety and Radiocommunications,
Operations & Environmental Programs,

Marine Safety Directorate,

Department of Transport,

Place de Ville, Tower C,

330 Sparks Street, Ottawa,

Ontario K1A 0N5

Subject: Canada Gazette, Part I, Saturday, February 27th, 2010; Vol. 144, No. 9: proposed Northern Canada Vessel Traffic Services Zone Regulations

Dear Mr. Turner,

On behalf of the Government of the United States of America, the Embassy wishes to provide comments on the proposed Northern Canada Vessel Traffic Services Zone Regulations (NORDREG) published in the Canada Gazette on February 27, 2010.

The United States of America compliments the Government of Canada's continued efforts to provide for the safety of navigation and protection of the marine environment in the Arctic area. As conditions in the Arctic evolve, all Arctic coastal states will need to consider ways to protect and preserve this sensitive region. We note the collaborative efforts we have taken with Canada in this regard.

The notice of proposed regulations states that the proposed regulations are “consistent with international law regarding ice-covered areas.” In light of this, the United States understands that Canada considers Article 234 of the Law of the Sea Convention (LOSC), entitled, “Ice-covered areas,” to provide an international legal basis for its proposed NORDREG Zone Regulations. That article provides a coastal state with authorities to adopt and enforce certain laws and regulations for the prevention, reduction and control of marine pollution from vessels in ice-covered areas within the limits of its exclusive economic zone when certain conditions are met. While we appreciate Canada's stewardship efforts in the Arctic region, we wish to take this opportunity to express our concerns that the new regulations appear to be inconsistent with international law, including LOSC Article 234.
First, the regulatory impact analysis statement accompanying the proposed regulations indicates that Canadian permission would be required for foreign flagged vessels to enter and transit certain areas that are within Canada's claimed exclusive economic zone and territorial sea and that enforcement action could include prosecution. If so, this would be a sweeping infringement of freedom of navigation within the exclusive economic zone and the right of innocent passage within the territorial sea, both of which are bedrock principles of the law of the sea. While Article 234 of the LOSC allows Coastal States to adopt and enforce certain laws and regulations in ice-covered areas within the limits of the exclusive economic zone, these laws and regulations must be for the prevention, reduction and control of marine pollution from vessels and have "due regard to navigation." The United States does not believe that requiring permission to transit these areas meets the obligation set forth in Article 234 of having due regard to navigation.

Second, under LOSC Article 234, laws and regulations for the prevention, reduction and control of marine pollution from vessels in ice-covered areas within the limits of the exclusive economic zone must also be non-discriminatory. The proposed regulations rely on Canada's Shipping Control Act, which exempts vessels chartered to the Canadian Forces. However, it appears neither the Shipping Control Act nor the proposed regulations contain a provision for similarly-situated foreign vessels. This would be discriminatory, in contravention of LOSC Article 234.

Third, while the Shipping Control Act exempts vessels belonging to a foreign military force, the proposed regulations do not appear to provide an exemption for all sovereign immune vessels, including chartered vessels carrying military supplies. However, LOSC Article 236 specifies that Article 234 is among those provisions of the Convention that "do not apply" to sovereign immune vessels.

Fourth, under LOSC Article 234, laws and regulations adopted must be based on the "best available scientific evidence." The Notice of the regulations did not refer to any scientific studies in developing the proposed regulations. The United States is interested to know the scientific evidence that was considered in the development of these proposed regulations. Article 234 is likewise limited to "ice-covered areas," namely those areas covered by ice for "most of the year." Recognizing that the Notice states that "ice levels have recently been observed to be at an all-time low," the United States is likewise interested to know what information has been used to determine how this condition has been met throughout the entire area covered by the NORDREG Zone.

Finally, we note that the usual process for ensuring safety of navigation and prevention of pollution from ships is to establish such measures at the International Maritime Organization (IMO). In this regard, we would like to bring to Canada's attention relevant provisions of the International Convention for the Safety of Life at Sea, in particular Chapter V, Regulations 10 and 11, that require mandatory ship routing and reporting systems to be submitted to the IMO for adoption. We would be interested to learn whether Canada will avail itself of such an approach. The United States would welcome the opportunity to work with Canada and with others at the IMO in this regard.

The United States also reiterates its longstanding view that the Northwest Passage constitutes a strait used for international navigation. At a minimum, a measure such as the NORDREG Zone Regulations for an international strait would need to be proposed and adopted at the IMO.

In conclusion, we wish to emphasize that the United States does not oppose the Government of Canada's voluntary vessel traffic services zone and voluntary provisions for vessel registration and reporting. We likewise do not discount the need for action to protect the sensitive areas of the Arctic.

The United States supports the stewardship goals of the proposed NORDREG Zone Regulations. Such proposals, however, must have a firm international legal foundation and be implemented in a manner consistent with the law of the sea.
Thank you for the opportunity to comment on the proposed regulations. We look forward to our continued collaboration on this and other areas of mutual interest.

Sincerely,

Eric Benjaminson
Minister--Counselor, Economic Energy and Environment Affairs

*116 Appendix C. Canadian Coast Guard, Vessel Traffic Reporting Arctic Canada Traffic Zone (NORDREG)

Canadian Coast Guard

Vessel Traffic Reporting Arctic Canada Traffic Zone (NORDREG)

The purpose of this notice is to describe to shipboard personnel the ship reporting procedures to be followed by vessels when within or intending to enter the waters of Arctic Canada.

Northern Canada Vessel Traffic Services Zone (NORDREG) includes the shipping safety control zones prescribed by the Shipping Safety Control Zones Order, the waters of Ungava Bay, Hudson Bay and Kugmallit Bay that are not in a shipping safety control zone, the waters of James Bay, the waters of the Koksoak River from Ungava Bay to Kuujjuaq, the waters of Feuilles Bay from Ungava Bay to Tasiujaq, the waters of Chesterfield Inlet that are not within a shipping safety control zone, and the waters of Baker Lake, and the waters of the Moose River from James Bay to Moosonee.

NORDREG objectives:

The Northern Canada Vessel Traffic Services Zone Regulations formally establish the Northern Canada Vessel Traffic Services (NORDREG) Zone and, consistent with international law regarding ice-covered areas, implement the requirements for vessels to report information prior to entering, while operating within and upon exiting Canada's northern waters. The Regulations replace the informal NORDREG Zone (i.e. Arctic Canada VTS zone) and the voluntary reporting system that has existed in Canada's northern waters, enhancing the effectiveness of the official NORDREG Zone and Canada's ability to facilitate the safe and efficient movement of marine traffic. The Regulations will enhance the safety of vessels, crew and passengers, and will safeguard the unique and fragile Arctic marine environment. The Regulations are designed to ensure that the most effective services are available to accommodate current and future levels of marine traffic.

The Northern Canada Vessel Traffic Services Zone regulations apply to:

a. vessels of 300 gross tonnage or more;

b. vessels that are engaged in towing or pushing another vessel, if the combined gross tonnage of the vessel and the vessel being towed or pushed is 500 gross tonnage or more; and

c. vessels that are carrying as cargo a pollutant or dangerous goods, or that are engaged in towing or pushing a vessel that is carrying as cargo a pollutant or dangerous goods.

Reports required:
Type of report

Every report required by any of sections below must begin with the term “NORDREG” and be followed by whichever of the following two letters corresponds to the report:
1. “SP”, in the case of a sailing plan report;
2. “PR”, in the case of a position report;
3. “FR”, in the case of a final report;
4. “DR”, in the case of a deviation report.

Sailing plan report

1. A sailing plan report must be provided
   a. when a vessel is about to enter the NORDREG Zone;
   b. more than one hour but not more than two hours before a vessel departs from a berth within the NORDREG Zone, unless the vessel is moving to another berth in the same port; and
   c. immediately before a vessel gets underway within the NORDREG Zone, if the vessel
      i. has been stranded,
      ii. has stopped as a result of a breakdown in the main propulsion or steering system, or
      iii. has been involved in a collision.

Position report

1. A position report must be provided
   a. immediately after a vessel enters the NORDREG Zone; and
   b. daily at 1600 Coordinated Universal Time (UTC), if a vessel is underway within the NORDREG Zone, unless the information required by regulation 19-1, Long-range identification and tracking of ships, of Chapter V of SOLAS, is being transmitted in accordance with that regulation.
Additional position report

1. A position report must also be provided as soon as feasible after a vessel's master becomes aware of any of the following, if the vessel is within or about to enter the NORDREG Zone:
   a. another vessel in apparent difficulty;
   b. any obstruction to navigation;
   c. an aid to navigation that is not functioning properly or is damaged, out of position or missing;
   d. any ice or weather conditions that are hazardous to safe navigation; and
   e. a pollutant in the water.

Final report

1. A final report must be provided
   a. on the arrival of a vessel at a berth within the NORDREG Zone; and
   b. immediately before a vessel exits the NORDREG Zone.

Deviation report

1. A deviation report must be provided when
   a. a vessel's position varies significantly from the position that was expected based on the sailing plan report; or
   b. a vessel's intended voyage changes from the sailing plan report.

Northern Canada Vessel Traffic Services Zone Regulations

Address of report

Every report must be addressed to NORDREG CANADA and be provided to one of the Marine Communications and Traffic Services Centres that is designated by the Canadian Coast Guard to receive the report.

Please forward your information to Iqaluit MCTS via radio, facsimile, email, telex or telephone.

Iqaluit MCTS
*118  Telephone: 867-979-5269
Fax: 867-979-4264

NORDREG

Iqaluit MCTS

P.O. Box 189
Iqaluit, NU
X0A 0H0

Telephone: 867-979-5724
Fax: 867-979-4264

Email: iqaNordreg@innav.gc.ca

Telex (telefax): 063-15529

Telegraphic Identifier - NORDREG CANADA

Date modified: 2013-06-24
Canadian Coast Guard, Vessel Traffic Reporting Arctic Canada Traffic Zone (NORDREG), http://www.ccg-gcc.gc.ca/eng/MCTS/Vtr_Arctic_Canada (last modified June 24, 2013).

*119  Appendix D. Charts Depicting Russia's Icebreaker Escort Fees

Tariffs for provision of icebreaking pilotage services provided by the FSUE # Atomflot# in the Northern Sea Route water area

For vessels with a gross tonnage up to 5 000

---

P.O. Box 189
Iqaluit, NU
X0A 0H0

*118  Telephone: 867-979-5269
Fax: 867-979-4264

NORDREG

Iqaluit MCTS

P.O. Box 189
Iqaluit, NU
X0A 0H0

Telephone: 867-979-5724
Fax: 867-979-4264

Email: iqaNordreg@innav.gc.ca

Telex (telefax): 063-15529

Telegraphic Identifier - NORDREG CANADA

Date modified: 2013-06-24
Canadian Coast Guard, Vessel Traffic Reporting Arctic Canada Traffic Zone (NORDREG), http://www.ccg-gcc.gc.ca/eng/MCTS/Vtr_Arctic_Canada (last modified June 24, 2013).

*119  Appendix D. Charts Depicting Russia's Icebreaker Escort Fees

Tariffs for provision of icebreaking pilotage services provided by the FSUE # Atomflot# in the Northern Sea Route water area

For vessels with a gross tonnage up to 5 000

---
### Table 1—Tariffs for the Summer-Autumn Navigation Period

<table>
<thead>
<tr>
<th>Vessel’s Ice Strengthening Class</th>
<th>Pilotage Within 1 Zone</th>
<th>Pilotage Within 2 Zones</th>
<th>Pilotage Within 3 Zones</th>
<th>Pilotage Within 4 Zones</th>
<th>Pilotage Within 5 Zones</th>
<th>Pilotage Within 6 Zones</th>
<th>Pilotage Within 7 Zones</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>893.68</td>
<td>1072.42</td>
<td>1251.16</td>
<td>1429.90</td>
<td>1608.63</td>
<td>1787.37</td>
<td>1787.37</td>
</tr>
<tr>
<td>Ice 1</td>
<td>625.58</td>
<td>750.70</td>
<td>875.81</td>
<td>1000.93</td>
<td>1126.04</td>
<td>1251.16</td>
<td>1251.16</td>
</tr>
<tr>
<td>Ice 2</td>
<td>580.90</td>
<td>697.07</td>
<td>813.25</td>
<td>929.43</td>
<td>1045.61</td>
<td>1161.79</td>
<td>1161.79</td>
</tr>
<tr>
<td>Ice 3</td>
<td>536.21</td>
<td>643.45</td>
<td>750.70</td>
<td>857.94</td>
<td>965.18</td>
<td>1072.42</td>
<td>1072.42</td>
</tr>
<tr>
<td>Arc 4</td>
<td>446.84</td>
<td>536.21</td>
<td>625.58</td>
<td>714.95</td>
<td>804.32</td>
<td>893.68</td>
<td>893.68</td>
</tr>
<tr>
<td>Arc 5</td>
<td>442.37</td>
<td>530.85</td>
<td>619.32</td>
<td>707.80</td>
<td>796.27</td>
<td>884.75</td>
<td>884.75</td>
</tr>
<tr>
<td>Arc 6–Arc 9</td>
<td>437.91</td>
<td>525.49</td>
<td>613.07</td>
<td>700.65</td>
<td>788.23</td>
<td>875.81</td>
<td>875.81</td>
</tr>
<tr>
<td>VESSEL'S ICE STRENGTHENING CLASS</td>
<td>PILOTAGE WITHIN 1 ZONE</td>
<td>PILOTAGE WITHIN 2 ZONES</td>
<td>PILOTAGE WITHIN 3 ZONES</td>
<td>PILOTAGE WITHIN 4 ZONES</td>
<td>PILOTAGE WITHIN 5 ZONES</td>
<td>PILOTAGE WITHIN 6 ZONES</td>
<td>PILOTAGE WITHIN 7 ZONES</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Arc 4</td>
<td>1117,11</td>
<td>1340,53</td>
<td>1563,95</td>
<td>1787,37</td>
<td>2010,79</td>
<td>2234,21</td>
<td>2234,21</td>
</tr>
<tr>
<td>Arc 5</td>
<td>1105,94</td>
<td>1327,12</td>
<td>1548,31</td>
<td>1769,50</td>
<td>1990,68</td>
<td>2211,87</td>
<td>2211,87</td>
</tr>
<tr>
<td>Arc 6--Arc 9</td>
<td>1094,76</td>
<td>1313,72</td>
<td>1532,67</td>
<td>1751,62</td>
<td>1970,58</td>
<td>2189,53</td>
<td>2189,53</td>
</tr>
<tr>
<td>Icebreaker 6 - Icebreaker 8</td>
<td>1083,59</td>
<td>1300,31</td>
<td>1517,03</td>
<td>1733,75</td>
<td>1950,47</td>
<td>2167,19</td>
<td>2167,19</td>
</tr>
</tbody>
</table>

**For vessels with a gross tonnage from 5 001 up to 10 000**
### TABLE 3—TARIFFS FOR THE SUMMER-AUTUMN NAVIGATION PERIOD

<table>
<thead>
<tr>
<th>VESSEL'S ICE STRENGTHENING CLASS</th>
<th>PILOTAGE WITHIN 1 ZONE</th>
<th>PILOTAGE WITHIN 2 ZONES</th>
<th>PILOTAGE WITHIN 3 ZONES</th>
<th>PILOTAGE WITHIN 4 ZONES</th>
<th>PILOTAGE WITHIN 5 ZONES</th>
<th>PILOTAGE WITHIN 6 ZONES</th>
<th>PILOTAGE WITHIN 7 ZONES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Her</td>
<td>804.32</td>
<td>965.18</td>
<td>1126.04</td>
<td>1286.91</td>
<td>1447.77</td>
<td>1608.63</td>
<td>1608.63</td>
</tr>
<tr>
<td>Ice 1</td>
<td>563.02</td>
<td>675.63</td>
<td>788.23</td>
<td>900.83</td>
<td>1013.44</td>
<td>1126.04</td>
<td>1126.04</td>
</tr>
<tr>
<td>Ice 2</td>
<td>522.81</td>
<td>627.37</td>
<td>731.93</td>
<td>836.49</td>
<td>941.05</td>
<td>1045.61</td>
<td>1045.61</td>
</tr>
<tr>
<td>Ice 3</td>
<td>482.59</td>
<td>579.11</td>
<td>675.63</td>
<td>772.14</td>
<td>868.66</td>
<td>965.18</td>
<td>965.18</td>
</tr>
<tr>
<td>Arc 4</td>
<td>402.16</td>
<td>482.59</td>
<td>563.02</td>
<td>643.45</td>
<td>723.88</td>
<td>804.32</td>
<td>804.32</td>
</tr>
<tr>
<td>Arc 5</td>
<td>398.14</td>
<td>477.76</td>
<td>557.39</td>
<td>637.02</td>
<td>716.65</td>
<td>796.27</td>
<td>796.27</td>
</tr>
<tr>
<td>Arc 6–Arc 9</td>
<td>394.12</td>
<td>472.94</td>
<td>551.76</td>
<td>630.58</td>
<td>709.41</td>
<td>788.23</td>
<td>788.23</td>
</tr>
<tr>
<td>VESSEL’S ICE STRENGTHENING CLASS</td>
<td>PILOTAGE WITHIN 1 ZONE</td>
<td>PILOTAGE WITHIN 2 ZONES</td>
<td>PILOTAGE WITHIN 3 ZONES</td>
<td>PILOTAGE WITHIN 4 ZONES</td>
<td>PILOTAGE WITHIN 5 ZONES</td>
<td>PILOTAGE WITHIN 6 ZONES</td>
<td>PILOTAGE WITHIN 7 ZONES</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Arc 4</td>
<td>1005,40</td>
<td>1206,47</td>
<td>1407,55</td>
<td>1608,63</td>
<td>1809,71</td>
<td>2010,79</td>
<td>2010,79</td>
</tr>
<tr>
<td>Arc 5</td>
<td>995,34</td>
<td>1194,41</td>
<td>1393,48</td>
<td>1592,55</td>
<td>1791,61</td>
<td>1990,68</td>
<td>1990,68</td>
</tr>
<tr>
<td>Arc 6–Arc 9</td>
<td>985,29</td>
<td>1182,35</td>
<td>1379,40</td>
<td>1576,46</td>
<td>1773,52</td>
<td>1970,58</td>
<td>1970,58</td>
</tr>
<tr>
<td>Icebreaker 6 - Icebreaker 8</td>
<td>975,23</td>
<td>1170,28</td>
<td>1365,33</td>
<td>1560,37</td>
<td>1755,42</td>
<td>1950,47</td>
<td>1950,47</td>
</tr>
</tbody>
</table>
FOR VESSELS WITH A GROSS TONNAGE FROM 10 001 UP TO 20 000

<table>
<thead>
<tr>
<th>VESSEL’S ICE STRENGTHENING CLASS</th>
<th>PILOTAGE WITHIN 1 ZONE</th>
<th>PILOTAGE WITHIN 2 ZONES</th>
<th>PILOTAGE WITHIN 3 ZONES</th>
<th>PILOTAGE WITHIN 4 ZONES</th>
<th>PILOTAGE WITHIN 5 ZONES</th>
<th>PILOTAGE WITHIN 6 ZONES</th>
<th>PILOTAGE WITHIN 7 ZONES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Her</td>
<td>714,95</td>
<td>857,94</td>
<td>1000,93</td>
<td>1143,92</td>
<td>1286,91</td>
<td>1429,90</td>
<td>1429,90</td>
</tr>
<tr>
<td>Ice 1</td>
<td>500,46</td>
<td>600,56</td>
<td>700,65</td>
<td>800,74</td>
<td>900,83</td>
<td>1000,93</td>
<td>1000,93</td>
</tr>
<tr>
<td>Ice 2</td>
<td>464,72</td>
<td>557,66</td>
<td>650,60</td>
<td>743,55</td>
<td>836,49</td>
<td>929,43</td>
<td>929,43</td>
</tr>
<tr>
<td>Ice 3</td>
<td>428,97</td>
<td>514,76</td>
<td>600,56</td>
<td>686,35</td>
<td>772,14</td>
<td>857,94</td>
<td>857,94</td>
</tr>
<tr>
<td>Arc 4</td>
<td>357,47</td>
<td>428,97</td>
<td>500,46</td>
<td>571,96</td>
<td>643,45</td>
<td>714,95</td>
<td>714,95</td>
</tr>
<tr>
<td>Arc 5</td>
<td>353,90</td>
<td>424,68</td>
<td>495,46</td>
<td>566,24</td>
<td>637,02</td>
<td>707,80</td>
<td>707,80</td>
</tr>
<tr>
<td>Arc 6–Arc 9</td>
<td>350,32</td>
<td>420,39</td>
<td>490,45</td>
<td>560,52</td>
<td>630,58</td>
<td>700,65</td>
<td>700,65</td>
</tr>
</tbody>
</table>
### TABLE 6—TARIFFS FOR THE WINTER-SPRING NAVIGATION PERIOD

<table>
<thead>
<tr>
<th>VESSEL’S ICE STRENGTHENING CLASS</th>
<th>PILOTAGE WITHIN 1 ZONE</th>
<th>PILOTAGE WITHIN 2 ZONES</th>
<th>PILOTAGE WITHIN 3 ZONES</th>
<th>PILOTAGE WITHIN 4 ZONES</th>
<th>PILOTAGE WITHIN 5 ZONES</th>
<th>PILOTAGE WITHIN 6 ZONES</th>
<th>PILOTAGE WITHIN 7 ZONES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arc 4</td>
<td>893,68</td>
<td>1072,42</td>
<td>1251,16</td>
<td>1429,90</td>
<td>1608,63</td>
<td>1787,37</td>
<td>1787,37</td>
</tr>
<tr>
<td>Arc 5</td>
<td>884,75</td>
<td>1061,70</td>
<td>1238,65</td>
<td>1415,60</td>
<td>1592,55</td>
<td>1769,50</td>
<td>1769,50</td>
</tr>
<tr>
<td>Arc 6—Arc 9</td>
<td>875,81</td>
<td>1050,97</td>
<td>1226,14</td>
<td>1401,30</td>
<td>1576,46</td>
<td>1751,62</td>
<td>1751,62</td>
</tr>
<tr>
<td>Icebreaker 6—Icebreaker 8</td>
<td>866,87</td>
<td>1040,25</td>
<td>1213,62</td>
<td>1387,00</td>
<td>1560,37</td>
<td>1733,75</td>
<td>1733,75</td>
</tr>
<tr>
<td>VESSEL’S ICE STRENGTHENING CLASS</td>
<td>PILOTAGE WITHIN 1 ZONE</td>
<td>PILOTAGE WITHIN 2 ZONES</td>
<td>PILOTAGE WITHIN 3 ZONES</td>
<td>PILOTAGE WITHIN 4 ZONES</td>
<td>PILOTAGE WITHIN 5 ZONES</td>
<td>PILOTAGE WITHIN 6 ZONES</td>
<td>PILOTAGE WITHIN 7 ZONES</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Her</td>
<td>536,21</td>
<td>643,45</td>
<td>750,70</td>
<td>857,94</td>
<td>965,18</td>
<td>1072,42</td>
<td>1072,42</td>
</tr>
<tr>
<td>Ice 1</td>
<td>375,35</td>
<td>450,42</td>
<td>525,49</td>
<td>600,56</td>
<td>675,63</td>
<td>750,70</td>
<td>750,70</td>
</tr>
<tr>
<td>Ice 2</td>
<td>348,54</td>
<td>418,24</td>
<td>487,95</td>
<td>557,66</td>
<td>627,37</td>
<td>697,07</td>
<td>697,07</td>
</tr>
<tr>
<td>Ice 3</td>
<td>321,73</td>
<td>386,07</td>
<td>450,42</td>
<td>514,76</td>
<td>579,11</td>
<td>643,45</td>
<td>643,45</td>
</tr>
<tr>
<td>Arc 4</td>
<td>268,11</td>
<td>321,73</td>
<td>375,35</td>
<td>428,97</td>
<td>482,59</td>
<td>536,21</td>
<td>536,21</td>
</tr>
<tr>
<td>Arc 5</td>
<td>265,42</td>
<td>318,51</td>
<td>371,59</td>
<td>424,68</td>
<td>477,76</td>
<td>530,85</td>
<td>530,85</td>
</tr>
<tr>
<td>Arc 6--Arc 9</td>
<td>262,74</td>
<td>315,29</td>
<td>367,84</td>
<td>420,39</td>
<td>472,94</td>
<td>525,49</td>
<td>525,49</td>
</tr>
</tbody>
</table>
### TABLE 8--TARIFFS FOR THE WINTER-SPRING NAVIGATION PERIOD

<table>
<thead>
<tr>
<th>VESSEL'S ICE STRENGTHENING CLASS</th>
<th>PILOTAGE WITHIN 1 ZONE</th>
<th>PILOTAGE WITHIN 2 ZONES</th>
<th>PILOTAGE WITHIN 3 ZONES</th>
<th>PILOTAGE WITHIN 4 ZONES</th>
<th>PILOTAGE WITHIN 5 ZONES</th>
<th>PILOTAGE WITHIN 6 ZONES</th>
<th>PILOTAGE WITHIN 7 ZONES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arc 4</td>
<td>670,26</td>
<td>804,32</td>
<td>938,37</td>
<td>1072,42</td>
<td>1206,47</td>
<td>1340,53</td>
<td>1340,53</td>
</tr>
<tr>
<td>Arc 5</td>
<td>663,56</td>
<td>796,27</td>
<td>928,99</td>
<td>1061,70</td>
<td>1194,41</td>
<td>1327,12</td>
<td>1327,12</td>
</tr>
<tr>
<td>Arc 6--Arc 9</td>
<td>656,86</td>
<td>788,23</td>
<td>919,60</td>
<td>1050,97</td>
<td>1182,35</td>
<td>1313,72</td>
<td>1313,72</td>
</tr>
<tr>
<td>Icebreaker 6--Icebreaker 8</td>
<td>650,16</td>
<td>780,19</td>
<td>910,22</td>
<td>1040,25</td>
<td>1170,28</td>
<td>1300,31</td>
<td>1300,31</td>
</tr>
</tbody>
</table>

For vessels with a gross tonnage from 40 001 up to 100 000
<table>
<thead>
<tr>
<th>VESSEL'S ICE STRENGTHENING CLASS</th>
<th>PILOTAGE WITHIN 1 ZONE</th>
<th>PILOTAGE WITHIN 2 ZONES</th>
<th>PILOTAGE WITHIN 3 ZONES</th>
<th>PILOTAGE WITHIN 4 ZONES</th>
<th>PILOTAGE WITHIN 5 ZONES</th>
<th>PILOTAGE WITHIN 6 ZONES</th>
<th>PILOTAGE WITHIN 7 ZONES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Her</td>
<td>446.84</td>
<td>536.21</td>
<td>625.58</td>
<td>714.95</td>
<td>804.32</td>
<td>893.68</td>
<td>893.68</td>
</tr>
<tr>
<td>Ice 1</td>
<td>312.79</td>
<td>375.35</td>
<td>437.91</td>
<td>500.46</td>
<td>563.02</td>
<td>625.58</td>
<td>625.58</td>
</tr>
<tr>
<td>Ice 2</td>
<td>290.45</td>
<td>348.54</td>
<td>406.63</td>
<td>464.72</td>
<td>522.81</td>
<td>580.90</td>
<td>580.90</td>
</tr>
<tr>
<td>Ice 3</td>
<td>268.11</td>
<td>321.73</td>
<td>375.35</td>
<td>428.97</td>
<td>482.59</td>
<td>536.21</td>
<td>536.21</td>
</tr>
<tr>
<td>Arc 4</td>
<td>223.42</td>
<td>268.11</td>
<td>312.79</td>
<td>357.47</td>
<td>402.16</td>
<td>446.84</td>
<td>446.84</td>
</tr>
<tr>
<td>Arc 5</td>
<td>221.19</td>
<td>265.42</td>
<td>309.66</td>
<td>353.90</td>
<td>398.14</td>
<td>442.37</td>
<td>442.37</td>
</tr>
<tr>
<td>Arc 6--Arc 9</td>
<td>218.95</td>
<td>262.74</td>
<td>306.53</td>
<td>350.32</td>
<td>394.12</td>
<td>437.91</td>
<td>437.91</td>
</tr>
<tr>
<td>VESSEL'S ICE STRENGTHENING CLASS</td>
<td>TARIFF RATE IN RUSSIAN RUBLES PER UNIT OF VESSEL'S GROSS TONNAGE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PILOTAGE WITHIN 1 ZONE</td>
<td>PILOTAGE WITHIN 2 ZONES</td>
<td>PILOTAGE WITHIN 3 ZONES</td>
<td>PILOTAGE WITHIN 4 ZONES</td>
<td>PILOTAGE WITHIN 5 ZONES</td>
<td>PILOTAGE WITHIN 6 ZONES</td>
<td>PILOTAGE WITHIN 7 ZONES</td>
</tr>
<tr>
<td>Arc 4</td>
<td>558,55</td>
<td>670,26</td>
<td>781,97</td>
<td>893,68</td>
<td>1005,40</td>
<td>1117,11</td>
<td>1117,11</td>
</tr>
<tr>
<td>Arc 5</td>
<td>552,97</td>
<td>663,56</td>
<td>774,15</td>
<td>884,75</td>
<td>995,34</td>
<td>1105,94</td>
<td>1105,94</td>
</tr>
<tr>
<td>Arc 6–Arc 9</td>
<td>547,38</td>
<td>656,86</td>
<td>766,33</td>
<td>875,81</td>
<td>985,29</td>
<td>1094,76</td>
<td>1094,76</td>
</tr>
<tr>
<td>Icebreaker 6–Icebreaker 8</td>
<td>541,80</td>
<td>650,16</td>
<td>758,52</td>
<td>866,87</td>
<td>975,23</td>
<td>1083,59</td>
<td>1083,59</td>
</tr>
</tbody>
</table>

For vessels with a gross tonnage more than 100 000
## TABLE 11--TARIFFS FOR THE SUMMER-AUTUMN NAVIGATION PERIOD

<table>
<thead>
<tr>
<th>VESSEL’S ICE STRENGTHENING CLASS</th>
<th>PILOTAGE WITHIN 1 ZONE</th>
<th>PILOTAGE WITHIN 2 ZONES</th>
<th>PILOTAGE WITHIN 3 ZONES</th>
<th>PILOTAGE WITHIN 4 ZONES</th>
<th>PILOTAGE WITHIN 5 ZONES</th>
<th>PILOTAGE WITHIN 6 ZONES</th>
<th>PILOTAGE WITHIN 7 ZONES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Her</td>
<td>268.11</td>
<td>321.73</td>
<td>375.35</td>
<td>428.97</td>
<td>482.59</td>
<td>536.21</td>
<td>536.21</td>
</tr>
<tr>
<td>Ice 1</td>
<td>187.67</td>
<td>225.21</td>
<td>262.74</td>
<td>300.28</td>
<td>337.81</td>
<td>375.35</td>
<td>375.35</td>
</tr>
<tr>
<td>Ice 2</td>
<td>174.27</td>
<td>209.12</td>
<td>243.98</td>
<td>278.83</td>
<td>313.68</td>
<td>348.54</td>
<td>348.54</td>
</tr>
<tr>
<td>Ice 3</td>
<td>160.86</td>
<td>193.04</td>
<td>225.21</td>
<td>257.38</td>
<td>289.55</td>
<td>321.73</td>
<td>321.73</td>
</tr>
<tr>
<td>Arc 4</td>
<td>134.05</td>
<td>160.86</td>
<td>187.67</td>
<td>214.48</td>
<td>241.29</td>
<td>268.11</td>
<td>268.11</td>
</tr>
<tr>
<td>Arc 5</td>
<td>132.71</td>
<td>159.25</td>
<td>185.80</td>
<td>212.34</td>
<td>238.88</td>
<td>265.42</td>
<td>265.42</td>
</tr>
<tr>
<td>Arc 6--Arc 9</td>
<td>131.37</td>
<td>157.85</td>
<td>183.92</td>
<td>210.19</td>
<td>236.47</td>
<td>262.74</td>
<td>262.74</td>
</tr>
</tbody>
</table>
TABLE 12--TARIFFS FOR THE WINTER-SPRING NAVIGATION PERIOD

<table>
<thead>
<tr>
<th>VESSEL’S ICE STRENGTHENING CLASS</th>
<th>PILOTAGE WITHIN 1 ZONE</th>
<th>PILOTAGE WITHIN 2 ZONES</th>
<th>PILOTAGE WITHIN 3 ZONES</th>
<th>PILOTAGE WITHIN 4 ZONES</th>
<th>PILOTAGE WITHIN 5 ZONES</th>
<th>PILOTAGE WITHIN 6 ZONES</th>
<th>PILOTAGE WITHIN 7 ZONES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arc 4</td>
<td>335,13</td>
<td>402,16</td>
<td>469,18</td>
<td>536,21</td>
<td>603,24</td>
<td>670,26</td>
<td>670,26</td>
</tr>
<tr>
<td>Arc 5</td>
<td>331,78</td>
<td>398,14</td>
<td>464,49</td>
<td>530,85</td>
<td>597,20</td>
<td>663,56</td>
<td>663,56</td>
</tr>
<tr>
<td>Arc 6--Arc 9</td>
<td>328,43</td>
<td>394,12</td>
<td>459,80</td>
<td>525,49</td>
<td>591,17</td>
<td>656,86</td>
<td>656,86</td>
</tr>
<tr>
<td>Icebreaker 6 - Icebreaker 8</td>
<td>325,08</td>
<td>390,09</td>
<td>455,11</td>
<td>520,12</td>
<td>585,14</td>
<td>650,16</td>
<td>650,16</td>
</tr>
</tbody>
</table>

*122 On approval of the tariff rates for provision of icebreaking pilotage services provided by the FSUE #Atomflot# on the Northern Sea Route water area (March 4, 2014), http://www.Arctic-lio.com/docs/nsr/tariffs/NSR_Tariff_Order.pdf.

*123 Appendix E. Northern Canada Vessel Traffic Services Zone Regulations (NORDREG), SOR/2010-127 (Excerpt)
### NORDREG INFORMATION

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESIGNATOR</th>
<th>SUBJECT</th>
<th>INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>A</td>
<td>Vessel</td>
<td>The vessel's name, the name of the state whose flag the vessel is entitled to fly and, if applicable, the vessel's call sign, International Maritime Organization ship identification number and Maritime Mobile Service Identity (MMSI) number.</td>
</tr>
<tr>
<td>2.</td>
<td>B</td>
<td>Date and time corresponding to the vessel's position under designator C or D given in Coordinated Universal Time (UTC)</td>
<td>A 6-digit group followed by a Z, the first 2 digits giving the day of the month, the next two digits giving the hour and the last two digits giving the minutes.</td>
</tr>
<tr>
<td>3.</td>
<td>C</td>
<td>Vessel's position by latitude and longitude</td>
<td>A 4-digit group giving the latitude in degrees and minutes suffixed with N, and a 5-digit group giving the longitude in degrees and minutes suffixed with W.</td>
</tr>
<tr>
<td>4.</td>
<td>D</td>
<td>Vessel's position by geographical name of place</td>
<td>If the vessel is at a known place, the name of the place. If the vessel is not at a known place, the name of a known place followed by the vessel's true bearing (3-digits) and distance in nautical miles from the place.</td>
</tr>
<tr>
<td>5.</td>
<td>E</td>
<td>Vessel's course</td>
<td>The true course. A 3-digit group.</td>
</tr>
<tr>
<td>6.</td>
<td>F</td>
<td>Vessel's speed</td>
<td>The speed in knots. A 2-digit group.</td>
</tr>
<tr>
<td>7.</td>
<td>G</td>
<td>Vessel's last port of call</td>
<td>The name of the port of call.</td>
</tr>
<tr>
<td>8.</td>
<td>H</td>
<td>Vessel's entry into the NORDREG Zone or departure from a berth within the NORDREG Zone</td>
<td>The estimated date and time that the vessel will enter the NORDREG Zone or depart the berth within the NORDREG Zone, as appropriate, with the date and time expressed as for designator B and the entry or departure position expressed as for designator C or D.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>ARTICLE 234 OF THE UNITED NATIONS CONVENTION...</strong>, 7 Harv. Nat'l Sec. J. 55</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>I</td>
<td><strong>Vessel's destination and expected time of arrival</strong></td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td>K</td>
<td><strong>Vessel's exit from the NORDREG Zone or arrival at the vessel's destination.</strong></td>
<td></td>
</tr>
<tr>
<td>11.</td>
<td>L</td>
<td><strong>Vessel's intended route</strong></td>
<td></td>
</tr>
<tr>
<td>12.</td>
<td>O</td>
<td><strong>Vessel's maximum present static draught</strong></td>
<td></td>
</tr>
<tr>
<td>13.</td>
<td>P</td>
<td><strong>Vessel's cargo</strong></td>
<td></td>
</tr>
<tr>
<td>14.</td>
<td>Q</td>
<td><strong>Defects, damage and deficiencies, as well as circumstances adversely affecting the vessel's normal navigation</strong></td>
<td></td>
</tr>
<tr>
<td>15.</td>
<td>S</td>
<td><strong>Weather and ice</strong></td>
<td></td>
</tr>
<tr>
<td>16.</td>
<td>T</td>
<td><strong>Vessel's authorized representative, agent or owner</strong></td>
<td></td>
</tr>
<tr>
<td>17.</td>
<td>W</td>
<td><strong>Persons on board the vessel</strong></td>
<td></td>
</tr>
<tr>
<td>18.</td>
<td>X</td>
<td><strong>(a) In the case of a sailing plan report,</strong></td>
<td></td>
</tr>
</tbody>
</table>

- (i) the amount of oil on board that is for use as fuel or carried as cargo;  
- (ii) if the vessel's owner or master holds an arctic pollution prevention certificate in respect of the vessel, the certificate;  

- (a) The following information:  
  - (i) the total amount of oil, expressed in cubic metres;  
  - (ii) the certificate's expiry date and the name of its issuing authority;
(iii) the vessel's ice class, if applicable; and

(iii) the vessel's ice class and the name of the classification society that assigned the ice class; and

(iv) if the report is referred to in paragraph 6(1)(c) of the Regulations, the applicable incident referred to in that paragraph.

(iv) a brief description of the applicable incident.

(b) In the case of a position report referred to in subsection 7(2) of the Regulations, the applicable matter referred to in that subsection.

(b) A brief description of the applicable matter.


Footnotes

a1 Lieutenant Commander, Judge Advocate, United States Coast Guard. Presently assigned as the Advanced Operational Law Fellow at The Judge Advocate General's Legal Center and School, Center for Law and Military Operations, United States Army, Charlottesville, Virginia. LL.M., 2015. The Judge Advocate General's Legal Center and School, United States Army, Charlottesville, Virginia. J.D., 2004, University of New Mexico; M.S., 2001, Eastern New Mexico University; B.S., 1997, Western New Mexico University. Previous military assignments include Staff Attorney, United States Coast Guard District 17, Juneau, Alaska, 2010-2014; Office of Claims and Litigation, Washington, D.C., 2009-2010; Office of Legal and Defense Services, 2007-2009, Arlington, Virginia. Additional legal assignments include Associate Attorney, Baxter Bruce & Sullivan, P.C., Juneau, Alaska, 2006-2007; Assistant Attorney General, Alaska Department of Law, Natural Resources Section, Juneau, Alaska, 2004-2006. Member of the bars of Alaska, the District of Alaska, Court of Appeals for the Armed Forces, and the Supreme Court of the United States. This article was submitted in partial completion of the Master of Laws requirements of the 63d Judge Advocate Officer Graduate Course. Special thanks to David H. Lee, LCDR, JAGC, USN, William G. Dwyer III, CDR, USCG, and The Judge Advocate General's Legal Center and School for their time and effort, without which this article would not have been possible.


3 There are additional examples of U.S. Government reliance on Russia for help in Arctic conditions, such as that the National Science Foundation in recent years has been relegated to seeking charter icebreaking services from Russia and Sweden in order to get to McMurdo Station in Antarctica. RONALD O'ROURKE, CONG. RESEARCH SERV., RL34391, COAST GUARD POLAR ICEBREAKER MODERNIZATION: BACKGROUND AND ISSUES FOR CONGRESS 17 (2014) (“Although Coast Guard polar icebreakers in the past have performed the annual McMurdo break-in mission, the NSF in certain recent years has chartered Russian and Swedish contractor-operated icebreakers to perform the mission ...”).

Ahlers, supra note 4 (“[I]t would have taken more than 300 flights, each carrying 4,000 to 5,000 gallons, to meet the town's needs .... Shipping costs would have added $3 or $4 to the price of a gallon of gasoline, which already approaches $6 a gallon ....”).


Ahlers, supra note 4. It should be noted that USCGC HEALY assisted with the Nome, Alaska, fueling operation by helping to break ice for RENDA. HEALY's deployment was extended by nearly two months to ensure the operation was successful. Id.

Daniel Velez, Arctic Regulations, 70 COAST GUARD PROC., Summer 2013, at 42, 45, n. 2; Ahlers, supra note 4.


See Christina Nunez, What Happens When Oil Spills in the Arctic?, NAT'L GEOGRAPHIC (Apr. 24, 2014), http://news.nationalgeographic.com/news/energy/2014/04/140423-national-research-council-on-oil-spills-in-arctic/; Melissa Bert, A Strategy to Advance the Arctic Economy, COUNCIL ON FOREIGN REL. (2012), http://www.cfr.org/arctic/strategy-advance-arctic-economy/p27528 (“In the lower forty-eight states, response time to an oil spill or capsized vessel is measured in hours. In Alaska, it could take days or weeks to get the people and resources on scene. The nearest major port is in the Aleutian Islands, thirteen hundred miles from Point Barrow, and response aircraft are more than one thousand miles south in Kodiak, blocked by a mountain range and hazardous flying conditions. The Arctic shores lack infrastructure to launch any type of disaster response, or to support the growing commercial development in the region.”)).


Pedrozo, supra note 14, at 768-69; Diplomatic Note from the U.S. Embassy, Ottawa, Can., to Dep't of Foreign Affairs andIntl Trade of Canada, Appendix A (Aug. 18, 2010) (hereinafter Diplomatic Note from the United States to Canada),


U.S. CONST. pmbl. (“We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America.”); THE DECLARATION OF INDEPENDENCE para. 2 (U.S. 1776) (“We hold these truths to be selfevident, that all men ... are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness. That to secure these rights, Governments are instituted among Men ....”); CREED OF THE UNITED STATES COAST GUARDSMAN, http://www.uscg.mil/hq/cg3/cg3pcx/corevalues.asp (“I shall sell life dearly to an enemy of my country, but give it freely to rescue those in peril.”).


Nunez, supra note 11; UNITED STATES COAST GUARD, ARCTIC STRATEGY, supra note 10, at 14-16; Bert, supra note 11 (“In Alaska, it could take days or weeks to get the right people and resources on scene. The nearest major port is in the Aleutian Islands, thirteen hundred miles from Point Barrow, and response aircraft are more than one thousand miles south in Kodiak, blocked by a mountain range and hazardous flying conditions. The Arctic shores lack infrastructure to launch any type of disaster response, or to support the growing commercial development in the region.”); Jerry Bellinson, What if a Cruise Ship Wrecked in Alaska?, POPULAR MECHANICS (Jan. 25, 2012), http://www.popularmechanics.com/technology/engineering/extreme-machines/what-if-a-cruise-ship-wrecked-in-alaska-6645471. See also THE PEW ENV’T GROUP, POLICY RECOMMENDATIONS: OIL SPILL PREVENTION AND RESPONSE IN THE U.S. ARCTIC OCEAN 12-13 (2010), http://www.arctic-report.net/wp-content/uploads/2012/02/PEW-Oil-Spill-Prevention-and-Response-in-the-US-Arctic-Ocean.pdf.

Adam Shaw, The Big Chill, 70 COAST GUARD PROCEEDINGS 2:26 (2013), http://www.uscg.mil/proceedings/archive/2013/Vol70_No2_Sum2013.pdf. See generally UNITED STATES COAST GUARD, ARCTIC STRATEGY, supra note 10, at 20-21; Bert, supra note 11 (“In Alaska, it could take days or weeks to get the right people and resources on scene. The nearest major port is in the Aleutian Islands, thirteen hundred miles from Point Barrow, and response aircraft are more than one thousand miles south in Kodiak, blocked by a mountain range and hazardous flying conditions. The Arctic shores lack infrastructure to launch any type of disaster response, or to support the growing commercial development in the region.”).

See Beilinson, supra note 20; Bert, supra note 11 (“In the lower forty-eight states, response time to an oil spill or capsized vessel is measured in hours. In Alaska, it could take days or weeks to get the right people and resources on scene. The nearest major port is in the Aleutian Islands, thirteen hundred miles from Point Barrow, and response aircraft are more than one thousand miles south in Kodiak, blocked by a mountain range and hazardous flying conditions. The Arctic shores lack infrastructure to launch any type of disaster response, or to support the growing commercial development in the region.”).


“Multi-year” ice exists through multiple years and is typically much harder than “first-year” ice that has frozen within the previous year. NAT’L SNOW AND ICE DATA CENTER, MULTIYEAR ICE, http://nsidc.org/cryosphere/seaice/
characteristics/multiyear.html; Peter Wadhams, ARCTIC THEME PAGE, NAT'L OCEANIC AND ATMOSPHERIC ADMIN., HOW DOES ARCTIC SEA ICE FORM AND DECAY? (Jan. 1, 2003), http://www.arctic.noaa.gov/essay_wadhams.html.

See Byers and Lalonde, supra note 10, at 1141-46 (forecasting increased vessel traffic due to less ice and shorter shipping distances that allow for more shipping traffic, adventure cruises, natural resource activities, etc.); UNITED STATES COAST GUARD, ARCTIC STRATEGY, supra note 10, at 5, 7; Keil, supra note 10; Insinna, supra note 10 (forecasting that decreased ice will increase vessel traffic and thus allow for more activity related to fishing, tourism, natural resource extraction, etc.); Michels, supra note 10, at 2.


ARCTIC VESSEL ACTIVITY SUMMARY DATA, supra note 26 (explaining that in 2014 heavy ice conditions on NSR into mid-August, economics, China's efforts to develop alternate land, and economic sanctions negatively impacted the use of the NSR); NORTHERN SEA ROUTE INFO. OFFICE, supra note 27.

ARCTIC VESSEL ACTIVITY SUMMARY DATA, supra note 26.

Id.


Oil and Gas Lease Sale 242, Alaska OCS Region, Beaufort Sea Planning Area, 78 Fed. Reg. 59715-18 (proposed Sep. 12, 2014) (“Since 2005, the federal government has held several OCS lease sales in Alaska, and bonus payments to the federal treasury have exceeded $3 billion for ten-year leases in the Beaufort and Chukchi Seas.” “While approximately 700 leases netting the federal government billions of dollars have been awarded to companies interested in oil and gas exploration in federal waters offshore Alaska since 2005, federal regulatory obstacles have helped preclude the drilling of even one well to hydrocarbon depth.”); Sue E. Moore et al., A New Framework for Assessing the Effects of Anthropogenic Sound on Marine Mammals in a Rapidly Changing Arctic, 62 BIONSCIENCE 289, 289 (Mar. 2012), http://ocr.org/pdfs/papers/2012_new_arctic_noise_assmt_fnwk_biosc.pdf (“In 2008, oil companies paid a record $2.6 billion for leases in the Alaskan Chukchi Sea.”); Bert, supra note 11 (“In 2008, the United States collected $2.6 billion from offshore lease sales in the Beaufort and Chukchi Seas (off Alaska's north coast), and the royalty tax rate in the region is 19 percent, which would cover operation and maintenance of [a deepwater port and military airbase] facilities down the road.”); U.S. DEPT OF THE INTERIOR, MINERALS MGMT. SERV. ALASKA OCS REGION, FINAL BID RECAP, (2008), http://www.boem.gov/uploadedFiles/BOEM/About_BOEM/BOEM_Regions/
The Federal Government has failed to produce any legitimate plan for implementing safety and security in the U.S. Arctic. Instead, it simply provides very general guidance, omits any specific plans, and omits funding any of the additional general guidance provided. See, e.g., WHITE HOUSE ARCTIC STRATEGY, supra note 16, at 6 (“The United States will endeavor to appropriately enhance sea, air, and space capabilities as Arctic conditions change, and to promote maritime-related information sharing with international, public, and private sector partners, to support implementation of activities such as the search-and-rescue agreement signed by Arctic states.”).


See generally supra notes 14-15.

United Nations Convention on the Law of the Sea Art. 236, Dec. 10, 1982, 1833 U.N.T.S. 397 (“The provisions of this Convention regarding the protection and preservation of the marine environment do not apply to any warship, naval auxiliary, other vessels or aircraft owned or operated by a State and used, for the time being, only on government noncommercial service.”), http://www.un.org/depts/los/convention_agreements/texts/unclos/closindx.htm; see also Pedrozo, supra note 14, at 770-71.

46 U.S.C. § 6101(a) (2015) defines marine casualties that require mandatory reporting as “(1) death of an individual. (2) serious injury to an individual. (3) material loss of property. (4) material damage affecting the seaworthiness or efficiency of the vessel. (5) significant harm to the environment.”; 46 C.F.R. § 4.03-1(b) (2015) defines “marine casualty or accident” as any “events caused by or involving a vessel and includes, but is not limited to, the following: (1) Any fall overboard, injury, or loss of life of any person. (2) Any occurrence involving a vessel that results in—(i) Grounding; (ii) Stranding; (iii) Foundering; (iv) Flooding; (v) Collision; (vi) Allision; (vii) Explosion; (viii) Fire; (ix) Reduction or loss of a vessel's electrical power, propulsion, or steering capabilities; (x) Failures or occurrences, regardless of cause, which impair any aspect of a vessel's operation, components, or cargo; (xi) Any other circumstance that might affect or impair a vessel's seaworthiness, efficiency, or fitness for service or route; or (xii) Any incident involving significant harm to the environment.”

Letter from Rebecca J. Lent, supra note 23, at 1, 5, 8; NICHOLAS CUNNINGHAM, OFFSHORE OIL DRILLING IN THE ARCTIC 9 (2012), https://www.americansecurityproject.org/ASP%20Reports/Ref%200076%20-%20Offshore%20Oil%20Drilling%20in%20the%20Arctic.pdf.

See Nunez, supra note 11; UNITED STATES COAST GUARD, ARCTIC STRATEGY, supra note 10, at 14-16; Bert, supra note 11; Beilinson, supra note 20; see also THE PEW ENV'T. GROUP, supra note 20, at 12-13.


Kraska, supra note 19, at 1116 (Describing “a new ‘cold war’ developing between Russia and Canada. Disputes over competing claims to the continental shelf of the North Pole have unnecessarily ignited a contest of words and wills featuring Moscow and Ottawa as the principle antagonists.” (citing Randy Boswell, Canada, Russia Play Political Game in Arctic: Experts, NAT'L POST (Toronto), (Aug. 16, 2009)).
WHITE HOUSE ARCTIC STRATEGY, supra note 16, at 10 (“While the United States is not currently a party to the Convention, we will continue to support and observe principles of established customary international law reflected in the Convention.”);

UNITED STATES COAST GUARD, ARCTIC STRATEGY, supra note 10, at 14 (“The United States is not a party to the Convention, but accepts and acts in accordance with the provisions of the Convention relating to traditional uses of the oceans—such as navigation and overflight—as reflective of customary international law and practice.”).


As per the U.S. Department of State, “[t]he Arctic Council is the preeminent intergovernmental forum for addressing issues related to the Arctic Region. The members of the Arctic Council include the eight countries with territory above the Arctic Circle (Canada, Denmark, Finland, Iceland, Norway, Sweden, the Russian Federation, and the United States).” U.S. DEPT. OF STATE, http://www.state.gov/e/oes/ocns/opa/arc/ac/.

Koren, supra note 1.

See Discussion supra, at Sections I.A. and II.A.

See ALASKA ESKIMO WHALING COMM’N, supra note 23; Byers and Lalonde, supra note 10, at 1178-79.

See Michael Byers, Canada's Arctic Nightmare Just Came True: The Northwest Passage is Commercial, THE GLOBE AND MAIL (Sept. 20, 2013), http://www.theglobeandmail.com/globe-debate/canadas-Arctic-nightmare-just-came-true-the-northwest-passage-is-commercial/article14432440/ (crashed Canadian Coast Guard helicopter results in death of crew and sinking of aircraft because icebreaker is unable to respond quickly enough); Bert, supra note 11 (“In the lower forty-eight states, response time to an oil spill or capsized vessel is measured in hours. In Alaska, it could take days or weeks to get the right people and resources on scene. The nearest major port is in the Aleutian Islands, thirteen hundred miles from Point Barrow, and response aircraft are more than one thousand miles south in Kodiak, blocked by a mountain range and hazardous flying conditions. The Arctic shores lack infrastructure to launch any type of disaster response, or to support the growing commercial development in the region.”).

Letter from Rebecca J. Lent, supra note 23, at 8.


ARTICLE 234 OF THE UNITED NATIONS CONVENTION..., 7 Harv. Nat'l Sec. J. 55

55 BONDAREFF AND ELLIS, supra note 31, at 5, 7 ("The U.S. is not prepared to protect its interests in the Arctic over the next decade .... The U.S.'s strategic and economic interests in the Arctic are too great for the nation to continue to fail to come to grips with both the legal and operational requirements of protecting those interests, and we will have squandered our opportunity to do so if Congress and the Administration do not act soon."); Beilinson, supra note 20; Bert, supra note 11 ("In the lower forty-eight states, response time to an oil spill or capsized vessel is measured in hours. In Alaska, it could take days or weeks to get the right people and resources on scene. The nearest major port is in the Aleutian Islands, thirteen hundred miles from Point Barrow, and response aircraft are more than one thousand miles south in Kodiak, blocked by a mountain range and hazardous flying conditions. The Arctic shores lack infrastructure to launch any type of disaster response, or to support the growing commercial development in the region."); see also UNITED STATES COAST GUARD, ARCTIC STRATEGY, supra note 10, at 13-14; Kraska, supra note 52, at 279 ("In order to maintain security in the Arctic, the Coast Guard is grossly under-resourced. Coast Guard force structure is insufficient to confront all of the tasks in its portfolio. Lawmakers should expand the Coast Guard, and in particular build a feet of icebreakers and ice-strengthened patrol craft.").

56 Sec. e.g., Yereth Rosen, Icebreaker Fleet Will Need Makeover by About 2020, Coast Guard Says, ALASKA DISPATCH NEWS (Sept. 18, 2014), http://www.military.com/dailynews/2014/09/18/icebreaker-fleet-will-need-makeover-by-about-2020-coast-guards.html?ESRC=coastguard.nl ("The U.S. icebreaker fleet is meager compared to those in other Arctic countries ... said [RADM Daniel Abel, Commander, U.S. Coast Guard Seventeenth District, which includes all of Alaska and the U.S. Arctic]. Russia has 37 icebreakers, Sweden and Finland each have seven and Canada has six and is acquiring a seventh, he said."); Bert, supra note 11 ("The U.S. government is further hindered by the lack of ships, aircraft, and infrastructure to enforce sovereignty, criminal laws, and to protect people and the marine environment from catastrophic incidents."); Duignan, supra note 4, at 57-59; Ahlers, supra note 4.

57 Primary Duties (U.S. Coast Guard), 14 U.S.C. § 2 (2014) ("The Coast Guard shall ... develop, establish, maintain, and operate, with due regard to the requirements of national defense ... icebreaking facilities, and rescue facilities.") (emphasis added); Coordination and review of budget requests; Office of Science and Technology Policy; Office of Management and Budget, 15 U.S.C. § 4109(b)(2) (2014) ("The Office of Management and Budget shall seek to facilitate planning for the design, procurement, maintenance, deployment, and operations of icebreakers needed to provide a platform for Arctic research by allocating all funds necessary to support icebreaking operations, except for recurring incremental costs associated with specific projects, to the Coast Guard.") (emphasis added); Federal agency cooperation, 16 U.S.C. § 2441(c) (2014) ("Icebreaking. The Department of Homeland Security shall facilitate planning for the design, procurement, maintenance, deployment, and operation of icebreakers needed to provide a platform for Antarctic research. All funds necessary to support icebreaking operations, except for recurring incremental costs associated with specific projects, shall be allocated to the United States Coast Guard.") (emphasis added); Revised Memorandum of Agreement Between the Department of the Navy and the Department of the Treasury on the Operation of Icebreakers (July 22, 1965), https://www.uscg.mil/history/docs/1965IcebreakerMOUUSCGUSN.pdf ("The U.S. Coast Guard will maintain and operate all U.S. icebreakers.") (emphasis added).


59 See e.g., Bondareef and Ellis, supra note 31, at 6-7; O'Rourke, supra note 3, at 14-15; Todaro, supra note 31; Munnell, supra note 31; Taddeh, supra note 31; Magnuson, supra note 31; WHITE HOUSE ARCTIC STRATEGY, supra note 16.


Interestingly, the U.S. Navy may find funding from outside its own budget to construct the replacement submarines (SSBN-X) for the current Ohio-class ballistic missile submarines. The National Defense Authorization Act of 2015 created a National Sea Based Deterrence Fund that will allow unspent funds to be redirected to this account for the acquisition of vessels
carrying operational intercontinental ballistic missiles. The premise is that the new class of ballistic missile submarines will be national assets that simply happen to be in the care of the U.S. Navy, and that the cost of building the replacement class of submarines should not be taken from the Navy’s shipbuilding budget because it would “rob” the Navy of its ability to build other ships. Notwithstanding that it is unlikely an icebreaker will be armed with intercontinental ballistic missiles, the basic factors used to provide funding from outside the Navy’s budget would be applicable to the construction of an icebreaker as well. Given that the U.S. Navy, U.S. Coast Guard, and National Science Foundation are all on record indicating that they need additional icebreakers for national missions, these multi-mission platforms can easily fit the description of a national asset that simply happen to be in the care of the Coast Guard. At $1 billion per icebreaker, the funding for acquisition of a new icebreaker should also not come from the Coast Guard’s $1 billion acquisition budget because it would swallow the service’s entire acquisition budget, effectively preventing the Coast Guard from constructing any other ships. See Hugh Lessig, Funding New Submarines Outside the Navy?, DAILY PRESS (Jan. 11, 2015), http://www.dailypress.com/news/military/dp-nws-boomer-budget-20150111-story.html#page=1; Carl Levin and Howard P. “Buck” McKeon, National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, § 1022 (2014); U.S. COAST GUARD, U.S. COAST GUARD FACT SHEET, FISCAL YEAR 2015 PRESIDENT'S BUDGET (Mar. 7, 2014), http://www.uscg.mil/budget/docs/FY2015_Budget_Fact_Sheet.pdf.

62 The Exclusive Economic Zone is defined as “an area beyond and adjacent to the territorial sea, subject to the specific legal regime established in this Part, under which the rights and jurisdiction of the coastal State and the rights and freedoms of other States are governed by the relevant provisions of this Convention.” United Nations Convention on the Law of the Sea Art. 55, Dec. 10, 1982, 1833 U.N.T.S. 397. It is further defined as an area that “shall not extend beyond 200 nautical miles from the baselines from which the breadth of the territorial sea is measured.” Id. Art. 57. “[S]ubject to the relevant provisions of [UNCLOS],” freedom of navigation in the EEZ is secured to all nations. Id. Art. 58.

63 The term “within the limits of the exclusive economic zone” has been the object of a great amount of review and commentary due to the possibility of different, reasonable interpretations. The prevailing view is based on the premise that it would be nonsensical for Article 234 to grant a coastal state greater authority with regard to its EEZ than its territorial seas. Accordingly, in the limited context of Article 234, it is most logical to interpret the term “within the limits of the exclusive economic zone” to include all waters landward of the outer limit of the EEZ. See Bartenstein, supra note 14, at 28-30 (citing Donat Pharand, The Arctic Waters and the Northwest Passage: A Final Revisit, 38 OCEAN DEV. & INT'L L. 47 (2007); R. Douglas Brubaker, Straits of the Russian Arctic, 32 OCEAN DEV. & INT'L L. 263 (2001); NORDQUIST ET AL., supra note 14, at 396 (“[C]oastal States may enact their own rules and regulations applicable within the limits of the exclusive economic zone. They remain bound by international rules and standards as a minimum, but may impose more stringent requirements unilaterally.”); Leonard Legault, Protecting the Marine Environment, in CANADA AND THE NEW INTERNATIONALISM, 99, 107 (John Holmes & John Kirton eds., 1988); Bernard Oxman, Legal Regimes of the Arctic, 40 AMER. SOC. INT'L L. PROC. 315, 333-34 (1988); Donald M. McRae, The Negotiation of Article 234, in POLITICS OF THE NORTHWEST PASSAGE, 98, 108-09 (F. Griffiths ed., 1987); Donald M. McRae & D. J. Goundrey, Environmental Jurisdiction in Arctic Waters: The Extent of Article 234, 16 U. B.C. L. REV. 197, 221 (1982); see also BRUBAKER, supra note 14, at 56-58.


66 Id. Art. 24.
ARTICLE 234 OF THE UNITED NATIONS CONVENTION..., 7 Harv. Nat'l Sec. J. 55

Id. Art. 38 ("Transit passage means ... freedom of navigation and overflight solely for the purpose of continuous and expeditious transit of the strait between one part of the high seas or an exclusive economic zone and another part of the high seas or an exclusive economic zone.").

See Donald McRae, Arctic Sovereignty? What is at Stake?, 64 BEHIND THE HEADLINES 1, 18 (2007); BRUBAKER, supra note 14, at 134-36.

D. Ginsberg & Sons, Inc. v. Popkin, 285 U.S. 204, 208 (1932) (citing Kepner v. United States, 195 U.S. 100, 125 (1904); United States v. Chase, 135 U.S. 255, 260 (1890); In re Hassenbusch, 108 F. 35, 38 (6th Cir. 1901); United States v. Peters, 166 F. 613, 615 (E.D. Ill. 1909)).


BRUBAKER, supra note 14, at 136; see, e.g., NAVIGATING THE NORTHERN SEA ROUTE ADVISORY, supra note 58; Rob Huebert, Article 234 and Marine Pollution in the Arctic, in THE LAW OF THE SEA AND POLAR MARITIME DELIMITATION AND JURISDICTION 249, 263 (Alex Elferink & Donald Rothwell eds., 2001).

See BRUBAKER, supra note 14, at 105, 136; see also NORDQUIST ET AL., supra note 14, at 398.

See BRUBAKER, supra note 14, at 53, 61-65, 109 (providing a review of apparent contradictions between U.S. legislation and official U.S. declarations); see also supra note 71.

See Diplomatic Note from the Embassy of the United States of America to the Department of Foreign Affairs and International Trade of Canada, supra note 15, Appendix A; Letter from Eric Benjaminson, supra note 15, Appendix B; but cf. Moore, supra note 14, at 22-23 ("[Canada] now had the ability to set environmental standards uniquely for all commercial vessels going through those ice-covered areas, and, yes, there was an important obligation to protect navigation, and we included navigation in it, but obviously this was to be taken along with the power of the coastal State to set vessel source pollution standards for vessels not entitled to sovereign immunity ... This is an extraordinary area of otherwise coastal State control as a result of Article 234."); U.S. DEPT. OF STATE, UNITED STATES RESPONSES TO EXCESSIVE MARITIME CLAIMS, LIMITS IN THE SEAS, NO. 112, 73 n. 114 (1992).

Pedrozo, supra note 14, at 769; Kraska, supra note 52, at 274; see also Diplomatic Note from the United States to Canada, supra note 15, Appendix A; Letter from Eric Benjaminson, supra note 15, Appendix B.

See, e.g., Pedrozo, supra note 14, at 769-70.

"[S]ubject to the relevant provisions of [UNCLOS],” freedom of navigation in the EEZ is secured to all nations. United Nations Convention on the Law of the Sea Art. 58; “Subject to this Convention, ships of all States, whether coastal or land-locked, enjoy the right of innocent passage through the territorial sea.” Id. Art. 17; and “Transit passage means ... freedom of navigation and overflight solely for the purpose of continuous and expeditious transit of the strait between one part of the high seas or an exclusive economic zone and another part of the high seas or an exclusive economic zone.” Id. Art. 38.

See, e.g., id.; see also Diplomatic Note from the United States to Canada, supra note 15, Appendix A; Letter from Eric Benjaminson, supra note 15, Appendix B.

This is an altogether questionable strategy at best given the grave inadequacy of U.S. response capabilities in the Arctic. See Discussion supra, at Sections I.A. and II.A.

David Lauter, Legally Drunk Ship's Captain Fired by Exxon, LOS ANGELES TIMES (Mar. 31, 1989), http://articles.latimes.com/1989-03-31/news/mn-704_1_exxon-valdez (“The National Transportation Safety Board reported Thursday that the captain of the Exxon Valdez was legally drunk when he was tested some 10 hours after his tanker hit a reef last week, causing the worst oil spill in U.S. history.” “Coast Guard Commandant Paul Yost called it 'almost unbelievable' that the Exxon Valdez had legally the right to sail from a 10-mile-wide shipping channel to crash into Bligh Reef. 'This was not a treacherous area,’ he said .... 'your children could drive a tanker through it.'”).

Id.

*Id.*

*See supra* note 36; *see also* McRae, *supra* note 68, at 17-18.


*Id.* Art. 38(2).

*Id.* Art. 34.

*Id.* Art. 34(1).

*Id.* Art. 34(2).

Arctic Waters Pollution Prevention Act, R.S.C. 1985, c. A-12 (Can.); *see also* Canadian Coast Guard, Vessel Traffic Reporting Arctic Canada Traffic Zone (NORDREG) (*last modified* June 24, 2013), http://www.ccg-gcc.gc.ca/eng/MCTS/Vtr_Arctic_Canada ("The Northern Canada Vessel Traffic Services Zone Regulations formally establish the Northern Canada Vessel Traffic Services (NORDREG) Zone and, consistent with international law regarding ice-covered areas, implement the requirements for vessels to report information prior to entering, while operating within and upon exiting Canada's northern waters.").


Bartenstein, *supra* note 14, at 25; FRANCKX, *supra* note 92, at 76 ("And as it turned out, these icebreaker escorts proved not to be without reason! The Manhattan [sic] became stuck in the ice not less than 25 times during these voyages requiring icebreaker assistance to set her free.").


*See* Bartenstein, *supra* note 14, at 26; Byers and Lalonde, *supra* note 10, at 1150.

*See Arctic Waters Pollution Prevention Act, R.S.C. 1985, c. A-12, § 12(1) (Can.).

Northern Canada Vessel Traffic Services Zone Regulations (NORDREG), SOR/2010-127 (Can.), http://laws-lois.justice.gc.ca/eng/regulations/SOR-2010-127/FullText.html#h-3, Appendix E; *see also* Canadian Coast Guard, Vessel Traffic Reporting Arctic Canada Traffic Zone (NORDREG), http://www.ccg-gcc.gc.ca/eng/MCTS/Vtr_Arctic_Canada ("consistent with international law regarding ice-covered areas, implement the requirements for vessels to report information prior to entering, while operating within and upon exiting Canada's northern waters. [I] The Regulations will enhance the safety of vessels, crew and passengers, and will safeguard the unique and fragile Arctic marine environment.")., *see Appendix C; It should also be noted that Canada has historically claimed other bases for exercising jurisdiction over Arctic waters, but due to the substantive limitations of this article, discussion is limited to Article 234 of UNCLOS and does not address Canadian claims of sovereignty over the NWP. See Bartenstein, *supra* note 14, at 26; BRUBAKER, *supra* note 14, at 65-66 (2005)(claim by Canada based upon internal waters discussed); *see also* James Kraska, *The Law of the Sea Convention and the Northwest Passage*, 22 INT'L J. OF MARINE AND COASTAL L. 257, 274-75 (2007)(providing an in-depth analysis of other
jurisdictional claims Canada has made with respect to its Arctic waters). Nonetheless, it is quite settled that “Article 234 ‘has no implication for any claims to sovereignty or other aspects of jurisdiction’ in those areas.” (Id. at 275 (citing NORDQUIST ET AL., supra note 14, at 398)).


101 See Canadian Coast Guard, Vessel Traffic Reporting Arctic Canada Traffic Zone (NORDREG), http://www.ccg-gcc.gc.ca/eng/MCTS/Vtr_Arctic_Canada (“consistent with international law regarding ice-covered areas, implement the requirements for vessels to report information prior to entering, while operating within and upon exiting Canada’s northern waters.”); see also Navigation Safety Regulations, SOR/2005-134, Sec. 76.(1), 82.(2)-(4) (establishing ice reporting requirements for dangerous ice conditions and severe ice accretions on ship superstructures); Ship Station (Radio) Regulations, 1999, SOR/2000-260, Sec. 15. (establishing additional Arctic communications equipment requirements so that vessels operating in the Canadian Arctic can “receiv[e] transmissions of ice information from radio stations and ice reconnaissance aircraft in the area in which the ship is navigating.”).

102 GOVERNMENT OF CANADA, STATEMENT ON CANADA’S ARCTIC FOREIGN POLICY (2010), http://www.international.gc.ca/Arctic-arctique/assets/pdfs/canada_Arctic_foreign_policy-eng.pdf; Stephen Harper, Prime Minister of Canada, Expanding Canadian Forces Operations in the Arctic (Aug. 10, 2007), http://www.pm.gc.ca/eng/news/2007/08/10/expanding-canadian-forces-operations-Arctic; see also UNITED STATES COAST GUARD, MAJOR ICEBREAKERS OF THE WORLD (July 18, 2013), http://www.uscg.mil/hq/eng/c5g5/c5g552/docs/20130718%20Major%20Icebreaker%20Chart.pdf (Depicting Canada with six icebreakers, and another under construction that is expected to be delivered in 2017. For purposes of comparison, the chart also depicts the U.S. with two operational icebreakers, and having no plans for an additional icebreaker (e.g., “TBD’)).

103 GOVERNMENT OF CANADA, STATEMENT ON CANADA’S ARCTIC FOREIGN POLICY, supra note 102; Prime Minister of Canada, Stephen Harper, supra note 102; CANADIAN COAST GUARD, ICEBREAKING PROGRAM, http://www.ccg-gcc.gc.ca/eng/CCG/Ice_Fleet; see also UNITED STATES COAST GUARD, MAJOR ICEBREAKERS OF THE WORLD, supra note 102. It should be noted, however, that Canada's own plans have shifted due to unforeseen environmental issues and cost overruns. Nevertheless, Canada has an actual plan and is implementing it, even though it may eventually do so with modifications. See Emma Jarratt and James Thomson, Canada Slow to Deliver on Arctic Commitments, BARENTS OBSERVER (Nov. 24, 2014), http://barentsobserver.com/en/2014/11/canada-slow-deliver-Arctic-commitments-27-11.

104 The text of the Russian legislation indicates that it is overtly focused on satisfying Article 234 of UNCLOS;

2. Principles, subject, and goals of regulating:
The Regulations shall, on the basis of non-discrimination for vessels of all States, regulate navigation through the Northern Sea Route for purposes of ensuring safe navigation and preventing, reducing, and keeping under control Marine environment pollution from vessels. Since the specifically severe climatic conditions that exist in the Arctic Regions and the presence of ice during the larger part of the year bring about obstacles, or increased danger, to navigation while pollution of sea, or the northern coast of the USSR might cause great harm to the ecological balance or upset it irreparably, as well as inflict damage on the interests and well-being of the peoples of the Extreme North.

REGULATIONS FOR THE NORTHERN SEA ROUTE, supra note 64; see also Huebert, supra note 64, at 267; Skaridov, supra note 64, at 295; Erik J. Molenaar, Arctic Marine Shipping: Overview if the International Legal Framework, Gaps, and Options, J. OF TRANSNATIONAL L. & POL’Y 289, 307 (2009) (“In addition to Canada, the Russian Federation also relies on Article 234 for prescribing standards that are more stringent than [generally accepted international rules and standards].”); Pedrozo, supra note 14, at 769.

105 See REGULATIONS FOR THE NORTHERN SEA ROUTE, supra note 64, at sec. 1.2 (defining Northern Sea Route as; The Northern Sea Route--national transportation route of the USSR, which is situated within the inland waters, territorial sea (territorial waters), or exclusive economic zone adjoining the USSR northern coast, and includes seaways suitable for guiding ships in ice. The extreme points of which in the west are the western entrances to the Novaya Zemlya straits and the meridian running from Mys Zhelaniya northward. And in the east, in the Bering Strait, by the parallel 66°N and the meridian 168°58’37”W.)

REGULATIONS FOR THE NORTHERN SEA ROUTE, supra note 64, at Sec. 3.

Id. at Sec. 1.4, 1.5, and 4.

Id. at Sec. 3. Guiding is explained in further detail in Section 7.4 (“Mandatory icebreaker guiding of vessels with ice pilot on board each vessel is established in the Proliv Vil'kitskogo, Proliv Shokal'skogo, Proliv Dmitriya Lapteva ... and Proliv Sannikova ... due to unfavourable navigational situation and ice conditions and for the purpose of ensuring safe navigation. In other regions the Marine Operations Headquarters shall, in consideration of ensuring safe navigation and for the purpose of providing the most favourable navigating conditions, prescribe one of the following types of guiding: 1) Guiding from shore along recommended routes up to a certain geographic point; 2) Airplane, or helicopter guiding; 3) Conventional pilotage; 4) Icebreaker guiding; 5) Icebreaker guiding combined with conventional pilotage of vessels. The Marine Operations Headquarters shall be entitled to substitute one type of guiding for another.”).

See Erik Franckx, The Legal Regime of Navigation in the Russian Arctic, 18 J. OF TRANSNAT'L L. & POL'Y 327, 339-40 (2009) (providing applied discussion on the different rates of fees based upon cargo type and vessel size.); see also ON APPROVAL OF THE TARIFF RATES FOR PROVISION OF ICEBREAKING PILOTAGE SERVICES PROVIDED BY THE FSUE “ATOMFLOT” ON THE NORTHERN SEA ROUTE, supra note 64; see Appendix C for charts depicting Russia's icebreaker escort fees (establishing that fees are dependent upon vessel ice classification, size, time of season, and number of zones traveled through on the NSR. In sum, it is difficult to establish the fee rate without information for the multiple factors upon which Russian fees are based. For example, a 50,000 DWT bulk carrier with a minimum ice classification of 1 that is going through three separate zones of the Northern Sea Route in September (i.e., the summer/autumn time period of the regulations) could incur an applicable to the entire NSR, which passes through its territorial seas and approximate charge of 21,895,500 Rubles or $392,000 (U.S.) for the icebreaker escort (based on the conversion rate as of Dec. 22, 2014.).


Article 26 states:
 Charges which may be levied upon foreign ships
 1. No charge may be levied upon foreign ships by reason only of their passage through the territorial sea.
 2. Charges may be levied upon a foreign ship passing through the territorial sea as payment only for specific services rendered to the ship. These charges shall be levied without discrimination. United Nations Convention on the Law of the Sea Art. 26, supra note 111.


Id. Art. 26(2).
REGULATIONS FOR THE NORTHERN SEA ROUTE, \textit{supra} note 64, at \textit{Sec. 2}; see also ICEBREAKER ESCORTING IN THE NORTHERN SEA ROUTE, \textit{supra} note 106; ON APPROVAL OF THE TARIFF RATES FOR PROVISION OF ICEBREAKING PILOTAGE SERVICES PROVIDED BY THE FSUE “ATOMFLOT” ON THE NORTHERN SEA ROUTE, \textit{supra} note 64; see Appendix D for charts depicting Russia’s icebreaker escort fees; Becker, \textit{supra} note 112, at 241 (describing Russian application of icebreaker escort fees in a non-discriminatory manner), \textit{but cf.} Claes Lykke Ragner, \textit{Den Norra Sjövägen}, in BARENTS--ETT GRÄNSLAND I NORDEN 114, 119 (Torsten Hallberg ed., 2008) (indicating that Russia may, in practice, not be charging fees in a manner that is actually linked to services rendered).


\textit{See} ON APPROVAL OF THE TARIFF RATES FOR PROVISION OF ICEBREAKING PILOTAGE SERVICES PROVIDED BY THE FSUE “ATOMFLOT” ON THE NORTHERN SEA ROUTE, \textit{supra} note 64; Appendix D.

See Section III.E., \textit{infra}.

This may be due to the difficulty of obtaining specific information regarding actual fees charged and the actual costs to Russia for providing the services. Some reviewers have indicated that the regulations have been implemented in a manner consistent with the text of the Russian regulations and Article 234. Becker, \textit{supra} note 112, at 241 (describing Russian application of icebreaker escort fees to Russian commercial vessels). However, other commenters have indicated that the icebreaker escort regulations are being enforced in a manner with little relationship to services rendered. \textit{See, e.g.}, Ragner, \textit{supra} note 116, at 119 (“Russia's mandatory icebreaker fees are high, and the fees are not directly linked to actual services rendered.”); Kraska, \textit{supra} note 52, at 277 (“The transit fees [] are disconnected from the actual cost of services rendered [].”); BRUBAKER, \textit{supra} note 14, at 94 (“The Russian provisions are probably discriminatory in their operation.”) (These commentators, however, simply provide conclusions. The author is unaware of any study that calculates the costs of operating icebreakers in the NSR. The factors for assessing costs would be quite complex, but ultimately, it is the responsibility of the coastal state to provide an accounting of the rates charged for services rendered.).

Scott Borgerson, Lawson Brigham, Michael Byers, Heather Conley, and Marlene Laruelle, \textit{The Emerging Arctic}, COUNCIL ON FOREIGN REL. (2014), http://www.cfr.org/Arctic/emerging-Arctic/p32620#f/ (“‘I want to stress the importance of the Northern Sea Route as an international transport artery that will rival traditional trade lanes.’ Vladimir Putin, President of Russia”); Kitagawa Hiromitsu, \textit{Japan and Russia: Breaking the Ice}, NIPPON.COM (Dec. 11, 2013), http://www.nippon.com/en/currents/d00099/ (“Russian President Vladimir Putin has encouraged commercial use of the Northern Sea Route, pledging to turn it into a major artery for international transport.”); \textit{see also} Huebert, \textit{supra} note 71, at 286; \textit{see also} Ragner, \textit{supra} note 116, at 116.

\textit{See} Becker, \textit{supra} note 112, at 24; Ragner, \textit{supra} note 116, at 119; BRUBAKER, \textit{supra} note 14, at 95 (providing discussion of Russia’s implementation of the icebreaker escort fee regulations).

RULES OF NAVIGATION ON THE NORTHERN SEA ROUTE, \textit{supra} note 106, at \textit{Sec. II.14-20}.

\textit{See supra} notes 105, 106, and 109.

UNITED STATES COAST GUARD, MAJOR ICEBREAKERS OF THE WORLD, \textit{supra} note 102 (Depicting Russia with twenty operational icebreakers, with four additional icebreakers under construction that are expected to be delivered in 2015, 2016, and 2017. For purposes of comparison, the chart also depicts the U.S. with two operational icebreakers, and having no plans for an additional icebreaker (e.g., “TBD”).

markets. The result: the challenging, ice-infested waters will cause oil spills, and the multiplying number of ships will bring crews from distant and unsavory lands will discover the new superhighway between Asian manufacturers and European environmental disasters are extremely likely.

See, e.g., note 92, at 75-77 (describing the MANHATTAN casualty).

See also

BRUBAKER, supra note 14; RASPUTNIK, supra note 14; BRUBAKER, supra note 14, at 107; see also McRae, supra note 68, at 17-18 (In the context of examining the Canadian regulatory regime, finding that Article 234 provides authority to coastal state to adopt and enforce regulations for environmental protection, and that “the rules relating to transit passage are still subject to the authority of the coastal state to regulate in respect of ice-covered areas.”).

BRUBAKER, supra note 14, at 105-09.

Id. at 106; see, e.g., NAVIGATING THE NORTHERN SEA ROUTE ADVISORY, supra note 58.

Classification Societies, 46 U.S.C. § 3316 (2014) (“Each department, agency, and instrumentality of the United States Government shall recognize the American Bureau of Shipping as its agent in classifying vessels owned by the Government and in matters related to classification [.]’’); Recognized Classification Society, 46 C.F.R. 90.10-35 (2014) (“The term recognized classification society means the American Bureau of Shipping or other classification society recognized by the Commandant.” (alteration in original)); See, e.g., NAVIGATING THE NORTHERN SEA ROUTE ADVISORY, supra note 58, at 4-22.


See Becker, supra note 112, at 241 (describing Russian application of icebreaker escort fees in a non-discriminatory manner), but cf. Ragner, supra note 116, at 119 (indicating that Russia may, in practice, be charging fees not linked to services rendered); see also BRUBAKER, supra note 14, at 80-81 (concluding that any practical application of the legal regime that excludes Russian flagged vessels would be in violation of Article 234).

Bert, supra note 11 (“Oil, gas, and mineral drilling, as well as fisheries and tourism[,] are inherently dangerous, because icebergs and storms can shear apart even large tankers, offshore drilling units, fishing vessels, and cruise ships. As a result, human and environmental disasters are extremely likely.’’); see also Bartenstein, supra note 14, at 22-23, 25-26, 38-46; FRANCKXX, supra note 92, at 75-77 (describing the MANHATTAN casualty).

See, e.g., Dennis Bryant, Polar Code Afoot, MARINELINK.COM (Sept. 2, 2014), http://www.marinelink.com/news/polar-afoot-code376184.aspx (providing summary of multiple vessel casualties in ice-covered areas); Bert, supra note 11 (“Oil, gas, and mineral drilling, as well as fisheries and tourism[,] are inherently dangerous, because icebergs and storms can shear apart even large tankers, offshore drilling units, fishing vessels, and cruise ships. As a result, human and environmental disasters are extremely likely.’’); Kraska, supra note 19, at 1125 (“Poorly maintained Third World merchant ships and their multinational crews from distant and unsavory lands will discover the new superhighway between Asian manufacturers and European markets. The result: the challenging, ice-infested waters will cause oil spills, and the multiplying number of ships will bring
illegal migrants or, even worse, terrorists.”); Franckx, supra note 110, at 338 (“Given the extremely hazardous navigation conditions that can be encountered when sailing the Northern Sea Route, a detailed set of requirements have been adopted in order to ensure the safety of navigation and the protection of the Arctic marine environment from pollution.”).


139 See, e.g., Northern Canada Vessel Traffic Services Zone Regulations, supra note 64; ON APPROVAL OF THE TARIFF RATES FOR PROVISION OF ICEBREAKING PILOTAGE SERVICES PROVIDED BY THE FSUE “ATOMFLOT” ON THE NORTHERN SEA ROUTE, supra note 64; Appendix D; see also Canadian Coast Guard, Coast Guard makes rescue in the high Arctic, http://www.ccg-gcc.gc.ca/shorelinesfall2011-3 (last modified Apr. 9, 2014), (describing marine casualty where Canadian Coast Guard icebreaker was dispatched to a vessel that ran aground in order to remove the petroleum products onboard); Oil or Hazardous Material Pollution Prevention Regulations for Vessels, 33 C.F.R. Part 155 (2014); Bert, supra note 11 (“The United States and other Arctic nations track AIS ships and are able to respond to emergencies based on its signals. For this reason, mandating AIS for all vessels in the Arctic is needed. The U.S. government also needs to work with Russia to impose a traffic separation scheme in the Bering Strait, where chances for a collision are high. Finally, the United States should push for compulsory tandem sailing for all passenger vessels operating in the Arctic. Tandem sailing for cruise ships and smaller excursion boats will avert another disaster like RMS Titanic.”).

140 See NORTHERN SEA ROUTE INFORMATION OFFICE, http://www.Arctic-lio.com/nsr_ice (“There are no specific dates for commencement and completion of navigation; it all depends on particular ice conditions. In 2011 the navigation season on the NSR seaways for large vessels constituted 141 days in total, i.e. more than 4.5 months.”); CANADIAN ICE SERVICE, CANADIAN ARCTIC SEA ICE MINIMUM WAS NEAR-NORMAL IN 2013 (Oct. 24, 2013), http://ec.gc.ca/glaces-ice/default.asp?lang=En&n=71777A6E-1 (“The southern route of the Northwest Passage has been navigable since 2006 (for a few days/weeks each year.”); The U.S. Arctic maritime domain is also covered with ice for a vast majority of the year. See Letter from Rebecca J. Lent, supra note 23, at 6 (Indicating ice-covered waters for approximately eight (08) months of the year. (“the open-water season (1 July to 31 October.”)); Thoman, supra note 140 (“Prior to about 2000, the typical summer at Barrow would find sea ice lingering into late June or early July. From then on, the ice would melt at an increasing rate and be pushed to and fro by the wind. Usually there was a period from early August until sometime in September when the sea near Barrow would be largely ice-free. However, the main ice pack was rarely more than 150 miles offshore at the end of summer, and by sometime in October, cooling temperatures and autumn storms would typically return the sea ice to Barrow.”).

141 RICK THOMAN, CLIMATE.GOV, NAT'L OCEANIC AND ATMOSPHERIC ADMIN., IN BARROW, ALASKA, CLIMATE CHANGE IN ACTION (Sept. 6, 2013), https://www.climate.gov/newsfeatures/understanding-climate/barrow-alaska-climate-change-action (“Not all years [on the sea near Barrow] were “typical,” of course. Sometimes the sea ice never completely moved out of the Barrow area all summer.”); Bert, supra note 11 (“The NSR was not navigable for years because of heavy ice, but it now consists of water with floating ice during the summer months.”); KARL MAGNUS EGER, CENTRE FOR HIGH NORTH LOGISTICS (CHNL), ARCTIC RESOURCES AND TRANSPORTATION INFORMATION SYSTEM (ARCTIS DATABASE) (2010), http://www.arctis-search.com/Comparison+of+Operational+Conditions+along+the+Arctic+Routes.

142 See e.g., supra note 136.


145 See FRANCKX, supra note 92, at 75-77.

146 Id.

147 Id.


152 See Kraska, *supra* note 99, at 281 (“[T]he Northwest Passage, the world’s longest and perhaps most environmentally sensitive international strait.”).


156 See Byers, *supra* note 50; Bert, *supra* note 11 (“In the lower forty-eight states, response time to an oil spill or capsized vessel is measured in hours. In Alaska, it could take days or weeks to get the right people and resources on scene. The nearest major port is in the Aleutian Islands, thirteen hundred miles from Point Barrow, and response aircraft are more than one thousand miles south in Kodiak, blocked by a mountain range and hazardous flying conditions. The Arctic shores lack infrastructure to launch any type of disaster response, or to support the growing commercial development in the region.”).


158 See *supra* note 36.


160 Convention on the Law of the Sea Art. 234, *supra* note 12 (“Such laws and regulations shall have due regard to navigation and the protection and preservation of the marine environment [].”).


162 See Pedrozo, *supra* note 14, at 769-70; see also Diplomatic Note from the United States to Canada, *supra* note 15, Appendix A; Letter from Eric Benjaminson, *supra* note 15, Appendix B.


164 See, e.g., Pedrozo, *supra* note 14, at 771 (“neither government has provided sufficient data to demonstrate that their domestic laws and regulations are based on the best available scientific evidence, as required by UNCLOS Article 234.”).
See id. (Pedrozo's assertion might simply be a conclusion that Canada and Russia have failed to explain the scientific bases for their legal regimes.).

See Bryant, supra note 137 (providing a summary of multiple vessel casualties in icecovered areas); Bert, supra note 11 (“Oil, gas, and mineral drilling, as well as fisheries and tourism ... are inherently dangerous, because icebergs and storms can shear apart even large tankers, offshore drilling units, fishing vessels, and cruise ships. As a result, human and environmental disasters are extremely likely.”); Kraska, supra note 19, at 1125 (“Poorly maintained Third World merchant ships and their multinational crews from distant and unsavory lands will discover the new superhighway between Asian manufacturers and European markets. The result: the challenging, ice-infested waters will cause oil spills, and the multiplying number of ships will bring illegal migrants or, even worse, terrorists.”); Franckx, supra note 110, at 338 (“Given the extremely hazardous navigation conditions that can be encountered when sailing the Northern Sea Route, a detailed set of requirements have been adopted in order to ensure the safety of navigation and the protection of the Arctic marine environment from pollution.”).

The multiple days it takes to respond to incidents in the Arctic, which is considered a normal response time for the Arctic, stands in stark contrast with the nearly immediate response capabilities the continental U.S. experiences. This is valuable time that can serve to mitigate or even stave off a humanitarian or environmental disaster. See, e.g., Transcript of Record at 37, USCG/MMS Marine Board of Investigation into the Marine Casualty, Fire, Pollution, and Sinking of Mobile Offshore Drilling Unit Deepwater Horizon, with Loss of Life in the Gulf of Mexico 21-22 April 2010 (May 11, 2010), http://www.uscg.mil/hq/cg5/cg545/dw/exhib/Deepwater%20Horizon%20Joint%20Investigation%20Transcript%20-%20May%2011,%202010.pdf (Describing the 64-minute response time for USCG assets to respond to the DEEPWATER HORIZON incident in the EEZ located in the Gulf of Mexico, approximately 45 miles offshore); Shaw, supra note 21, at 26; see generally UNITED STATES COAST GUARD, ARCTIC STRATEGY, supra note 10, at 20-21; Bert, supra note 11 (“In the lower forty-eight states, response time to an oil spill or capsized vessel is measured in hours. In Alaska, it could take days or weeks to get the right people and resources on scene. The nearest major port is in the Aleutian Islands, thirteen hundred miles from Point Barrow, and response aircraft are more than one thousand miles south in Kodiak, blocked by a mountain range and hazardous flying conditions. The Arctic shores lack infrastructure to launch any type of disaster response, or to support the growing commercial development in the region.”).


This is not to say that every clause of every legal requirement of these regulatory frameworks is based on the best available scientific evidence. This is simply a broad assessment of the general reporting, engineering, and icebreaker escort requirements. A line-by-line, in-depth analysis of these legal frameworks to ensure consistency with the best available scientific evidence is not appropriate for the general nature of examining the legality of employing Article 234 as an exception to freedom of navigation regimes nor as a basis to charge fees for services rendered.


Id. Art. 24(1).

See, e.g., Bartenstein, supra note 14, at 42.

See Bartenstein, supra note 14, at 36-37, 42-44; see also BRUBAKER, supra note 14, at 57.
See also Bartenstein, supra note 14, at 30, 45.


Id. Art. 26(1).

Id. Art. 26(2).

Bert, supra note 11 (“Oil, gas, and mineral drilling, as well as fisheries and tourism[] are inherently dangerous, because icebergs and storms can shear apart even large tankers, offshore drilling units, fishing vessels, and cruise ships. As a result, human and environmental disasters are extremely likely.”); see also Bartenstein, supra note 14, at 22-23, 25-26, 38-46; FRANCKX, supra note 92, at 75-77 (describing the MANHATTAN casualty). Furthermore, the existence of Article 234 and countless international and national requirements specific to vessel navigation in polar environments provide further evidence that vessels are subject to different and greater hazards than other maritime environments.


Id. Art. 38(2).

Id. Art. 34(1).

Id. Art. 34(2).

Article 34(2) states that “[t]he sovereignty or jurisdiction of the [coastal state] is exercised subject to this Part and to other rules of international law.” The “subject to” language connotes limitations on the authority and jurisdiction of the coastal state rather than an increase in authority and jurisdiction under Article 34.

Id. Art. 42 (emphasis added).

Id. Art. 42(1), (4).

Id. Art. 42(5) (“The flag State of a ship or the State of registry of an aircraft entitled to sovereign immunity which acts in a manner contrary to such laws and regulations or other provisions of this Part shall bear international responsibility for any loss or damage which results to States bordering straits.”).

Id.

Id. Art. 42(2).

Id. (emphasis added).

See generally, Bartenstein, supra note 14, at 37-39, 44-45; Byers and Lalonde, supra note 10, at 1186.

See supra note 162.

See also, e.g., REQUIREMENTS FOR VESSELS NAVIGATING THE NORTHERN SEA ROUTE, supra note 105, at § 2.3 (“Icebreakers are permitted to navigate along the NSR under ice conditions that correspond to the designation of their respective ice resistance category. Operation of an icebreaker under more severe ice conditions than these envisaged by its ice resistance category is permitted in each individual case upon decision of the Administration (Headquarters) following a review of the appropriate documentation provided by the owner of the icebreaker confirming that the state of the hull, machinery and systems of re [sic] particular icebreaker is such as to ensure the necessary navigation safety in the NSR area, as well as preclude a possibility of pollution of the sea.”).


Id. Art. 234.
Notably, this assessment does not include the operational application of these legal regimes. As mentioned previously, operational application is not assessed in this paper due to the requirement for brevity. Suffice it to say that commentators have called into question the practical application of these legal regimes. See, e.g., supra notes 116, 121-23, and 135.)

See generally supra note 168.


Id. Art. 58(1) (emphasis added).

Id. Art. 58(3).

Id. Art. 42(2).

See Section III.E.2.d, supra.


Id. (Section 5 addresses International Rules and National Legislation to Prevent, Reduce and Control Pollution of the Marine Environment; Section 6 addresses Enforcement of the Rules and Legislation adopted under Section 5; and Section 7 addresses Safeguards pertaining to the enforcement mechanisms under Section 6, relating to the conduct of investigations, legal proceedings, etc.).

Id.

See Bartenstein, supra note 14, at 34 (discussing how Article 233 might impact the interpretation of Article 234).


Article 234 states in relevant part that the laws “shall have due regard to navigation and the protection and preservation of the marine environment based on the best available scientific evidence.” Due regard is required for both the right of navigation AND for protection and preservation of the environment. This suggests that there is balancing between two important goals of UNCLOS: freedom of navigation and the right and responsibility of nations to protect the environment. Consequently, the most reasonable interpretation of Article 234 is that there is a rebuttable presumption that a right to transit passage exists, subject to a demonstration by the coastal state that a vessel does not comply with laws enacted pursuant to Article 234, thereby presenting a threat to the environment. See also Section II.E.3, infra (discussing a rebuttable presumption of right to transit passage); United Nations Convention on the Law of the Sea Art. 192, Dec. 10, 1982, 1833 U.N.T.S. 397, http://www.un.org/depts/los/convention_agreements/texts/unclos/closindx.htm (“States have the obligation to protect and preserve the marine environment.”). But see United Nations Convention on the Law of the Sea Art. 38, Dec. 10, 1982, 1833 U.N.T.S. 397, http://www.un.org/depts/los/convention_agreements/texts/unclos/closindx.htm (“all ships and aircraft enjoy the right of transit passage, which shall not be impeded.”); see also Bartenstein, supra note 14, at 39.

Sec, e.g., McRae, supra note 68, at 18.


Id.; see also Pedrozo, supra note 14, at 757, 770-71; see Bartenstein, supra note 14, at 42; McRae, supra note 68, at 17-18.

See supra note 36.

Arctic Waters Pollution Prevention Act, R.S.C. 1985, c. A-12, § 12(2) states:

(2) The Governor in Council may by order exempt from the application of any regulations made under subsection (1) any ship or class of ship that is owned or operated by a sovereign power, other than Canada, where the Governor in Council is satisfied
that (a) appropriate measures have been taken by or under the authority of that sovereign power to ensure the compliance of
the ship with, or with standards substantially equivalent to, standards prescribed by regulations made under paragraph (1)(a)
that would otherwise be applicable to it within any shipping safety control zone; and
(b) in all other respects all reasonable precautions have been or will be taken to reduce the danger of any deposit of waste
resulting from the navigation of the ship within that shipping safety control zone.

---

214 See generally NAVIGATING THE NORTHERN SEA ROUTE ADVISORY, supra note 58, at 4-22; Int'l Maritime

convention_agreements/texts/unclos/UNCLOS-TOC.htm.

216 See D. Ginsberg & Sons, Inc., supra note 69, at 208 (“the cardinal rule that, if possible, effect shall be given to every clause
and part of a statute.” (citing Market Co. v. Hoffman, 101 U.S. 112, 115 (1879); Ex parte Public National Bank, 278 U.S.
101, 104 (1928)).

217 The NWP and the NSR constitute vast portions of the area subject to Article 234 authority, e.g., “ice-covered areas within
the limits of the exclusive economic zone.” See supra note 17.

218 See Bartenstein, supra note 14, at 45.


220 See supra note 208.

depts/los/convention_agreements/texts/unclos/closindx.htm (“States have the obligation to protect and preserve the marine
environment.”); see also supra note 208.


223 Id.

224 This would likely require a case-by-case analysis of the factors before and after performing a measure as drastic as denying
entry to a particular vessel for non-compliance with regulations adopted and enforced pursuant to Article 234. See also
Bartenstein, supra note 14, at 45.

225 See BRUBAKER, supra note 14, at 45, 94-95, 109.

226 See, e.g., supra notes 71 and 72.

227 It is worth noting that there were three nations primarily involved with the drafting and adoption of Article 234; the U.S.,
Russia, and Canada. See Bartenstein, supra note 14, at 24-25; Huebert, supra note 71, at 249-51. Therefore the interpretations
of these nations should be given considerable regard when determining the meaning and application of the Article. The lack
of agreement on meaning, and the deviation in application, among these three nations has served to further confuse the issue.
However, two of those nations have a consistent interpretation and application that the intent of the Article was to provide the
unilateral right to establish and enforce laws under the narrow exception carved out by Article 234. Furthermore, the context
in which the Article was developed and adopted is helpful in determining the intent of the Article; the MANHATTAN voyages
and the adoption of the 1970 Canadian Arctic Waters Pollution Prevention Act, which the world community, including
Canada, found inconsistent with international law at the time, provide evidence that one of the primary intentions of Article
234 was to provide authority that would make such laws and regulations consistent with international law. See generally
Moore, supra note 14, at 18-23; Huebert, supra note 71, at 249-56; FRANCKX, supra note 92, at 75-76, 88; NORDQUIST
ET AL., supra note 14, at 398.

228 See Byers and Lalonde, supra note 10, at 1207-10 (recommending U.S. and Canada coordinate to ensure regulatory regimes in
Alaska and the Canadian Arctic are consistent in order to collaboratively address environmental, safety, and security issues).
See, e.g., supra notes 115-18; It should be noted that the decision to charge a stricken vessel with fees for services rendered generally carries with it an important balancing test of its own. While the possibility of being charged fees may help to dissuade reckless ventures into the Arctic, it may also dissuade those in peril from requesting assistance until it is too late for an effective response. Consequently, the decision regarding whether to charge fees for services rendered in emergent search-and-rescue type incidents should not be taken lightly and should be primarily made by those with decades of experience, and whose agency has been performing the mission for more than 200 years--the U.S. Coast Guard. Nonetheless, having this option available will help to offset the costs. With wise implementation based on good judgment and experience, fees for services rendered could likely have the desired effect of dissuading reckless ventures into the Arctic, but not dissuading mariners from requesting assistance when needed.

See Bert, supra note 11 (“The U.S. government should invest in icebreakers, aircraft, and shore-based infrastructure. A ten-year plan should include the building of at least two heavy icebreakers, at a cost of approximately $1 billion a piece, and an air station in Point Barrow, Alaska, with at least three helicopters. Such an air station would cost less than $20 million, with operating, maintenance, and personnel costs comparable to other northern military facilities. Finally developing a deepwater port with response presence and infrastructure is critical.”).

This is a definite possibility given that many vessels have recently found themselves stuck in ice and in need of assistance in polar environments. See, e.g., Shannon Riddle, U.S. Coast Guard Vessel Assists Sailboat Trapped in Arctic Ice, KTUU (July 13, 2014), http://www.ktuu.com/news/news/us-coast-guard-vessel-assists-sailboat-trapped-in-Arctic-ice/26932292; see also Byers and Lalonde, supra note 10, at 1197-98 (describing a casualty in the Antarctic that “could just as easily have sunk in the Northwest Passage[].”).

See supra note 230.

See Public Comments, Proposed Oil and Gas Lease Sale 242, Alaska OCS Region, Beaufort Sea Planning Area, supra note 32; Moore et al., supra note 32; Bert, supra note 11; ALASKA OCS REGION, MINERALS MANAGEMENT SERVICE, U.S. DEPARTMENT OF THE INTERIOR, FINAL BID RECAP, supra note 32.

See, e.g., supra notes 20-23.

See Letter from Rebecca J. Lent, supra note 23, at 8; Knickmeyer, supra note 2 (quoting U.S. Rep. John Garamendi, D-Cal.); Koren, supra note 1 (quoting U.S. Sen. Lisa Murkowski, R-Alaska, and U.S. Rep. Rick Larsen, D-Wash.); O’Rourke, supra note 3, at 8-9, 41; Francis, supra note 43 (quoting U.S. Sen. Mark Begich, D-Alaska); see also Bert, supra note 11 (“In the lower forty-eight states, response time to an oil spill or capsized vessel is measured in hours. In Alaska, it could take days or weeks to get the right people and resources on scene. The nearest major port is in the Aleutian Islands, thirteen hundred miles from Point Barrow, and response aircraft are more than one thousand miles south in Kodiak, blocked by a mountain range and hazardous flying conditions. The Arctic shores lack infrastructure to launch any type of disaster response, or to support the growing commercial development in the region.”); see also NAT’L ACAD. OF SCIENCES, OCEAN STUD. BD., POLAR RES. BD., MARINE BD., REPORT IN BRIEF, RESPONDING TO OIL SPILLS IN THE U.S. ARCTIC MARINE ENV’T (April 2014), http://dels.nas.edu/resources/static-assets/materials-based-on-reports/reports-in-brief/Arctic-Oil-Spill-Brief-Final02.pdf (“Lack of infrastructure and oil spill response equipment in the U.S. Arctic could present a significant liability in the event of a large oil spill.”).

See Letter from Rebecca J. Lent, supra note 23, at 1, 5, 8; Shaw, supra note 21; UNITED STATES COAST GUARD, ARCTIC STRATEGY, supra note 10, at 20-21; Bert, supra note 11 (“In Alaska, it could take days or weeks to get the right people and resources on scene. The nearest major port is in the Aleutian Islands, thirteen hundred miles from Point Barrow, and response aircraft are more than one thousand miles south in Kodiak, blocked by a mountain range and hazardous flying conditions. The Arctic shores lack infrastructure to launch any type of disaster response, or to support the growing commercial development in the region.”).

See supra notes 38, 39, 42, 49, 149-52, and 237.

See supra notes 47-49, 102-10, 116-21, and 126-30.
See supra notes 2-8.

241

See Letter from Rebecca J. Lent, supra note 23, at 1, 5; ALASKA ESKIMO WHALING COMM'N, supra note 23; UNITED STATES COAST GUARD, ARCTIC STRATEGY, supra note 10; THE PEW ENV'T GROUP, supra note 20.

242

See Byers and Lalonde, supra note 10, at 1207-10 (recommending U.S. and Canada coordinate to ensure regulatory regimes in Alaska and the Canadian Arctic are consistent in order to collaboratively address environmental, safety, and security issues).
GLOBAL WARMING HEATS UP THE AMERICAN-CANADIAN RELATIONSHIP: RESOLVING THE STATUS OF THE NORTHWEST PASSAGE UNDER INTERNATIONAL LAW

ABSTRACT

Global warming is turning the hypothetical Northwest Passage into a reality. Shipping that utilizes the Northwest Passage can save over 4000 miles in travel, with the attendant economic benefits. However, the legal status of the Northwest Passage, in particular the portion of the Northwest Passage which cuts through the Canadian Arctic Archipelago, remains indeterminate and is a source of contention between the United States and Canada. Canada takes the position that the Northwest Passage is internal Canadian waters, which gives them broad authority to regulate and restrict maritime traffic through the Northwest Passage. In contrast, the United States takes the position that the Northwest Passage constitutes an international strait, with international shipping having the right of transit passage. While it is currently unlikely that either the United States or Canada would be willing to submit this dispute to an international tribunal, the dispute in the Northwest Passage showcases the difficulty that even closely allied neighbors can face in protecting their own interests under international law.

Introduction

On September 14, 2007, the European Space Agency announced that analysis of satellite imagery showed that the accelerating shrinkage in ice cover had opened up the Northwest Passage, a “short cut between Europe and Asia that had been historically impassable.” Using the Northwest Passage had previously been considered commercially impractical due to multi-year pack ice that rendered navigation hazardous or impossible. However, lured by the savings of almost 4000 miles compared to the Panama Canal route, international shipping is already attempting to use the Northwest Passage. These developments inject new tension into the disagreement between the United States and Canada over the status of the Northwest Passage under international law.

Canada takes the position that the Northwest Passage constitutes internal Canadian waters, which gives them broad authority to regulate and restrict maritime traffic through the Northwest Passage. In contrast, the United States takes the position that the Northwest Passage constitutes an international strait, with international shipping having the right of transit passage. While it is currently unlikely that either the United States or Canada would be willing to submit this dispute to an international tribunal, the dispute in the Northwest Passage showcases the difficulty that even closely allied neighbors can face in protecting their own interests under international law.

Part I of this article provides a historical overview of the Northwest Passage and prior disputes between the United States and Canada regarding the Northwest Passage. Part II analyzes the development of international law relevant to the Northwest Passage dispute. Part III analyzes the strengths and weaknesses of the positions held by the United States...
and Canada. Part IV will conclude by examining the practical limitations on resolving this issue through an international tribunal.

I. The History of the Northwest Passage

A. Geographical Background

The Northwest Passage refers to the body of Arctic water that connects the Atlantic and Pacific oceans along the northern coast of North America. It stretches from the Bering Strait in the west, runs along the northern coast of Alaska and Canada, and then weaves through the Canadian Arctic Archipelago until it exits through the Davis Strait and Baffin Bay in the east. Since European colonization of North America began, explorers have sought a usable route around the northern coast of North America. However, arctic weather conditions created insurmountable barriers for early explorers, particularly the multi-year pack ice common in the waterways that did not melt during the summers, but instead built up year after year.

B. Successful Navigations of the Northwest Passage

The first successful transit of the Northwest Passage took three years of hard sailing and was completed by Roald Amundson in 1906. In the wake of this accomplishment, the Canadian government made a formal claim to possession of the lands and islands within the Northwest Passage using a “sector” theory of sovereignty. However, this sector claim has never been recognized internationally. While the United States formally protested this sector claim, the practical difficulties of navigating the Northwest Passage meant that no real confrontation between Canada and the United States occurred. It did, however, mark the first time that Canada made the claim that the waters of the Northwest Passage constituted “internal Canadian waters” as well as the first United States rejection of this claim.

No ship would repeat Amundson's achievement for nearly four decades, until the St. Roch, with Henry Larsen of the Royal Canadian Mounted Police in command, successfully navigated the Northwest Passage. The 1950s marked the first transit of the Northwest Passage by a ship flying the United States flag, when the U.S. Coast Guard cutter Storis successfully transited the Northwest Passage in 1957. Four years later, in 1961 the U.S.S. Seadragon completed the first submarine transit of the Northwest Passage. As the 1960s drew to a close, Exxon sent a specially modified super-tanker, the S.S. Manhattan, through the Northwest Passage in an experiment to test the viability of the Northwest Passage as a commercial shipping route. Although neither Exxon nor the U.S. government sought Canadian permission for this voyage, the Canadian government preemptively granted permission anyways.

In the wake of the Manhattan's voyage, the Canadian government enacted the Arctic Waters Pollution Prevention Act (AWPPA) in 1970. Although international law at that time did not recognize coastal state rights further than twelve nautical miles from shore, the AWPPA imposed requirements on all shipping within 100 miles of Canada's Arctic shore. Shortly thereafter Canada attempted to propose legislation at the Intergovernmental Maritime Consultative Organization (IMCO) that would have validated the range of the AWPPA. However, this proposal was rejected by the IMCO. Canada's efforts met with greater success in the 1982 UN Convention on the Law of the Sea (UNCLOS) with the adoption of Article 234, which granted coastal states additional rights over ice-covered seas within their Exclusive Economic Zone (EEZ). However, at least one scholar noted that while this gives coastal nations the right to enact environmental legislation protecting the waterways, it fails entirely to address the question of sovereignty over those waterways.
C. The Voyage of the Polar Sea: The Northwest Passage Dispute Comes to a Head

The Northwest Passage dispute between Canada and the United States came to a head in 1984, when the U.S. informed Canada that the U.S. Coast Guard icebreaker *Polar Sea* would utilize the Northwest Passage to sail from Thule, Greenland to its home port of Seattle, Washington. The United States clearly stated that its notification was a courtesy and did not constitute recognition of the Canadian position regarding the Northwest Passage. While Canada was inclined to work with the United States to address logistical concerns regarding the *Polar Sea*, Canadian public opinion forced Canada to take a more confrontational posture.

Diplomatic negotiations between the United States and Canada eventually led to the 1988 Agreement on Arctic Cooperation. While neither nation conceded the validity of the other's position regarding the status of the Northwest Passage, the Agreement did specify that the United States would only operate icebreakers within the Northwest Passage with Canadian consent. The Agreement on Arctic Cooperation did not apply to any ships besides icebreakers, and explicitly preserved each nation's original position regarding the Northwest Passage.

D. Recent Developments in the Northwest Passage

Since the implementation of the 1988 Agreement on Arctic Cooperation, neither the United States nor Canada has forced a confrontation over the status of the Northwest Passage. However, the European Space Agency's announcement that sea ice in the Northwest Passage had shrunk to the point that the Northwest Passage could be considered open raises the specter of increasing commercial use of the Northwest Passage. An increasing number of commercial vessels, including cruise ships, have utilized the Northwest Passage in the past decade.

Currently, registration of ships using the Northwest Passage is voluntary under Canadian law, with approximately 98% of shipping complying. In 2008, Canadian Prime Minister announced that Canada would be making registration mandatory. However, Canada has not yet done so, potentially due to United States' concerns about validating Canada's claims to sovereignty over the Northwest Passage. The increased commercial traffic and Canada's attempt to regulate it makes it increasingly likely that the formal status of the Northwest Passage under international law will become an issue of concern for both the United States and Canada.

II. The Northwest Passage and International Law

Article 38 of the Statute of the International Court of Justice (“I.C.J.”) recognizes three primary sources of international law. First, the I.C.J. recognizes “international conventions,” which are usually formulated as treaties, but which could include conventions, protocols, and declarations. Second, the I.C.J. recognizes international customs where those customs are accepted as a general practice required by law. Third, the I.C.J. recognizes the general principles of law recognized by civilized nations. In addition, Article 38 also identifies as a “subsidiary means for the determination of rules of law” prior judicial decisions and the teachings of the publicists.

A. Treaties Alone Cannot Determine International Law in the Northwest Passage

With the exception of the previously mentioned Agreement on Arctic Cooperation, there are no treaties concerning the Northwest Passage that bind both the United States and Canada. While as a body of water the Northwest...
Passage would seem to fall within the purview of the United Nations Convention on the Law of the Sea, the United States has not yet ratified the UNCLOS. Thus, despite the fact that Canada ratified the UNCLOS on November 7, 2003, the failure of the United States to ratify the UNCLOS prevents it from being considered international law by virtue of its status as a binding treaty. While both the United States and Canada are signatories to Convention on the Territorial Sea and the Contiguous Zone (CTSCZ), a predecessor of the UNCLOS, Article 311 of the UNCLOS specifically supersedes its predecessors and thus keeps the CTSCZ from being binding upon Canada.

The 1988 Agreement on Arctic Cooperation, while binding both the United States and Canada, is a document of extreme brevity. Only a page and a half long, the agreement contains very few applicable provisions, and those provisions are both specific and limited. After the customary introductions, paragraph 3 focuses on the substance of the treaty:

3. In recognition of the close and friendly relations between their two countries, the uniqueness of ice-covered maritime areas, the opportunity to increase their knowledge of the marine environment of the Arctic through research conducted during icebreaker voyages, and their shared interest in safe, effective icebreaker navigation off their Arctic coasts:

--The Government of the United States and the Government of Canada undertake to facilitate navigation by their icebreakers in their respective Arctic waters and to develop cooperative procedures for this purpose;

--The Government of Canada and the Government of the United States agree to take advantage of their icebreaker navigation to develop and share research information, in accordance with generally accepted principles of international law, in order to advance their understanding of the marine environment of the area;

--The Government of the United States pledges that all navigation by U.S. icebreakers within waters claimed by Canada to be internal will be undertaken with the consent of the Government of Canada.

A careful reading of the Agreement on Arctic Cooperation reveals that its scope encompasses only icebreakers of the United States and Canada. Commercial shipping, private craft, and non-icebreaker military vessels are excluded from the Agreement. Furthermore, both nations specifically reserved their original positions regarding waters in question and prevented the Agreement from affecting their respective positions through Article 4.

No other treaties relating to the Arctic waters or the Northwest Passage have been registered with the United Nations. Thus, it is clear that there is no treaty binding both the United States and Canada which can be used to determine international law applicable to the Northwest Passage dispute.

B. The United States Largely Accepts the UN Convention on the Law of the Sea as Customary International Law

Despite the failure of the United States government to ratify the UN Convention on the Law of the Sea, this failure is not due to an overall rejection of the UNCLOS. Instead, the United States objected to Part XI of the UNCLOS, particularly as it dealt with mineral exploitation of the seabed beyond the limits of national jurisdiction. The United
States accepts most of the UNCLOS as codifying customary international law. This position was recently reaffirmed by United States diplomats participating in the Arctic Ocean Conference, held in Ilulissat, Greenland in May of 2008. Thus, the UNCLOS, although not a treaty binding both the United States and Canada, can largely be viewed as a codification of customary international law. As such, both the United States and Canada would be bound by those provisions that are determined to be customary international law, despite the United States failure to ratify the UNCLOS.

I. Treatment of “Internal Waters” Under the UNCLOS

Canada's position is that the Northwest Passage constitutes “internal waters.” Article 8 of the UNCLOS defines internal waters as “waters on the landward side of the baseline of the territorial sea.” Article 8 makes an exception for archipelagic states, of which Canada does not qualify. However, Article 7 of the UNCLOS allows for the drawing of straight baselines where “there is a fringe of islands along the coast in its immediate vicinity.” In 1985, one month after the voyage of the Polar Sea through the Northwest Passage, the Canadian Foreign Minister announced that Canada would use straight baselines to determine the limits of Canada's internal waters. Canada's baselines surrounded the entirety of the Canadian Arctic archipelago, thus covering that portion of the Northwest Passage.

Several nations, including the United States, protested Canada's claim on the basis that the baselines were excessively long and diverted too much from the direction of the mainland coast. This position relies on the third paragraph of Article 7, which states that “[t]he drawing of straight baselines must not depart to any appreciable extent from the general direction of the coast, and the sea areas lying within the lines must be sufficiently linked to the land domain to be subject to the regime of internal waters.”

Canada, by declaring that the Northwest Passage was internal Canadian waters, sought the ability to exercise its sovereignty over the waters of the Northwest Passage, in accordance with Article 2 of the UNCLOS. This sovereignty is not unlimited; in particular, Article 18 of the UNCLOS establishes the right of “innocent passage” for foreign ships. “Innocent passage” is defined by the UNCLOS to mean “navigation through the territorial sea” for the purpose of traversing that sea in a “continuous and expeditious” manner. Innocent passage must also be conducted in a manner that is “not prejudicial to the peace.” Articles 21 through 26 give the coastal state a wide variety of powers (and some limitations) to regulate and oversee shipping through internal waters.

In addition, Canada also invokes Article 234 of the UNCLOS, which grants coastal states additional rights to regulate waters in ice-covered areas for the purpose of preventing, reducing, or controlling pollution. This article was a compromise added at the behest of Canada, which sought the additional legitimacy for its ability to protect its claimed waters from pollution. Canada originally sought to enshrine its sovereignty claims over the Northwest but could not gain enough support for its position. However, the applicability of Article 234 may itself be in question, since it deals specifically with “ice-covered areas.” Since the effect of global warming, and the underlying reason for the heightened concern regarding the Northwest Passage, is the loss of surface ice, it is uncertain as to whether Article 234 still applies.

*177 2. Treatment of “International Straits” Under the UNCLOS

The position of the United States is that the Northwest Passage constitutes an international strait, with foreign vessels having the right of transit passage. Article 37 of the UNCLOS applies to “straits which are used for international navigation between one part of the high seas or an exclusive economic zone and another part of the high seas or an
exclusive economic zone.” In regards to the Northwest Passage, the applicable high seas are the Atlantic Ocean on the eastern end of the Northwest Passage, and the Pacific Ocean on the western end.

If it is classified as an international strait, foreign ships would enjoy the right of transit passage, defined as “the freedom of navigation and overflight solely for the purpose of continuous and expeditious transit of the strait between one part of the high seas ... and another part of the high seas.” Ships exercising the right of transit passage are required to comply with a number of conditions, including proceeding through the strait without delay, refraining from the threat or use of force, refraining from activities beyond those incident to normal transit, and compliance with international regulations for safety and pollution control. In addition, ships exercising transit passage may not conduct research or surveys without the permission of the coastal state.

Coastal states are also restricted in their ability to regulate an international strait where the right of transit passage exists. Article 41 specifically gives coastal states the right to designate sea lanes to prescribe traffic separation schemes when necessary. In addition, Article 42 allows coastal states to adopt laws and regulations with respect to safety, pollution, fishing, and customs-related activity. However, these laws and regulations may not discriminate against foreign ships and their application cannot have the practical effect of “denying, hampering, or impairing the right of transit passage.” Transit passage may also not be suspended.

While, under the UNCLOS, transit passage is only possible through an international strait, an international strait does not automatically allow for transit passage. Article 35 limits the scope of transit passage by excluding “any areas of internal waters within a strait, except where the establishment of straight baselines ... has the effect of enclosing as internal waters areas which had not previously been considered as such.” The key question thus becomes whether or not the Northwest Passage was considered internal Canadian waters prior to Canada's application of straight baselines.

It is also unclear whether Article 234 of the UNCLOS applies to international straits, because the negotiators did not expressly deal with the issue. While Article 234 itself is written in broad manner that could encompass international straits, Article 42, which governs the “laws and regulations of states bordering straits relating to transit passage,” specifically limits itself “to the provisions of this section.” However, Article 42 then goes on to list pollution as an acceptable subject for regulation, although with a more limited scope. This lack of clarity in the UNCLOS creates additional potential for conflict over the legal status of the Northwest Passage. The UNCLOS also creates an additional loophole in pollution-related laws and regulations for military vessels used only in governmental, non-commercial service.

C. Relevant Prior Judgments from the International Court of Justice

While prior decisions of international tribunals are not binding precedent, those decisions are a “subsidiary means for the determination of rules of law.” The principles used by the I.C.J. in two cases have a direct bearing on the issues involved in the dispute over the Northwest Passage. These cases have been cited by both the United States and Canada in support of their respective positions.

I. The Norwegian Fisheries Case--Defining Appropriate Straight Baselines

The Norwegian Fisheries case was decided by the I.C.J. in 1951. It involved a dispute between the United Kingdom and Norway over fishing rights, in particular how the presence of Norway's “skjaergaard,” a collection of rocks, islands, and reefs, affected the delineation of Norwegian territorial waters through the drawing of straight baselines. The
United Kingdom disputed Norway's use of straight baselines to enclose the entire skjaergaard as territorial waters, instead arguing that the baselines must be drawn on the “low-water mark on permanently dry land which [was] a part of Norwegian territory, or the proper closing line of Norwegian internal waters.” The court rejected this contention, stating that geographic realities dictated that outer lines of the skjaergaard must be taken into account when delimiting Norwegian territorial waters.

The United Kingdom also argued that if baselines could be used, then each baseline could be no longer than ten nautical miles. This contention was also rejected by the I.C.J., which noted that while the ten-mile rule enjoyed a certain amount of support, it had “not acquired the authority of a general rule of international law.” The I.C.J. also refused to endorse any particular system of drawing baselines, instead noting that “the coastal State would seem to be in the best position to appraise the local conditions dictating the selection.”

Another pertinent point involved the United Kingdom's attempt to define portions of the waters in the skjaergaard as a strait, which would have prevented Norway from classifying them as internal waters. The United Kingdom argued that the portions followed by the Indreleia navigational route constituted a maritime strait. However, the I.C.J. noted that the Indreleia was more accurately described as “a navigational route prepared as such by means of artificial aids to navigation provided by Norway.” Given that, the I.C.J. declined to treat the Indreleia differently than the other waters of the skjaergaard.

After finding that the Norwegian government had not violated international law by drawing straight baselines, the I.C.J. then proceeded to expound on the characteristics of valid straight baselines under international law. The court first noted that land granted a coastal state the right to the waters off its coast. Thus, “while such a State must be allowed the latitude necessary in order to be able to adapt its delimitation to practical needs and local requirements, the drawing of base-lines must not depart to any appreciable extent from the general direction of the coast.” The court noted that a second consideration would be the relationship between “sea areas and the land formations which divide or surround them.” Finally, the court noted that considerations beyond “purely geographic” factors are valid, such as economic interests evidenced through historical usage.

After determining the basic rules of permissible baselines, the ICJ then examined how Norway had created its system, what effect Norway's system had against the United Kingdom, and whether it was applied in a way that conformed to international law. By using a variety of historical documents, the court established that Norway had established a coherent system for establishing baselines stretching back to 1812, and that this system had been encountered no opposition from other states. Furthermore, the United Kingdom's position in the North Sea, the United Kingdom's own interests, and the United Kingdom's failure to protest against early iteration of the Norwegian position justified enforcement against the United Kingdom.

When examining whether Norway's baselines conformed to international law, the I.C.J. gave great weight to Norway's historical claims that marginalized the United Kingdom's concerns that the baselines deviated too severely from the general direction of the Norwegian coast. Additionally, it found that the “vital needs of the population,” supported by “ancient and peaceful usage” could legitimately be taken into consideration when determining whether the baselines were “moderate and reasonable.” Taking all of its findings into consideration, the I.C.J. found that baselines drawn by Norway were permissible under international law.
2. The Corfu Channel Case--What is an International Strait

Decided in 1949, the Corfu Channel case involved a dispute between the United Kingdom and Albania. The case emerged from an incident in 1946 when a squadron of British warships departed from the port of Corfu and proceeded through the North Corfu Channel, where they struck mines. The mines were encountered while the British ships were transiting through Albanian territorial waters. A substantial portion of the Corfu Channel decision addressed the question of whether the Albanian government was responsible for the mines which had damaged the British warships and whether the court had jurisdiction to impose a penalty. It is, however, the second issue addressed by the Corfu Channel case that is relevant to the Northwest Passage dispute: whether the passage of British warships through the Corfu Channel violated Albanian sovereignty.

The Albanian government had previously claimed that foreign warships and merchant vessels had no right to pass through Albanian territorial waters without the prior notification and consent of the Albanian government. The British government vigorously protested this position, claiming that “innocent passage through straits [was] a right recognized by international law.” The I.C.J. found that it was “generally recognized and in accordance with international custom that States in time of peace have a right to send their warships through straits used for international navigation between two parts of the high seas without the previous authorization of a coastal state.” Further, the court stated that “[u]nless otherwise prescribed in an international convention, there is no right for a coastal State to prohibit such passage through straits in time of peace.”

The Albanian government did not contest this rule of international law directly, but instead attempted to argue that although the North Corfu Channel was geographically a strait, it did not qualify as an “international highway.” The Albanian position was based on the claim that the North Corfu Channel was of “secondary importance,” was not a “necessary route,” and that it was used almost exclusively for local traffic. The I.C.J. began its analysis by attempting to determine what factors were most important in determining whether a waterway was an international strait:

It may be asked whether the test is to be found in the volume of traffic passing through the Strait or in its greater or lesser importance for international navigation. But in the opinion of the Court the decisive criterion is rather its geographical situation as connecting two parts of the high seas and the fact of its being used for international navigation. Nor can it be decisive that this Strait is not a necessary route between two parts of the high seas, but only an alternative passage between the Egean (sic) and the Adriatic Seas.

In determining that the North Corfu Channel had been a useful route for international traffic, the I.C.J. referred to records showing that almost three thousand ships of various nationalities passed through the North Corfu Channel over a 21-month period. It also noted that the channel had been used regularly by the British for over eighty years and that other navies also used the Channel. The court then concluded that the “North Corfu Channel should be considered as belonging to the class of international highways through which passage cannot be prohibited by a coastal State in times of peace.”

III. The Northwest Passage Dispute

Despite the generally close relationship between the United States and Canada, the Northwest Passage has proven to be a source of contention between the two neighbors. Driven by national economic, security, and environmental
concerns, Canada seeks to establish its control and sovereignty over the waters of the Northwest Passage. As a practical matter, the United States shares many of Canada's concerns and in the past has been willing to work with the Canadian government to protect the Northwest Passage. In contrast, the United States is more concerned with the establishment of precedent that would allow other nations to close off or restrict navigational rights in other areas of the world.

A. Canada's Position Regarding the Northwest Passage

Canada's position is that the Northwest Passage is “internal waters” as defined by the UNCLOS in international law. Canada also asserts that their position is supported by the reasoning of the I.C.J. in the *Norwegian Fisheries* case. Beginning with Canada's 1906 declaration of sovereignty over the Northwest Passage, Canada has consistently maintained its sovereignty claim. However, the reasoning behind that claim has shifted over the years. Its initial claim in 1906 utilized a “sector” theory of delineation, claiming “everything within a pie-shaped sector extending from the continental coastline to the geographic North Pole.” The validity of this claim was never recognized internationally, and was eventually dropped by the Canadian government. Currently, Canada espouses two separate rationales for its claim of sovereignty over the Northwest Passage.

1. Canada's First Claim: Internal Waters by Historic Title

Canada attempts to support its own claim to the Northwest Passage by historic use, similar to how Norway established its claim in the *Norwegian Fisheries* case by establishing its historic use to the waterways within and surrounding the skjaergaard. Canadian legal scholars point to three centuries of exploration by British explorers, followed by the transfer of title from the United Kingdom to Canada in 1880. Canadian scholars also point to legislation enacted by the Canadian government in the early 1900s regulating various activities within the Arctic Archipelago and annual patrols conducted by the Royal Canadian Mounted Police. Noted Canadian legal scholar Donat Pharand has pointed out that the historical title claim has a serious flaw: none of the pre-1900 activities were combined with an explicit claim to the *waters* of the Northwest Passage, and the claims in the 1900's that did include such a claim were consistently opposed by the United States.

Canadian legal scholar Michael Byers has attempted to rectify the weaknesses in this claim by using the native Inuit's historical occupation of the Arctic Archipelago, who ranged over both the islands and the ice-covered waterways for hundreds of years. However, even Byers has noted that in order for this claim to succeed, Canada would need to establish that “(1) sea ice can be subject to occupancy and appropriation like land (2) under international law, indigenous people can acquire and transfer sovereign rights and (3) indigenous rights holders ceded such rights, if they did exist, to Canada.” The first element is the most problematic, as there is no support in international law for such a proposition.

Comparing the Canadian claim, that the Northwest Passage constitutes historic internal waters, with the situation in the *Norwegian Fisheries* case, it is clear that Norway possessed a much stronger historical claim to the skjaergaard than Canada does to the Northwest Passage. Norway's historical claim included nearly a century of expressed sovereignty over the waters of the skjaergaard, uncontested by other states. In contrast, Canada's express claims of sovereignty over the Northwest Passage were consistently challenged by the United States and other nations. Thus, Canada's historical internal waters claim is likely insufficient to establish that Canada should be allowed to classify the Northwest Passage as internal waters. Perhaps due to recognition of these weaknesses, Canada has sought other means to establish the
Northwest Passage as internal waters, although it has never explicitly dropped that claim as it did with its sector theory claim.

2. Canada’s Second Claim: Straight Baselines

Following the voyage of the United States Coast Guard icebreaker USCGC *Polar Sea* in 1985, the Canadian Minister for External Affairs announced the adoption of straight baselines around the entire Arctic Archipelago, to take effect on January 1, 1986. This claim was subject to official protest by the United States government. The European Community also protested Canada's use of straight baselines, stating that:

> The Member States acknowledge that elements other than purely geographical ones may be relevant for purposes of drawing baselines in particular circumstances but are not satisfied that the present baselines are justified in general.

Moreover, the Member States cannot recognize the validity of a historic title as justification for the baselines drawn in accordance with the order.

*186* The European Community further specified that it protested Canada's use of straight baselines on the basis that the baselines were “excessively long and diverted too much from the general direction of the mainland coast.”

Byers attempts to use the *Norwegian Fisheries* case as a justification for Canada's application of straight baselines to encompass the entire Arctic Archipelago and the Northwest Passage. However, Byers's argument depends on the inclusion of Canada's historic internal waters claim for validity. In the *Norwegian Fisheries* case, Norway's use of straight baselines to enclose the skjaergaard was justified because of Norway's long-standing historical use and the lack of protest by foreign states of Norway's sovereignty claim. Since historical use of the Northwest Passage is dependent on the dubious contention that Inuit use of surface ice can satisfy the usage requirement, Canada cannot establish that its claims of sovereignty were ever accepted by the international community.

The Canadian position regarding the length of their baselines appears to rest upon a misunderstanding of the *Norwegian Fisheries* case. In that case, the I.C.J. rejected the United Kingdom's contention that a 10-mile rule existed preventing certain baselines from being drawn absent a historical claim. However, the 10-mile rule rejected did not relate to the length of the baseline itself, but rather the distance from the baseline to a low-water mark.

When discussing the length of the baseline itself, the I.C.J. approved a baseline of 38.6 nautical miles in length. In contrast, Canada's baselines surrounding the Arctic Archipelago include baselines of nearly 100 miles in length. The extreme length of Canada's baselines makes their use questionable under international law. Unfortunately, the UNCLOS does not define the length of permissible baselines.

In addition, Canada's reliance on the *Norwegian Fisheries* case to justify its use of straight baselines also appears to ignore one significant difference between the Norwegian skjaergaard and the Northwest Passage. The Norwegian skjaergaard, and most of the waterways in question in *Norwegian Fisheries*, are fjords. The Merriam-Webster Dictionary defines “fjord” as “a narrow inlet of the sea between cliffs or steep slopes.” By definition, a fjord has only a single point of egress, as compared to a strait (or series of straits like the Northwest Passage) which has multiple points of egress.
Thus, while Canada's use of straight baselines may be permissible under the broadest reading of the UNCLOS, the length of those baselines and the lack of a historical basis recognized by other nations lends weight to the position of those nations that protest Canada's use of strait baselines to encompass the entire Arctic Archipelago. However, while it would be incorrect to state that international law supports the Canadian position, neither would it be correct to state that international law rejects the Canadian position. The geographically unique features of the Northwest Passage make analogizing to previous situations difficult.

B. The United States Position Regarding the Northwest Passage

The United States position is that the Northwest Passage constitutes an international strait between two high seas and that foreign shipping thus has the right of transit passage. This position rests on both the UNCLOS as a codification of customary international law and the clarification of customary international law by the I.C.J. in the Corfu Channel Case. The decisive characteristic of an international strait under both the UNCLOS and Corfu Channel is twofold: (1) the waterway must connect two high seas, and (2) it must be used for international navigation. Of those two factors, the only real area in dispute is whether the Northwest Passage satisfies the second factor of being used for international navigation.

1. How Much Use is Enough?

The question of use is difficult to resolve because historically the Northwest Passage has been commercially impassable due to surface ice. The few ships that did transit the Northwest Passage did so largely with Canadian permission, even if the ships involved did not actively seek Canadian permission. James Kraska, a U.S. Navy Judge Advocate General (JAG), attempted to sidestep the issue of use by writing:

There is nothing in the Law of the Sea Convention to suggest additional tests or requirements for recognition as an international strait, so there is no authority for the idea that a strait is only a strait if it meets a certain minimum threshold of shipping traffic, a specific number of transits, a timetable or regularity of transits, transit by certain types of vessels, or whether the vessel is accompanied or not accompanied by icebreakers.

Kraska's statement is technically correct, in that the UNCLOS does not set a minimum threshold of shipping traffic. However, the I.C.J.'s decision in Corfu Channel is often cited as justification for the existence of some sort of threshold. Pro-Canadian legal scholars point out that international shipping in the Northwest Passage falls far short of the 2,884 ships that transited the North Corfu Channel over a twenty-one-month period. However, Corfu Channel does not necessarily establish any kind of standard for satisfying the usage criteria of an international strait, because in that case, the evidence showing the 2,884 transits was entered to counter the assertion of the Albanian government that the North Corfu Channel was not used for international shipping. While Corfu Channel can serve to establish that some actual international shipping is required to qualify a strait as an international strait, it does not refute the assertion that a single transit of international shipping would qualify that strait as an international strait under the UNCLOS.

While satisfying the usage requirement of an international strait will likely require more use than a single transit, it is simply unclear as to how much use will be required. The situation becomes even more uncertain when the issue of submarines are added into the calculation. Several legal scholars believe that submarine navigation plays a key part in motivating the United States position.
passage may pass through the internal waters of coastal states; however, they are required to travel on the surface. \(^{147}\) When transiting through an international strait, submarines may remain submerged. \(^{148}\)

The passage of non-Canadian submarines through the Northwest Passage could potentially establish sufficient use to qualify it as an international strait. \(^{149}\) Unfortunately, it is difficult to determine whether such transits have occurred, because movements of U.S. Navy submarines are classified and unavailable to the public, as are any agreements or notifications which the Canadian government may have received. It is thus impossible to determine if submarine transits of the Northwest Passage have occurred in a manner that would satisfy the usage requirements of an international strait.

2. Has Canada Acquiesced to the Claim that the Northwest Passage is an International Strait?

The passage of submarines through the Northwest Passage also raises the issue of whether Canada has acquiesced to the United States position that the Northwest Passage constitutes an international strait. \(^{150}\) Under the general principles of international law, a nation's practice of acquiescence can create a binding *190 obligation. \(^{151}\) In addition, as a general principle of law and equity, principles of estoppel are also a valid part of international law. \(^{152}\)

The actions, or more specifically the lack of actions, taken by the Canadian government in regard to the submerged movements of submarines through the Northwest Passage creates the potential that Canada has acquiesced to the United States and European Community position that the Northwest Passage constitutes an international strait. In 1995, Canadian Defense Minister David Collenette stated publicly that the Canadian government acquiesced to the use of Canadian waters by U.S. submarines. \(^{153}\) However, Collenette later clarified this statement by saying that while there was no formal agreement, information on submarine activities was shared between Canada and its allies for the purposes of safety and minimizing interference. \(^{154}\) While not conclusive, these statements by a high-ranking Canadian official could be seen as an acknowledgement by Canada that it had acquiesced to the use of the Northwest Passage as an international strait by American submarines.

In addition, Canada has continually failed to take concrete action disputing the United States claim that the Northwest Passage is an international strait. NORDREG, Canada's registration system, established in 1977 under the AWPPA, is a voluntary registration system. 2% of international shipping fails to register with NORDREG without legal consequence. \(^{155}\) Canada does, however, have the capability to monitor shipping through the Northwest Passage, through its RADARSAT-2 satellite. \(^{156}\) Taken together, the Canadian government is able to detect potential challenges to its sovereignty claims by looking for unregistered traffic, but is unwilling to take *191 concrete steps to challenge ships that are utilizing the Northwest Passage in defiance of their sovereignty claim. This kind of inactivity could be considered acquiescence to the United States position that the Northwest Passage is an international strait, because Canada has failed to develop or exercise the capability to enforce its sovereignty claim.

3. Was the Northwest Passage an International Strait Prior to 1985?

While Canada's historical internal waters claim has weaknesses due to its reliance on the untested argument that indigenous peoples can claim title to sea ice, the United States strongest historical argument relies on the fact that Canada first utilized straight baselines in 1985. Article 35(a) of the UNCLOS states that the right of transit passage can still exist through an international strait that has been classified as internal waters, where the use of straight baselines “has the effect of enclosing as internal waters areas which had not previously been considered as such.” \(^{157}\) It is for this reason that the Canadian “historic internal waters” argument is so critical. Even if Canada's method of using straight baselines is found to be valid under international law, if the Northwest Passage was not considered internal waters prior to the
enactment of straight baselines in 1985, then international shipping would retain the right of transit passage through the Northwest Passage.  

The question then becomes whether Canada can establish its claim that the Northwest Passage constitutes historic internal Canadian waters. As discussed previously, this is problematic for Canada because explicit claims to the waters of the Northwest Passage were protested by the United States and other nations.  

Canada is therefore unable to point to widespread acceptance, by foreign states, of their claim that the Northwest Passage constitutes internal waters, a key factor in the I.C.J.'s *Norwegian Fisheries* judgment.

Canada's position would be greatly strengthened if native peoples could claim title to sea ice, but this proposition has never been tested in any international forum. The closest analogy would be an advisory opinion by the I.C.J. that ruled that indigenous nomadic peoples can claim title to land, by virtue of long-standing occupation and use. However, applying this advisory opinion to the Inuit in the Arctic Archipelago is difficult because of the changing nature of sea ice. In addition the *Western Sahara* decision did not specify what rights were gained by the nomadic peoples, only that the colonization by Spain was not a result of occupation *terra nullius*, but rather through agreements concluded with local rulers. While this basic principle could apply, it would require that (1) international law recognize that peoples can claim title to sea ice, and that (2) that title would transfer from sea ice to the waterway if the sea ice should melt. As this appears to be an entirely new principle of international law, Canada would need to convince other states to adopt these principles.

Thus, it is difficult for Canada to conclusively establish that, prior to the enactment of straight baselines in 1985 the Northwest Passage constituted internal Canadian waters. Without establishing this historical factor, Canada's use of straight baselines does not meet the standards established under customary international law. Unless they can do so, the waters of the Northwest Passage would likely be considered an international strait, with foreign vessels having the right of transit passage.

**C. Resolving the Northwest Passage Dispute Between the United States and Canada**

Given the nature of international law and international tribunals, it is unlikely that the United States and Canada will consent to placing this dispute before an international tribunal. Canadian concerns regarding its sovereignty and the weaknesses in the Canadian position make it unlikely that Canada would consent to having a third party determine the outcome. Similarly, weaknesses in the United States' position and the concern for setting an unfavorable precedent make it equally unlikely that the United States would consent to jurisdiction. In addition, the generally strong relationship between Canada and the U.S. and the likelihood that the United States and Canada have some sort of tacit agreement regarding usage of the Northwest Passage by U.S. Navy vessels reduces the impetus to quickly resolve this issue. Thus, both nations will likely be satisfied with the status quo and allow the present situation to continue.

However, should the United States ratify the UNCLOS, the dispute resolution provisions of Part XV would become relevant. While Section 1 of Part XV of the UNCLOS requires states to use peaceful means to achieve a settlement, Sections 2 and 3 set forth procedures for binding decisions. The binding decision provisions, however, are only invoked at the request of one of the parties. Given the close ties and shared concerns of Canada and the United States, and the unpredictability of the outcome, the likelihood that either nation would invoke the binding decision provisions is probably low.

Thus, the means for resolving this dispute would most likely be diplomatic and result in a document similar to the 1988 Arctic Cooperation Agreement. Due to the American priority of preserving freedom of navigation, any agreement
would likely contain provisions similar to those in the Arctic Cooperation Agreement which preserved the original positions of the United States and Canada. 170 Canada could likely gain significant control and oversight over maritime transit of the Northwest Passage through such an agreement, addressing its key concerns. 171 While not a final or perfect solution to the dispute regarding the Northwest Passage, such an agreement would likely be in the best interests of both nations and place minimal stresses on the relationship between the United States and Canada.

IV. Conclusion

Both the United States and Canada have weaknesses in their respective positions over the status of the Northwest Passage. Canada's claim that the Northwest Passage constitutes internal Canadian waters has never been accepted by the international community. In addition, their usage of straight baselines exceeds those previously accepted under international law, and their historical claim depends on a principle that has never previously been proposed: that indigenous peoples can gain and transfer title to sea ice. The United States position that the Northwest Passage constitutes an international strait relies on an extremely small number of movements to satisfy the usage characteristic of international straits and is not aided by the classified nature of submarine navigation. However, formal protests by the United States and other nations do preserve a fallback position: that even if Canada's use of straight baselines to claim the Northwest Passage as internal waters is acceptable under *194 international law, this would not preclude the right of transit passage due through the Northwest Passage due to the lack of valid historical claims.

As a practical matter, the close relationship between Canada and the United States means that the dispute over the Northwest Passage is unlikely to become a matter of serious contention between the two nations. Canada and the United States share significant concerns, including security, economic development, and environmental protection. However, these shared interests diverge greatly when the legitimate Canadian desire to exercise and protect its sovereignty clashes with the equally legitimate American need to protect free transit rights throughout the globe.

This dispute is unlikely to be put before an international tribunal that could issue a judgment unfriendly to either nation's interests. Thus, the most likely resolution to this dispute would be diplomatic, in a manner similar to the 1988 Agreement on Arctic Cooperation which provided the United States and Canada with a framework for operation of icebreakers in the Northwest Passage without unnecessarily compromising either nation's legal position. A similar agreement could satisfy Canada's need to protect its sovereignty and address its immediate environmental concerns, while ensuring that the United States could avoid creating the kind of international legal precedent that would jeopardize the principle of freedom of the seas.

Footnotes
1 J.D, Michigan State University College of Law.
2 ESA Portal--Satellites witness lowest Arctic ice coverage in history, ESA.INT, http://www.esa.int/esaCP/SEMYTC13J6F_index_0.html (last visited Dec. 6, 2010).
6 Id. at 42.

BYERS, supra note 5 at 36-37.

BYERS, supra note 5 at 37. All prior attempts to navigate the Arctic passage failed. Id.

See John Kennair, An Inconsistent Truth: Canadian Foreign Policy and the Northwest Passage, 34 VT. L. REV. 15, 23-24 (2009); Luke R. Peterson, International Strait or Internal Waters? The Navigational Potential of the Northwest Passage, PROCEEDINGS OF THE MARINE SAFETY COUNCIL, Summer 2009, at 44, 47. Both articles note that the Canadian government no longer attempts to use the sector theory to claim sovereignty over the Northwest Passage.

Peterson, supra note 12 at 47.


Dictionary of American Naval Fighting Ships: Seadragon II, HISTORY.NAVY.MIL, http://www.history.navy.mil/danfs/s8/seadragon-ii.htm (last visited Dec. 6, 2010). It is notable that this is one of the few instances where the course taken by a submarine is publicly available, since submarine operations are classified by the U.S. government and are thus generally unavailable. See, e.g. Byers & Lalond, supra note 3 at 1177.

BYERS, supra note 5 at 44-45.

BYERS, supra note 5 at 46.

BYERS, supra note 5 at 51.

Id. Byers also notes that Canada effectively admitted that these requirements violated international law at the time by taking steps to prevent the matter from being litigated at the I.C.J. Id.

Kennair, supra note 12 at 17.


Kennair, supra note 12 at 18.

BYERS, supra note 5 at 18.

Id. The Agreement on Arctic Cooperation also states that all icebreakers are also by definition research vessels, and both nations agreed to share information gained from the research activities of their icebreakers. Id.


Byers, supra note 5 at 70-71.

Id. at 71.

Id. at 71-72. A spokesperson for the United States embassy stated that “[w]e want to ensure that any enhanced protection of the Canadian Arctic marine environment is achieved in a manner that is consistent with the international law of the sea.” Id. at 72.


Byers, supra note 5 at 70-71.

Agreement on Arctic Cooperation, supra note 29.


Agreement on Arctic Cooperation, supra note 29.

Id. Paragraph 4 reads, “Nothing in this agreement of cooperative endeavor between Arctic neighbours and friends nor any practice thereunder affects the respective positions of the Governments of the United States and of Canada on the Law of the Sea in this or other maritime areas or their respective positions regarding third parties.” Id.


See, e.g. Letter from David Wilkins, Ambassador of the U.S., to Peter Boehm, Assistant Deputy Minister, N.Am., Dept't of Foreign Affairs & Int'l Trade (Can.) (Oct. 27, 2006), available at www.state.gov/documents/organization/98836.pdf (last visited Dec. 10, 2010); Kraska, supra note 4 at 263.


Sec. e.g. North Sea Continental Shelf, Merits (Ger./Neth.; Ger./ Den.), 1969 I.C.J. 2 (Feb. 20). The judgement in the North Sea Continental Shelf case discussed the manner in which a treaty, which had not been ratified by Germany, might still be considered to codify customary international law and thus bind Germany. Id. at 14-16.
UNCLOS, art. 8.

UNCLOS, art. 46. Essentially, states composed of a continental landmass with a nearby archipelago cannot be considered archipelagic states under the UNCLOS. Id.

UNCLOS, art. 7, para. 1.

BYERS, supra note 5 at 52.

BYERS, supra note 5 at 53-54.

UNCLOS, art. 7, para. 3.

UNCLOS, art. 2.

UNCLOS, art. 18.

Id.

UNCLOS, art. 19. Article 19 also lists a variety of actions incompatible with innocent passage, including researching, fishing, intelligence gathering, and the use or threat of use of force. Id. In addition, submarines must travel on the surface and identify themselves. UNCLOS, art. 20.

UNCLOS, art. 234. Article 234 is restricted to areas “where particularly severe climatic conditions and the presence of ice covering such areas for most of the year create obstructions or exceptional hazards to navigation.” Id.

See Kennair, supra note 12 at 17-18; Kraska, supra note 4 at 274.

Kennair, supra note 12 at 17-18

See, e.g. Peterson, supra note 12 at 46; Byers & Lalonde, supra note 3 at 1200-01. It is interesting to note that the scholars from Canada (Byers & Lalonde) and the United States (Peterson) have noted this uncertainty.

BYERS, supra note 5 at 42.

UNCLOS, art. 37.

UNCLOS, art. 38, para. 2.

UNCLOS, art. 38, para. 1-2.

UNCLOS, art. 40.

UNCLOS, art. 41.

UNCLOS, art. 42, para. 1.

UNCLOS, art. 42, para. 2.

UNCLOS, art. 44.

UNCLOS, art. 35(a). Article 36 of the UNCLOS also excludes international straits where an alternative route “of similar convenience with respect to navigational and hydrographical characteristics” exists. UNCLOS, art. 36. No such alternative route exists in relation to the Northwest Passage.

Byers & Lalonde, supra note 3 at 1182-83.

UNCLOS, art. 42.
UNCLOS, art. 42(1)(a). Article 42 allows the coastal state to give effect “to applicable international regulations regarding the discharge of oil, oily wastes, and other noxious substances.” Id. Article 234 does not include the restriction of “giving effect to applicable international regulations. UNCLOS, art. 234.

Kennair, supra note 12 at 18. Kennair notes that when the Canadian government attempted to use Article 234 of the UNCLOS to justify regulation of ships through the Arctic ice shelf, the United States government responded by pointing out that Article 236 of the UNCLOS provided a sovereign immunity clause. Id. This sovereign immunity clause specifically exempts military vessels from provisions of the UNCLOS regarding protection and preservation of the environment. UNCLOS, art. 236.


Id. at 21-23.

Id. at 24.

Id. at 25-26. The I.C.J. justified this decision by noting that the western sector of the mainland was bordered by the skjaergaard and thus constituted a whole with the mainland. Id. The I.C.J. later explicitly gave its sanction to Norway's drawing of baselines between the outer islands of the skjaergaard. Id. at 29.

Id. at 29-30.

Id. at 32.

Id. at 33.

Id. at 33-34.

Id. at 34.

Id.

Id.

Id. at 34-35. The I.C.J. noted that these characteristics, “though not entirely precise, can provide courts with an adequate basis for their decisions, which can be adapted to the diverse, facts in question.” Id. at 35.

Id. at 36.

Id. The court further clarified this point by stating that “[t]he real question raised in the choice of base-lines is ... whether certain sea areas lying within those lines are sufficiently closely linked to the land domain to be subject to the regime of internal waters.” Id.

Id. at 36-37.

Id. at 38.

Id. at 45.

Id. at 52.

Id. at 57-58.

Id. at 58-59.

Id. at 60.

Id. at 17-18.
Id. at 22-23.
Id. at 42.
Id. at 49.
Id. at 50.
Id.
Id. at 52.
Id.
Id. at 52-53.
Id.
Id. at 53.
Id. at 53-54.
Id. at 54.
Id. at 55. The I.C.J. did note, however, that because technically a state of war existed between Albania and its neighbor Greece, that Albania would have been justified in “issuing regulations in respect of the passage of warships through the Strait, but not in prohibiting such passage or in subjecting it to the requirement of special authorization. Id.


BYERS, supra note 5 at 59-60. Byers notes that during the Cold War the U.S. and Canada collaborated on the DEW line of radar stations stretching from Alaska to Greenland, as well as in the deployment of underwater surveillance systems around the Arctic archipelago. Id.

See Kraska, supra note 4 at 270. Kraska identifies the United States core interest as “freedom of navigation.” Id.

BYERS, supra note 5 at 43.
Id. at 43-44.


DUFRESNE, supra note 119 at 2-3.
See, e.g. BYERS, supra note 5 at 49.
Id.
Id. at 50.
Id.

Byers & Lalonde, supra note 3 at 1156.
126 Kraska, supra note 4 at 271.
127 Fisheries, supra note 79 at 48-49.
128 DUFRESNE, supra note 119 at 3.
129 MARITIME CLAIMS, supra note 14 at 96.
131 BYERS, supra note 5 at 53.
132 BYERS, supra note 5 at 54.
133 Fisheries, supra note 79 at 48-49.
134 Fisheries, supra note 79 at 31-32.
135 Fisheries, supra note 79 at 55.
136 BYERS, supra note 5 at 54.
139 See, e.g. UNCLOS, art. 37; Corfu Channel, supra note 99 at 53.
140 See, e.g. BYERS, supra note 5 at 54. Byers, a Canadian legal scholar, acknowledges that the Northwest passage “clearly connects two parts of the high seas, namely the Atlantic and Arctic oceans.” Id.
141 See, e.g. BYERS, supra note 5 at 11.
142 Peterson, supra note 12 at 48. For example, permission was granted preemptively for the voyage of the S.S. Manhattan in 1969 despite not being sought by either the United States government or the ship’s owners. BYERS, supra note 5 at 44-45.
143 Kraska, supra note 4 at 275.
144 BYERS, supra note 5 at 55. Byers correctly notes that this number only accounts for ships that had put into the port of Corfu and registered with customs agents, and did not include ships which transited the channel without stopping at Corfu. Id.
145 Corfu Channel, supra note 99 at 53-54.
147 UNCLOS, art. 20.
148 BYERS, supra note 5 at 75.
149 While Canada possesses four submarines, they are all diesel-electric boats of the Victoria class. Submarines-- Victoria Class, navy.forces.gc.ca, http://www.navy.forces.gc.ca/cms/1/1-a_eng.asp (last visited Dec. 11, 2010). As diesel-electric boats, Canada’s submarines lack the ability of nuclear-powered submarines to remain submerged indefinitely, preventing them from operating beneath the Arctic ice cap. BYERS, supra note 5 at 75. Nuclear-powered submarines such as those operated by the United States, United Kingdom, Russia, China, France, and India, do not have this limitation.
BYERS, supra note 5 at 76. Byers notes that if submarine passage through the Northwest Passage were conducted without Canadian knowledge, the failure of Canada to enforce its claim would be excused on the basis of ignorance. However, Byers also considers it likely that Canada has been aware of American, French, and British submarine movements and has at least tacitly consented to those movements. Id.

See, e.g. Right of Passage over Indian Territory, Judgment (Portugal v. India), 1960 ICJ 5, 13-14 (Apr. 12). In that case, the I.C.J. stated that having found that “a practice clearly established between two States, which was accepted by the Parties as governing the relations between them, the Court must attribute decisive effect to that practice.” Id.

See, e.g. Delimitation of the Maritime Boundary in the Gulf of Maine Area, Judgment (Can./U.S.), 1984 ICJ 4 (Oct. 12). Canada argued that acquiescence, in relation to the recognition of rights, “[o]ne government's knowledge, actual or constructive, of the conduct or assertion of rights of the other party to a dispute, and the failure of protest in the face of that conduct, involves a tacit acceptance of the legal position represented by the other Party's conduct or assertion of rights.” Id. at 131-32.

BYERS, supra note 5 at 76.

Id. at 76-77.

Id. at 70-71.

Id. at 66-67. Byers notes that the prospect of losing RADARSAT-2's monitoring capabilities motivated the Canadian government to maintain RADARDSAT-2 as a vital Canadian asset. Id. at 67.

UNCLOS, art. 35(a).

UNCLOS, art. 35(a); see, e.g. Kennair, supra note 12 at 27; Kraska, supra note 130 at 1122.

See supra Part III(a)(1).


Id.

See supra section 0

See supra note 116 and accompanying text.

See supra note 150 and accompanying text.

UNCLOS, Part XV.

Id.

Id., Art. 286.

See, e.g. BYERS, supra note 5 at 78-80; Kennair, supra note 12 at 30-31; Kraska, supra note 4 at 267.

See Agreement on Arctic Cooperation, supra note 29.

See id. at Art. 4; see also supra note 150 and accompanying text.

See supra note 114 and accompanying text.

38 CUSLJ 167
SENATE ADVICE AND CONSENT
TO THE LAW OF THE SEA CONVENTION
Urgent Unfinished Business

Testimony of

John Norton Moore

Before the Senate Foreign Relations Committee
October 14, 2003
SENATE ADVICE AND CONSENT
TO THE LAW OF THE SEA CONVENTION

Testimony delivered by

John Norton Moore*

*The day is within my time as well as yours,
when we may say by what laws other nations
shall treat us on the sea.®

Thomas Jefferson

CHAIRMAN RICHARD G. LUGAR AND HONORABLE MEMBERS OF THE FOREIGN RELATIONS COMMITTEE --

Senate advice and consent to the 1982 Law of the Sea Convention is strongly in the national interest of the United States. Ratification of the Convention will restore United States oceans leadership, protect United States oceans interests, and enhance United States foreign policy. For these reasons the Convention is broadly supported by United States oceans organizations, including the United States Navy (one of the strongest supporters over the years), the National Ocean Industries Association1, the United States Outer Continental Shelf Policy Committee2, the American Petroleum Institute3, the Chamber of Shipping of

1On June 6, 2001, the National Ocean Industries Association submitted a resolution to the Chairman of the Senate Foreign Relations Committee declaring: [T]he National Ocean Industries Association (NOIA) is writing to urge your prompt consideration of the Convention on the Law of the Sea . . . . The NOIA membership includes companies engaged in all aspects of the Outer Continental Shelf oil and natural gas exploration and production industry. This membership believes it is imperative for the Senate to act on the treaty if the U.S. is to maintain its leadership role in shaping and directing international maritime policy.®

2On May 24, 2001, the Outer Continental Shelf (OCS) Policy Committee adopted the following recommendation: [T]he OCS Policy Committee recommends that the Administration communicate its support for ratification of UNCLOS to the United States Senate . . . . ®

3See the statement of Ms. Genevieve Laffly Murphy on behalf of the American Petroleum Institute at the recent oceans forum of the Center for Oceans Law and Policy, Oct. 1, 2003. Ms. Murphy stressed the energy security interest of the American petroleum industry both in access to the continental shelf beyond 200 miles and in protection of navigational freedom. See also the letter from the president of the American Petroleum Institute to the Chairman of the Senate Committee on Foreign Relations of October 1, 1996, which states: "The American Petroleum Institute wishes to express its support for favorable action by the
Urgent Unfinished Business

America\(^4\), The Center for Seafarers' Rights\(^5\), the Chemical Manufacturers Association\(^6\), and the congressionally established National Commission on Ocean Policy.\(^7\) This testimony will briefly explore reasons for United States adherence to the Convention. First, however, it will set out a brief overview of the Nation’s oceans interests and history of the Convention.

**Background of the Convention**

As the quote by Thomas Jefferson illustrates, the United States, surrounded by oceans and with the largest range of oceans interests in the world, has a vital national interest in the legal regime of the sea. Today those interests include naval mobility, navigational freedom for commercial shipping, oil and gas from the

---

4 In a letter to the Chairman of the Senate Foreign Relations Committee of May 26, 1998, the president of the Chamber of Shipping of America writes: "[t]he Chamber of Shipping represents 14 U.S. based companies which own, operate or charter oceangoing tankers, container ships, and other merchant vessels engaged in both the domestic and international trades. The Chamber also represents other entities which maintain a commercial interest in the operation of such oceangoing vessels. Over the past quarter century, the Chamber has supported the strong leadership role of the United States in the finalization of the UN Convention on the Law of the Sea (UNCLOS) into its final form, including revision of the deep seabed mining provision. We believe the United States took such a strong role due to its recognition that UNCLOS is of critical importance to national and economic security, regarding both our military and commercial fleets. … Mr. Chairman, we appreciate your consideration of these issues and strongly urge you to place the ratification of UNCLOS on the agenda of your Committee. The United States was a key player in its development and today, is one of the few industrialized countries who have not yet ratified this very important Convention. The time is now for the United States to retake its position of leadership."

5 On May 26, 1998, the Director of the Center for Seafarers' Rights wrote the following in a letter addressed to the Chairman of the Senate Foreign Relations Committee: "The 1982 United Nations Convention on the Law of the Sea creates a legal framework that addresses a variety of interests, the most important of which is protecting the safety and well-being of the people who work and travel on the seas. I urge you to support ratification of the 1982 United Nations Convention on the Law of the Sea."

6 In a July 17, 1998 letter to the Chairman of the Senate Foreign Relations Committee, the President of the Chemical Manufacturers Association wrote the following: "The Law of the Sea Convention promotes the economic security of the United States by assuring maritime rights of passage. More importantly, the Convention establishes a widely-accepted, predictable framework for the protection of commercial interests. The United States must be a full party to the Convention in order to realize the significant benefits of the agreement; and to influence the future implementation of UNCLOS at the international level. On behalf of the U.S. chemical industry, I strongly encourage you to schedule a hearing on UNCLOS, and favorably report the Convention for action by the Senate."

7 On November 14, 2001, the National Commission on Ocean Policy adopted a resolution B its first on any subject -- providing: The National Commission on Ocean Policy unanimously recommends that the United States of America immediately accede to the United Nations Law of the Sea Convention. Time is of the essence if the United States is to maintain its leadership role in the ocean and coastal activities. Critical national interests are at stake and the United States can only be a full participant in upcoming Convention activities if the country proceeds with accession expeditiously. @
Urgent Unfinished Business

continental margin, fishing, freedom to lay cables and pipelines, environmental protection, marine science, mineral resources of the deep seabed, and conflict resolution. Consistent with these broad interests the United States has been resolute in protecting its ocean freedoms. Indeed, the Nation has fought at least two major wars to preserve navigational freedoms; the War of 1812 and World War I. In point II of his famous 14 Points at the end of World War I, Woodrow Wilson said we should secure absolute freedom of navigation upon the seas . . . alike in peace and in war. And the Seventh Point of the Atlantic Charter, accepted by the Allies as their common principle for the post World War II world, provided such a peace should enable all men to traverse the high seas and oceans without hindrance.

In the aftermath of World War II the United States provided leadership in the First and Second United Nations Conferences to seek to protect and codify our oceans freedoms. The first such conference, held in 1958, resulted in four Geneva Conventions on the Law of the Sea which promptly received Senate Advice and Consent. One of these, the Convention on the Continental Shelf, wrote into oceans law the United States innovation from the 1945 Truman Proclamation -- that coastal nations should control the oil and gas of their continental margins. During the 1960's a multiplicity of illegal claims threatening United States navigational interests led to a United States initiative to promote agreement within the United Nations on the maximum breadth of the territorial sea and protection of navigational freedom through straits. This, in turn, led some years later, and with a broadening of the agenda, to the convening in 1973 of the Third United Nations Conference on the Law of the Sea. In this regard it should be clearly understood that the United States was a principal initiator of this Conference, and it was by far the preeminent participant in shaping the resulting Convention. Make no mistake; the United States was not participating in this Conference out of some fuzzy feel good notion. Its participation was driven at the highest levels in our Government by an understanding of the critical national interests in protecting freedom of navigation and the rule of law in the world = oceans. Today we understand even more clearly from public choice theory, which won the Nobel Prize in economics, why our choice to mobilize in a multilateral setting all those who benefited from navigational freedom was a sound choice in controlling individual illegal oceans claims. And the result was outstanding in protecting our vital

---

8 The reason supporting this is most easily understood as the high cost of organization of those affected by illegal oceans claims; claims which were externalizing costs on the international community. A multilateral strategy of response to such
Urgent Unfinished Business

Navigational and security interests. Moreover, along the way we solidified for the United States the world's largest offshore resource area for oil and gas and fishery resources over a huge 200 nautical mile economic zone, and a massive continental shelf going well beyond 200 miles. 9

Despite an outstanding victory for the United States on our core security and resource interests a lingering dispute remained with respect to the regime to govern resource development of the deep seabed beyond areas of national jurisdiction. Thus, when the Convention was formally adopted in 1982, this disagreement about Part XI of the Convention prevented United States adherence. Indeed, during the final sessions of the Conference President Reagan put forth a series of conditions for United States adherence, all of which required changes in Part XI. Following adoption of the Convention without meeting these conditions, Secretary Rumsfeld served as an emissary for President Reagan to persuade our allies not to accept the Convention without the Reagan conditions being met. The success of the Rumsfeld mission set the stage some years later for a successful renegotiation of Part XI of the Convention. In 1994, Part XI, dealing with the deep seabed regime beyond national jurisdiction, was successfully renegotiated meeting all of the Reagan conditions and then some. Subsequently, on October 7, 1994, President Clinton transmitted the Convention to the Senate for advice and consent. 10 Since that time no Administration, Democratic or Republican, has opposed Senate advice and consent and United States ratification.

Illegal claims, far from being simply a fuzzy effort at cooperation, effectively enabled coordination of nations to promote the common interest against such illegal claims. Counter to the perception of some that a unilateral U.S. response is always the best strategy, a multilateral forum was indeed the most effective forum for controlling such threats to our navigational freedom. Moreover, since a majority of coastal nations are completely zone locked, that is, they have no access to the oceans without traversing the 200 mile economic zones of one or more neighboring states, a multilateral strategy continues to offer an important forum for rebutting illegal unilateral oceans claims threatening navigational freedom. The fact is, because of this “zone locked” geography, a majority of nations should never either favor extending national jurisdiction beyond 200 nautical miles nor permitting interference with navigational freedom in the 200 nautical mile economic zone.

9 The Convention powerfully supports United States control of its fisheries resources. Indeed, with respect to fisheries, the United States is already a party to the “Agreement for the Implementation of the Provisions of the United Nations Convention on the Law of the Sea of 10 December 1982 Relating to the Conservation and Management of Straddling Fish Stocks and Highly Migratory Fish Stocks,” a treaty that implements certain fisheries provisions of the Law of the Sea Convention. Senator Ted Stevens provided crucial leadership in Senate advice and consent to this implementing Convention.

At present the Convention is in force; and with 143 states parties it is one of the most widely adhered conventions in the world. Parties include all permanent members of the Security Council but the United States, and all members of NATO but the United States, Denmark and Canada and Canada is expected to join in the immediate future as soon as the European Union formally adopts an important fisheries agreement implementing the 1982 Convention. The Convention unequivocally and overwhelmingly meets United States national interests indeed, it is in many respects a product of those interests.

If one were to travel back in time and inform the high-level members of the eighteen agency National Security Council Interagency Task Force which formulated United States oceans policy during the Convention process an effort never matched before or since in the care with which it reviewed United States international oceans interests that the Convention today in force, powerfully meeting all United States oceans interests, would not yet be in force for the United States nine years after being submitted to the Senate, the news would have been received with incredulity. As this suggests, the Senate should understand that United States oceans interests, including our critical security interests, are being injured and will continue to be injured until the United States ratifies the Convention. Among other costs of non-adherence we have missed out on the formulation of the mining code for manganese nodules of the deep seabed; we have missed participating in the development of rules for the International Law of the Sea Tribunal and the Commission on the Limits of the Continental Shelf, and in ongoing consideration of cases before the Tribunal as well as ongoing consideration of the Russian continental shelf claim now before the Continental Shelf Commission; we have had reduced effect in the ongoing struggle to protect navigational freedom and our security interests against unilateral illegal claims; and we have been unable to participate in the important forum of Convention States Parties.

Why should the United States give advice and consent to the Law of the Sea Convention? I will summarize the most important reasons under three headings:
Urgent Unfinished Business

I. 
Restoring United States Oceans Leadership

Until our prolonged non-adherence to the 1982 Convention, the United States has been the world leader in protecting the common interest in navigational freedom and the rule of the law in the oceans. We have at least temporarily forfeited that leadership by our continued non-adherence. United States ratification of the Convention will restore that leadership. Specifically, ratification will have the following effects, among others:

$ The United States will be able to take its seat on the Council of the International Seabed Authority. The authority is currently considering a mining code with respect to polymetallic sulfides and cobalt crusts of the deep seabed. Council membership will also give us important veto rights over distribution of any future revenues from deep seabed exploitation to national liberation groups;

$ The United States should, at the next election of judges for the International Tribunal for the Law of the Sea, see the election of a United States national to this important tribunal. Since this Tribunal frequently considers issues relating to navigational freedom and the character of the 200 mile economic zone it is a crucial forum for the development of oceans law;

$ The United States should, at the next election of members of the Commission on the Limits of the Continental Shelf, see the election of a United States expert to the Commission. This Commission is currently considering the Russian claim in the Arctic that is of real importance for the United States (and Alaska) and for appropriate interpretation of the Convention respecting continental margin limits. Over the next few years the Commission will begin to consider many other shelf limit submissions, beginning next with Australian and Brazilian claims. This is also the Commission that ultimately must pass on a United States submission as to the outer limits of our continental shelf beyond 200 nautical miles. The early work of the Commission, as it begins to develop its rules and guidelines, could significantly affect the limits of the United States continental shelf.
Urgent Unfinished Business

Not to actively participate in the work of this Commission could result in a loss of thousands of square kilometers of resource-rich United States continental shelf;

$ The United States will be able to participate fully in the annual meeting of States Parties that has become an important forum for ongoing development of oceans law. Of particular concern, United States presence as a mere observer in this forum has in recent years led to efforts by some to roll back critical navigational freedoms hard won in the LOS negotiations where we were a leader in the negotiations and our presence was powerfully felt; and

$ The United States will be far more effective in leading the continuing struggle against illegal oceans claims through our participation in specialized agencies such as the International Maritime Organization; in bilateral negotiations such as those with the archipelagic states; in acceptance by other states of our protest notes and our ability to coordinate such notes with others; and generally in organizing multilateral opposition to threats to our oceans interests and the rule of law in the oceans.

II. Protecting United States Oceans Interests

A second set of important reasons for United States adherence to the Law of the Sea Convention relate to the particularized protection of United States oceans interests. Some of the more important and immediate of these include:

$ More effectively engaging in the continuing struggle to protect our naval mobility and commercial navigational freedom. Protecting the ability of the United States Navy to move freely on the world’s oceans and the ability of commercial shipping to bring oil and other resources to the United States and for us to participate robustly in international trade overwhelmingly carried in ships is the single most important
oceans interest of the United States. This interest, however, is also the single most threatened interest; the continuing threat being the historic pattern of unilateral illegal oceans claims. As of June 22, 2001, there were at least 136 such illegal claims.\footnote{The best general discussion of these illegal oceans claims and their effect on United States interests is J. Ashley Roach \\& Robert W. Smith, Excessive Maritime Claims, 66 U.S. Naval War College International Law Studies (1994), and J. Ashley Roach \\& Robert W. Smith, United States Responses to Excessive Maritime Claims (2d ed. 1996).} This struggle has been the key historic struggle for the United States over the last half century and gives every indication of continuing. Adhering to the Convention provides numerous ways for the United States to engage more effectively in protecting these interests. An immediate and important effect is that we are able on ratifying the Convention to attach a series of crucial understandings under Article 310 of the Convention as to the proper interpretation of the Convention, as have many other nations too many of which have made erroneous interpretations as yet unrebutted by United States statements.\footnote{United States understandings under Article 310 could either be formulated and attached to the Convention by the Executive Branch at the time the United States ratifies the Convention or they could be attached to the Resolution of Senate Advice and Consent. I believe the second of these alternatives would have the greatest effect in the ongoing struggle for law as to the correct interpretation of the Convention. Given the highly technical nature of these understandings I would be pleased to work with the Committee to provide a draft of understandings for your consideration. It should be clearly understood that these are not reservations altering the correct legal meaning of the Convention. Such reservations or exceptions are barred by Article 309 of the Convention except as specifically permitted by the Convention, as, for example, in Article 298 of the Convention concerning optional exceptions to the compulsory dispute settlement provisions.} Moreover, as a party we will be far more effective in multiple fora in protecting the many excellent provisions in the Convention supporting navigational freedom. Indeed, much of the struggle in the future to protect our vital oceans interests will be in ensuring adherence to the excellent provisions in the Convention. Having won in the struggle to protect these interests within UNCLOS we now have a substantial advantage in the continuing struggle -- we need only insist that others abide by the nearly universally accepted Convention. Obviously, that is an advantage largely thrown away when we ourselves are not a party. And for our commercial shipping we will be able to utilize the important Article 292 to obtain immediate International Tribunal engagement for the release of illegally seized United States vessels and crew. It should be emphasized that the threat from these illegal claims is that of death from a thousand pin pricks rather than any single incident in response to which the United States is likely to be
Urgent Unfinished Business

willing to employ the military instrument. Moreover, some of the offenders may even be allies of the United States, our NATO partners, or even over zealous officials in our own country who are unaware of the broader security interests of the Nation;

More effective engagement with respect to security incidents and concerns resulting from illegal oceans claims by others. Examples include the new law of the People’s Republic of China (PRC) providing that Chinese civil and military authorities must approve all survey activities within the 200 mile economic zone, the PRC harassment of the Navy’s ocean survey ship the *USNS Bowditch* by Chinese military patrol aircraft and ships when the *Bowditch* was 60 miles off the coast, the earlier EP-3 surveillance aircraft harassment, Peruvian challenges to U.S. transport aircraft in the exclusive economic zone, including one aircraft shot down and a second incident in which two U.S. C-130s had to alter their flight plan around a claimed 650 mile Peruvian flight information area, the North Korean 50 mile security zone claim, the Iranian excessive base line claims in the Persian/Arabian Gulf, the Libyan line of death, and the Brazilian claim to control warship navigation in the economic zone;

More rapid development of the oil and gas resources of the United States continental shelf beyond 200 nautical miles. The United States oil and gas industry is poised in its technology to begin development of the huge continental shelf of the United States beyond 200 miles (approximately 15% of our total shelf). But uncertainties resulting from U.S. non-adherence to the Convention will delay the substantial investment necessary for development in these areas. Moreover, U.S. non-adherence is causing the United States to lag behind other nations, including Russia, in delimiting our continental shelf. Delimitation of the shelf is an urgent oceans interest of the United States;\(^{13}\)

\(^{13}\) For a state-of-the-art assessment of the extent of the United States continental shelf beyond the 200 mile economic zone see the work of Dr. Larry Mayer, the Director of the Center for Coastal and Ocean Mapping at the University of New Hampshire. As but one example indicating the great importance of performing this delimitation of the shelf well and the importance of the United States participating in the resulting approval process in the Commission on the Limits of the Continental Shelf Dr. Mayer’s work shows that sophisticated mapping and analysis of the shelf would enable the United States to claim an additional area off New Jersey within the lawful parameters of Article 76 of the Convention of approximately 500 square kilometers just by using a system of connecting seafloor promontories. The work of Dr. Mayer has been funded in part
Urgent Unfinished Business

- Reclaiming United States deep seabed mineral sites now virtually abandoned. United States firms pioneered the technology for deep seabed mining and spent approximately $200 million in claiming four first-generation sites in the deep seabed for the mining of manganese nodules. These nodules contain attractive quantities of copper, nickel, cobalt and manganese and would be a major source of supply for the United States in these minerals. Paradoxically, protecting our deep seabed industry has sometimes been a mantra for non-adherence to the Convention. Yet because of uncertainties resulting from U.S. non-adherence these sites have been virtually abandoned and most of our nascent deep seabed mining industry has disappeared. Moreover, it is clear that without U.S. adherence to the Convention our industry has absolutely no chance of being revived. I believe that as soon as the United States adheres to the Convention the Secretary of Commerce should set up a working group to assist the industry in reclaiming these sites. This working group might then recommend legislation that would deal with the industry problems in reducing costs associated with reacquiring and holding these sites until deep seabed mining becomes economically feasible;

- Enhancing access rights for United States marine scientists. Access for United States marine scientists to engage in fundamental oceanographic research is a continuing struggle. The United States will have a stronger hand in negotiating access rights as a party to the Convention. As one example of a continuing problem, Russia has not honored a single request for United States research access to its exclusive economic zone in the Arctic Ocean from at least 1998, and the numbers of turn-downs for American ocean scientists around the world is substantial. This problem could become even more acute as the United States begins a new initiative to lead the world in an innovative new program of oceans exploration;

$\text{Facilitating the laying of undersea cables and pipelines. These cables, through an innovative forward-looking grant supported by Senator Judd Gregg of New Hampshire. This work, however, is important for the Nation as a whole, and particularly for Alaska, which has by far the largest shelf beyond the 200 mile economic zone.}$
carrying phone, fax, and internet communications, must be able to transit through ocean jurisdictions of many nations. The Convention protects this right but non-adherence complicates the task of those laying and protecting cables and pipelines; and

$\text{It should importantly be noted in protecting United States oceans interests that no U.S. oceans interest is better served by non-adherence than adherence.} \text{ This is an highly unusual feature of the 1982 Convention. Most decisions about treaty adherence involve a trade off of some interest or another. I am aware of no such trade off with respect to the 1982 Convention. United States adherence is not just on balance in our interest it is broadly and unreservedly in our interest.}$

III. \textit{Enhancing United States Foreign Policy}

The United States would also obtain substantial foreign policy benefits from adhering to the 1982 Convention; benefits going quite beyond our oceans interests. These benefits include:

$\text{Supporting the United States interest in fostering the rule of law in international affairs.} \text{ Certainly the promotion of a stable rule of law is an important goal of United States foreign policy. A stable rule of law facilitates commerce and investment, reduces the risk of conflict, and lessens the transaction costs inherent in international life. Adherence to the Law of the Sea Convention, one of the most important law-defining international conventions of the Twentieth Century, would signal a continuing commitment to the rule of law as an important foreign policy goal of the United States;}$

$\text{United States allies, almost all of whom are parties to the Convention, would welcome U.S. adherence as a sign of a more effective United States foreign policy. For some years I have chaired the United}$
Urgent Unfinished Business

Nations Advisory Panel of the Amerasinghe Memorial Fellowship on the Law of the Sea in which the participants on the Committee are Permanent Representatives to the United Nations from many countries. Every year our friends and allies ask when we will ratify the Convention and they express their puzzlement to me as to why we have not acted sooner. In my work around the world in the oceans area I hear this over and over -- our friends and allies with powerful common interests in the oceans are astounded and disheartened by the unilateral disengagement from oceans affairs that our non-adherence represents;

$\text{Adherence would send a strong signal of renewed United States presence and engagement in the United Nations, multilateral negotiation, and international relations generally. At present those who would oppose United States foreign policy accuse the United States of unilateralism or a self-proclaimed American exceptionalism. Adhering to the Law of the Sea Convention will demonstrate that America adheres to those multilateral Conventions which are worthy while opposing others precisely because they do not adequately meet community concerns and our national interest;}

$\text{Efforts to renegotiate other unacceptable treaties would receive a boost when an important argument now used by other nations against such renegotiation with us was removed. This argument, now used against us, for example in the currently unacceptable International Criminal Court setting, is: Why renegotiate with the United States when the LOS renegotiation shows the U.S. won’t accept the Treaty even if you renegotiate with them and meet all their concerns? and finally}

$\text{The United States would obtain the benefit of third party dispute settlement in dealing with non-military oceans interests. The United States was one of the principal proponents in the law of the sea negotiations for compulsory third party dispute settlement for resolution of conflicts other than those involving military activities. We supported such mechanisms both to assist in conflict resolution}$
generally and because we understood that third party dispute resolution was a powerful mechanism to control illegal coastal state claims. Even the Soviet Union, which had traditionally opposed such third party dispute settlement, accepted that in the law of the sea context it was in their interest as a major maritime power to support such third party dispute settlement.\textsuperscript{14}

**Conclusion**

Senate advice and consent to the 1982 Convention on the Law of the Sea is strongly in the national interest of the United States. There are powerful reasons supporting United States adherence to the Convention; reasons rooted in restoring U.S. oceans leadership, protecting U.S. oceans interests, and enhancing U.S. foreign policy. I would urge the Senate to support advice and consent to the 1982 Convention at the earliest possible time.

\textsuperscript{14}The 1994 submission of the LOS Convention to the Senate recommended that the United States accept "special arbitration for all the categories of disputes to which it may be applied and Annex VII arbitration [general arbitration] for disputes not covered by … [this]." and that we elect to exclude all three categories of disputes excludable under Article 298." See U.S. Department of State Dispatch IX (No. 1 Feb. 1995).
About John Norton Moore

*John Norton Moore is the Walter L. Brown Professor of Law at the University of Virginia School of Law and Director of the Center for Oceans Law and Policy and the Center for National Security Law. He formerly served as the Chairman of the National Security Council Interagency Task Force on the Law of the Sea, which formulated United States international oceans policy for the law of the sea negotiations, he headed D/LOS, the office which coordinated both State Department and Interagency Policy on the law of the sea, and he served in the international negotiation as a Deputy Special Representative of the President and a United States Ambassador to the Third United Nations Conference on the Law of the Sea. Subsequently, he chaired the Oceans Policy Committee of the Republican National Committee and was a member of the National Advisory Committee on Oceans and Atmosphere (NACOA). In 1982, before the successful renegotiation of Part XI of the Treaty, he wrote to the incoming Reagan Administration opposing United States adherence until the problems with Part XI had been resolved. This letter was instrumental in triggering the Reagan review which in turn led to the successful Rumsfeld mission and ultimately effective renegotiation of Part XI.
THE FIFTH
SHABTAI ROSENNE
MEMORIAL LECTURE

The United Nations Convention on the Law of the Sea:
One of the Greatest Achievements in the International
Rule of Law

The United Nations, New York
ECOSOC Chamber

November 18, 2015

Delivered by

John Norton Moore
THE FIFTH
SHABTAI ROSENNE MEMORIAL LECTURE
November 18, 2015
UN ECOSOC Chamber, New York City
Delivered by
John Norton Moore

I.
Expression of Appreciation

His Excellency Ambassador David Roet, the Deputy Permanent Representative of Israel to the United Nations, His Excellency Miguel de Serpa Soares, the Under-Secretary-General for Legal Affairs of the United Nations, distinguished guests, and ladies and gentlemen:

Ambassador Shabtai Rosenne was a singular individual—a member of the British Royal Air Force in the fight against fascism, one of the creators of the State of Israel, a distinguished diplomat for Israel, and an eminent international lawyer and scholar. As a friend of Shabtai it is an honor and a pleasure for me to deliver this Memorial Lecture. I will deliver it on the United Nations Law of the Sea Convention, a subject of great interest for Ambassador Rosenne.

Before beginning the lecture, however, a word of appreciation for those who have arranged this lecture, and then a few words about Shabtai.

Thanks are due to Alan Stephens as Ambassador Rosenne’s Literary Editor, the United Nations Law of the Sea Office (DOALOS), The Israel Mission to the U.N., and Brill-Nijhoff Publishers. Thank you, not only for inviting me to deliver this distinguished lecture, but for the very fitting creation of this lecture series honoring one of the greatest international lawyers.

Shabtai Rosenne was one of those exceptional larger-than-life individuals who achieved enough for three lifetimes. He fought the ultimate evil of the Nazis in World War II as a member of the British Royal Air Force from 1940 to 1946. Subsequently, he worked in the Jewish Agency in London and Jerusalem, and as the British Mandate was ending he was appointed to

1 There is a brief bibliography for John Norton Moore at the end of this lecture. The views expressed are solely those of Professor Moore.
the Legal Secretariat of the Situation Committee where he helped create the new State of Israel. Surely that was enough historic contribution for any one individual.

But Shabtai went on to become a distinguished diplomat for Israel and one of the top international lawyers in the world. Thus, he served as the Legal Adviser to the Foreign Ministry of Israel from 1948 to 1967. Subsequently, as an Ambassador of Israel he served as the Deputy Permanent Representative of Israel to the United Nations in New York from 1967 to 1971, and as Israel’s Permanent Representative to the United Nations and other international organizations in Geneva from 1971 to 1974.

As to his credentials as an international lawyer, Shabtai wrote seminal works on three of the four most important law-making treaties in history; The World Court, The Vienna Convention on the Law of Treaties, and the United Nations Convention on the Law of the Sea. He was a member of the Permanent Court of Arbitration in The Hague, he was a member of the Institute of International Law, and he lectured at The Hague Academy of International Law, as well as the Rhodes Academy of Oceans Law & Policy. He taught international law at Cambridge, Amsterdam, Bar Ilan, and Virginia, among other distinguished Universities. And he was awarded the Israel Prize in Jurisprudence, the Manley O. Hudson Medal, The Hague Prize for International Law, and the Distinguished Onassis Scholar Award, as well as becoming an Honorary President of the American Society of International Law, among other top awards in international law. To review a bibliography of his works, written over almost seven decades from 1944 to 2012, reveals an enormously sophisticated and knowledgeable expert on the United Nations, the International Court of Justice, arbitration, the law of treaties, *jus ad bellum, jus in bello*, the law of the sea, recognition, state responsibility, the influence of Judaism on the development of international law, the International Criminal Court, and so many other subjects that his writings were virtually an encyclopedia of international law.

As befitting this lecture in his honor, Shabtai was also an important diplomat and scholar in the international law of the sea. He studied naval law in his first law degree at the University of London. He was the Vice-Chairman of the Israel Delegation to the First and Second United Nations Conferences on the Law of the Sea in 1958 and 1960. He was Chairman of the Israel Delegation to the Third United Nations Conference on the Law of the Sea from 1973 to 1982, and he served as a member of the UNCLOS Drafting Committee. Subsequently, he was one of the principal editors of the “*Virginia Commentary*” 7-volume series on the Law of the Sea, a work generally recognized as the most authoritative source for the *travaux* and interpretation of the Law of the Sea Convention,\(^2\) and he lectured at the Rhodes Academy of Oceans Law in Rhodes, Greece.

Finally, a word about my friendship with Shabtai. I first met Ambassador Rosenne while a young professor at the University of Virginia when I was putting together the first scholarly collection of documents on what was then called “The Arab-Israeli Dispute.” During my work on that project I sought out Ambassador Rosenne, who was at that time the Deputy Permanent

---

Representative of Israel to the United Nations in New York. Shabtai was enormously helpful and the final collection of documents, even before publication, was used by Secretary of State Henry Kissinger in his successful shuttle diplomacy. I then had occasion to work with Shabtai when I was a United States Ambassador to the Law of the Sea Negotiations while he headed the Israel Delegation. Because of my great respect for Shabtai as a person, and as a scholar, I invited him to Virginia to serve as one of the principal editors of the Virginia Commentary on the Law of the Sea Convention. Subsequently, I invited him year after year to lecture at the Rhodes Academy of Oceans Law which I had begun some years earlier, with colleagues from Europe, to train a younger generation of diplomats and scholars in the international law of the sea. Shabtai was a meticulous scholar with a rich knowledge of the law of the sea. He was warm and caring, but also a tough realist when it came to those who flaunted human rights and the United Nations Charter. He lived in challenging times and he fought against evil with an unshakable belief in the triumph of freedom and the rule of law. Writing definitive works on three of the four most important multilateral law-making treaties in history, he made an enormous contribution to international law. The world is a better place because of Shabtai. His friends, I among them, miss him dearly.

II.


A. Importance

Surely a list of the most important multilateral law-making treaties would include the Charter of the United Nations, the Statute of the International Court of Justice, and the Vienna Convention on the Law of Treaties. To that list might be added the four Geneva Conventions on the Law of War and numerous human rights, environmental and arms control conventions.

But by many indicia the United Nations Convention on the Law of the Sea (UNCLOS) is one of the greatest achievements in international law-making. The Convention provides a virtual constitution for over two-thirds of planet Earth, it resolved disagreements about oceans law going back at least four centuries, it deals with literally hundreds of substantive and procedural issues in its 302 Articles and nine annexes, on dispute settlement it created an important new international court, the International Tribunal for the Law of the Sea—along with two new arbitral procedures and a new conciliation procedure, and it created two important new functional international institutions, the International Sea-Bed Authority and the Commission on the Limits of the Continental Shelf. It was negotiated during the Cold War but remarkably with great power cooperation setting aside Cold War disagreements, with over 150 participating countries it was one of the first major law-making treaties to include the post-colonial world, it

3 There were also 45 observers participating at sessions of the conference representing states and territories, specialized agencies and other organizations, and intergovernmental organizations. And there were 57 non-
is one of the most important environmental treaties, it dealt successfully with an entirely new international issue, that of deep seabed mineral resources, and it overcame a decade long failure of agreement on these resources through an innovative United Nations led renegotiation of Part XI on deep seabed mining. It also developed an important new procedure in international law-making negotiations referred to as “the gentleman’s agreement” or “consensus procedure” and the related “package deal.” The Convention oversaw the greatest expansion of coastal nation resource rights in history, and it added to oceans law the concept of archipelagic states for certain mid-ocean island nations. Its negotiation, from early beginning in the mid-1960s through the final successful renegotiation of Part XI in 1994, consumed more than a quarter century. It broadly reflects community common interest rather than special interests, and today it is serving as a framework agreement for newer issues and remaining oceans governance challenges, and is broadly in force with 167 state parties plus the European Union. *That* is an achievement which stands in sharp contrast with the sad legacy of violent conflict and narrow nationalism all too evident in the twentieth and now the twenty-first centuries.

**B. The Convention and the Rule-of-Law**

The rule-of-law matters. Law serves to provide clear expectations as to jurisdictional boundaries and national rights and obligations so necessary for cooperative relations, economic life, and more broadly, human creativity. Thus, we need to know the breadth of the territorial sea, who manages coastal stocks of fish, the rules for straits transit, and a myriad of other rules to function cooperatively in the oceans. If some states claim three nautical miles for the territorial sea and others two hundred nautical miles we simply do not know the basic rules. But of even greater importance, the rule-of-law serves as a check on power. An oceans space driven by out-of-control national claims and a “might makes right” credo can neither serve community common interests nor restrain conflict. The Law of the Sea Convention is a remarkable achievement in the rule-of-law—serving both goals of stability of expectations and a check on power.

**C. The Background of the Negotiations**

The global context leading to the successful law of the sea negotiations was complex. It included four centuries of failure to functionally separate resource and navigational oceans issues with a preoccupation instead on a single line in the oceans focused on the breadth of the territorial sea. Since effective coastal fisheries management required a broad territorial sea and navigational freedom a narrow territorial sea, such a single line could neither serve the common interest nor could it work as the basis for agreement. Because of this failure to functionally separate the issues of fishery management and navigation, the First and Second United Nations Conferences on the Law of the Sea, held in 1958 and 1960, while making progress on the new concept of the continental shelf and rules for the high seas, simply could not reach agreement on the appropriate breadth of the territorial sea.

---

governmental organizations participating as observers, from the International Chamber of Commerce through the Sierra Club.
Other factors converging for a comprehensive new approach included the United States and Soviet Union discovery of the crucial straits issue—that transit through the more than 100 straits used for international navigation was of critical importance for global commerce and military transit and, as such, the rules developed for “innocent passage” through the territorial sea were hopeless for straits; the belated discovery of the environment during the late 1960s and early 1970s; a host of newly independent states which wished to participate in shaping oceans law; and, as the final catalyst, a speech by Ambassador Arvid Pardo, the Permanent Representative of Malta to the United Nations, electrifying developing countries with the prospect of little-known deep seabed resources as the “common heritage of mankind.”

D. Assessing the Common Interest

Now how should we assess the common interest in international oceans law matters and whether the Convention does a good job? The answer requires functional division of oceans uses. Uses such as navigation and laying of cables are uses which, for all practical purposes given the size of the world’s oceans, can be repeated over and over without scarcity. Such uses are also of enormous benefit to the world as a whole, with trade moving through oceans transportation driving the global economy. There is no case that these uses should be controlled by coastal nations. Nor do these uses require property rights in oceans space. Moreover, coastal nation efforts to control ship construction and operation for those transiting off their coast would create an impossible hodgepodge of standards. It would also threaten access for the more than half of all coastal nations in the world which are “zone-locked” by the 200 nautical mile exclusive economic zone adopted by UNCLOS. That is, counter to all our initial instincts about what a “coastal nation” is, nations such as Thailand, and over half of all other coastal nations, would have no access to the oceans without going through the economic zones of neighboring states. Understandably, this large block of coastal nations does not want to be turned into the functional equivalent of land-locked states with access controlled by their neighbors. For these and other reasons, environmental, safety and liability issues in shipping must be addressed through a single international entity rather than a myriad of coastal states. Today, given impetus by the decisions at UNCLOS, the International Maritime Organization (IMO) carries out these tasks. Similarly, the global interest in access from one ocean area to another through the narrow strait choke points supported a new regime of straits transit passage with full navigational freedom through, over, and under the more than 100 straits used for international navigation.

But fisheries, the oil and gas of the continental margins, and deep seabed minerals are all exhaustible and require the equivalent of property rights. Absent some management regime

---

4 The author gave the first speech on this concept of “zone-locked” states at the final Geneva session of the Seabeds Committee in 1973. He was as astounded as everyone else at the meeting to learn that a majority of all coastal nations would have no access to any ocean they faced without going through the 200 mile EEZ’s of neighboring states. He first discovered the problem over lunch with the Thai Representative to the Seabeds Committee. Thinking there might be other nations with the same access problem as Thailand, he asked the State Department Geographer to send him a list of states he termed as “zone-locked.” The result was this discovery of the enormous number of “zone-locked” states so crucial as to why coastal states should not be granted the ability to control vessel-source pollution in the 200 nautical mile EEZ. The speech effectively ended the effort by a few states to include jurisdiction over vessel-source pollution in the EEZ.
coextensive with the range of individual stocks, fisheries will be decimated through a free-for-all; and this was happening. This is the well-known “common pool” problem in economic theory. The solution was to provide a management regime coextensive with the major groupings of fish stocks—coastal, anadromous, catadromous, and highly migratory—and to provide for appropriate access rights and environmental standards for each. Since coastal nations already controlled a significant territorial sea off their coasts, the management of coastal stocks, and preferential access rights for these stocks, could easily and appropriately be given to coastal states. Similarly, since anadromous and catadromous stocks depended on a life-cycle relation even with a coastal state’s internal waters, the relevant coastal state, termed the host state, was the obvious answer for management of these stocks. Highly migratory stocks, on the other hand, required some degree of regional management throughout their range within and beyond areas of coastal state jurisdiction. With respect to the oil and gas of the seafloor on the continental margins, these resources too needed property rights. Since the coastal nations already controlled part of the continental shelf, through the 1958 Convention on the Continental Shelf, it was appropriate to turn over these resources to the coastal nations. Indeed, a decentralized global development of these resources was also likely more efficient than an effort to centralize their management. And with respect to both coastal fish stocks and the oil and gas of the continental margins, it was clear that agreement could never have been reached without assigning these to the coastal states. That is precisely what was done by the 200 nautical mile exclusive economic zone under Article 57 of the Convention and the “extended” continental shelf under Article 76 of the Convention.

But when it came to the mineral resources of the deep ocean floor, property rights were needed for development but there was no relation with any coastal nation. The appropriate answer was to create a new international functional agency which would provide the equivalent of property rights and regulate environmental issues in development of these mineral resources which were beyond areas of national jurisdiction. That is precisely what Part XI, and its renegotiation in 1994, achieved. While non-experts hypothesize a “fishing approach” to deep seabed minerals, that is simply turning firms loose to gather the resources like they would catch fish, the billions of dollars required for a seabed mining operation coupled with the reality that the refining operation for manganese nodules must be tailored to minerals from a particular site requires security of legal tenure not consistent with a “fishing approach.” That, in turn, requires the equivalence of internationally recognized property rights.

Assessing the Convention by these standards it was a remarkable success in supporting community common interest. The core genius of the Convention was the functional separation of oceans space by different oceans uses. Indeed, the political core of the Convention was an extension of coastal state resources rights in a 200 nautical mile exclusive economic zone and extended shelf while fully retaining navigational freedom in these areas, and adding a new critically needed regime for navigational freedom through, over, and under straits used for international navigation. This solution could both resolve the needed extended management regimes for fisheries while fully protecting navigational freedom. The same functional division, coupled with reasonable limitations on qualifying islands, resulted in acceptance of the archipelagic concept for certain mid-ocean islands nations such as Indonesia, the Philippines, Fiji
and the Bahamas. That is, acceptance of broad archipelagic state control of archipelagic waters subject to appropriate protection of navigation through these large oceans areas, including protecting navigational freedom in broad corridors through the archipelagoes. And the creation of a new regime for international recognition of the equivalent of property rights for exploration and exploitation of deep seabed minerals completed this common interest package.

Was there any oceans interest not appropriately resolved in the common interest? Theoretically, marine scientific research, as opposed to exploration and exploitation of resources, is also an ocean use which, with certain limitations such as drilling on the shelf, should remain free in areas beyond the territorial sea. Thus, conduct of research is not an exhaustible use of the oceans. Moreover, basic scientific research about the oceans, done for open publication, strongly benefits the world as a whole. But the 1958 Continental Shelf Convention had already prejudiced this issue by requiring the consent of the coastal state for “research concerning the continental shelf and undertaken there.” As such, it was not possible to walk the Shelf Convention back. But Part XIII of the Convention does seek to promote and facilitate marine scientific research and may well provide a better regime for science than the old Shelf Convention. It is to be hoped and encouraged that all nations will understand the global benefits from marine scientific research and that nations will work cooperatively to facilitate such research. I am pleased to report that the United States, while regarding the Convention provisions on traditional uses of the oceans as customary international law, places no restrictions on marine scientific research by other nations in its economic zone.

E. Substantive Contributions

UNCLOS has been of enormous importance both in resolving ancient oceans disputes and in modernizing oceans law for the twenty first century. Most importantly, it functionally separated oceans uses to permit an oceans law in the common interest. No longer would the choice be between protecting coastal fish stocks or navigational freedom. The 200 nautical mile economic zone places coastal stocks under a coastal state management regime throughout the range of most such stocks, while simultaneously preserving high seas navigational freedom in the zone. This was the core genius of the Convention; enabling success where there had been only failure when the issue was drawing a single territorial sea which could never accommodate both needs. But the Convention went on to modernize and improve oceans law in multiple ways. These include, among many other new and innovative provisions:

- Agreement on the maximum breadth of the territorial sea as twelve nautical miles (Article 3);
- A new straight baseline provision for a highly unstable coast line of Bangladesh (Article 7(2));
- Clarification of the regime of “innocent passage” through the territorial sea, including providing an exhaustive list of activities which would make passage non-innocent (Article 19(2)), and clarifying that coastal states may not make laws and regulations for the design, construction, manning or equipment of foreign ships passing through the territorial sea (Article 21(2)). This provision importantly
prevents an impossible situation for shipping of a hodgepodge of national laws and regulations rather than the international standards as set by IMO;

- Extension of the contiguous zone to a maximum breadth of 24 nautical miles (Article 33);
- Addition of coastal state control over “objects of an archaeological and historical nature found at sea” throughout the contiguous zone (Article 303);
- A critically important new Part III on Straits Used for International Navigation providing a regime of transit passage through, over and under such straits rather than the inappropriate “innocent passage” regime (Part III);
- A new Part IV recognizing special provisions for archipelagic states while both appropriately limiting the concept to certain island nations, and providing full high seas navigational freedom in broad corridors through the archipelagoes (Part IV);
- A new 200 nautical mile Exclusive Economic Zone (EEZ) in which the coastal state not only controls the natural resources of the zone but also “other activities for the economic exploitation and exploration of the zone,” yet there is full high seas navigational freedom in the zone (Part V);
- New conservation obligations binding on the coastal state in its management of the living resources of the zone (Article 61);
- The placing of anadromous and catadromous stocks under the control of the host state in whose internal waters they spend part of their life cycle (Articles 66 & 67);
- A special regime for highly migratory species of fish (Article 64);
- A special regime for marine mammals, including an obligation for states to “cooperate with a view to the conservation of marine mammals and in the case of cetaceans . . . [to] work through the appropriate international organizations for their conservation, management and study.” (Article 65);
- A new provision to reduce conflict among states by ending fishermen’s prison and requiring that “[a]rrested vessels and their crews shall be promptly released upon the posting of reasonable bond or other security.” (Article 73);
- New provisions for delimitation of economic zones and continental shelves between states with opposite or adjacent coasts (Articles 74 & 83);
- Resolving the outer boundary of the continental shelf which had been left uncertain in the 1958 Shelf Convention, recognizing coastal state control over the natural resources of the shelf even beyond the 200 nautical mile EEZ throughout the shelf, slope and rise (that is the full geologic “continental margin”), and creating a new Commission on the Limits of the Continental Shelf to assist, and quietly police, states in establishing the outer limits of their shelf (Part VI);
- Creating a modest revenue sharing system for the non-living resources of the continental shelf where the extended shelf of a coastal state goes beyond 200 nautical miles as a *quid pro quo* for granting the resources of the extended shelf to coastal nations (Article 82);

---

5 The author was pleased to have initiated this provision for the protection of cetaceans after he left the United States Delegation and was back at the University of Virginia.
• An updating of high seas law (Part VII);
• An updating of the rights of access of land-locked states (Part X);
• Creation of a new regime for the mineral resources of the deep ocean floor beyond national jurisdiction, including establishing a new International Sea-Bed Authority to create the equivalent of property rights for such mining to take place and for the necessary environmental and safety regulations;
• For the first time in oceans law a new and comprehensive series of obligations for protection of the marine environment (Part XII);
• A special provision for coastal state authority over vessel-source pollution in “Ice-Covered Areas” (Articles 234, 236 & 297(1));
• An updated regime of “Marine Scientific Research” (Part XIII); and
• A completely new regime and machinery for dispute resolution, including creation of a new standing International Tribunal for the Law of the Sea, two new arbitral procedures, and a new conciliation procedure.

F. The Negotiating Process

The UNCLOS negotiating process was as remarkable as the Convention. From the first preparatory work in the Seabeds Committee in 1967, through the successful renegotiation of Part XI on Seabed Mining in 1994, the process spanned over a quarter century. Even the formal sessions of the Conference ran from 1970 to 1982, a span of over twelve years. This, in turn, demonstrates the potential of keeping at a negotiation consistently through time instead of the more usual one-off short conference effort. Indeed, I believe that one of the mistakes made in UNCLOS was to end the conference in 1982 instead of continuing to negotiate the remaining issues in Part XI for as long as was necessary to obtain agreement.

UNCLOS was also remarkable for its inclusiveness. There were approximately 150 countries participating in the negotiations. And, with respect to oceans law issues at least, this was the first opportunity for many newly independent developing countries to fully participate in the shaping of oceans law. China too was actively engaged on issues of concern.

Perhaps most unusual, however, and a likely requirement for the UNCLOS success, was the cooperation across traditional Cold War lines between the United States, France, the United Kingdom and Japan, on one side of the then Cold War, and the then Soviet Union, on the other side. There was no magic here, the participants, working together in a group known as the Group of Five in the negotiations, simply shared common interests, particularly in protecting navigational freedom. This cooperation was, of course, in sharp contrast with the non-cooperation across cold war boundaries in UNCLOS I in 1958 and UNCLOS II in 1960, earlier Conferences which were unable to reach agreement on the maximum breadth of the territorial sea, much less resolve fisheries issues. Secretary Kissinger and others were no doubt surprised by the ongoing level of coordination within the Group of Five between major western states and the then Soviet Union, but despite hundreds of reporting telegrams from me and the United States delegation keeping the Secretary and our Government informed, Kissinger never sought to intervene. Nor, to my knowledge, did anyone in the other governments. The lesson here may be
that we should work harder at cooperation on matters of genuine common interest, and not necessarily be deterred by ongoing foreign policy schisms.

The United States played a particularly constructive and active role early in the negotiations. Thus, by the last year of the Seabeds Committee it had created an eighteen-agency Task Force through the National Security Council system. This enabled the United States to effectively coordinate its national position and then to reach out actively to resolve one issue after another in the international negotiation, leading to the successful adoption of the Conference “text,” the Single Negotiating Text (SNT), concluded at the end of the second substantive conference session in Geneva in 1975. This SNT included over 90% of the final Convention, including the provisions on the breadth of the territorial sea, baselines, the crucial provisions on innocent passage in the territorial sea and on straits transit, the archipelagic chapter, the exclusive economic zone, most of the provisions dealing with the continental shelf, the high seas articles, the marine science chapter, the environment chapter and the dispute resolution provisions. Principal unresolved issues at the end of this 1975 Geneva session, few in number, included Part XI on deep seabed mining, the boundary delimitation articles on the EEZ and on the shelf, and Article 76 on the outer edge of the continental shelf.

Unfortunately, inadequate progress was made in Committee I dealing with deep seabed mining and the SNT provisions on this subject were far from adequate. The fourth through eleventh sessions of the Conference from 1975 through 1982, though resolving principal remaining issues concerning the outer edge of the shelf and boundary delimitation, were unable to satisfactorily resolve the Committee I impasse before the recorded vote ending the Conference in 1982. The Convention was overwhelmingly adopted at this Eleventh Session, with only the United States (based on Committee I problems), Turkey and Venezuela (based on delimitation issues), and Israel, voting no.

A decade later negotiations on the unresolved Committee I issues were reenergized in 1992 under the auspices of Ambassador Satya Nandan, the then United Nations Under-Secretary-General for the Law of the Sea. This led to a remarkable broad-based consensus on a substantial revision of Part XI leading to international agreement two years later in 1994. While developed nations, including the United States, had held off accepting the Convention because of the problems with Part XI, the successful renegotiation led to rapid acceptance by developed nations and prompt entry into force of the Convention. The United States, a key participant in the renegotiation, accepted the new Part XI and promptly presented the Convention to the Senate for advice and consent. Sadly, the Senate has, as yet, not voted on advice and consent.

G. A Few Misperceptions

There have, from the start, been a few misperceptions about the Convention and the negotiations. First, the early days of the Committee I effort to negotiate a regime for deep seabed mining coincided with “the new economic order” as a negotiating philosophy for some newer nations. In addition, there was an understandable focus from developing countries to maximum “common heritage” revenues from seabed mining, thought by some to be an economic bonanza. The result was a push by developing countries for some kind of international
development agency to directly mine the deep seabed. Along with this came draconian fees and efforts to protect land-based producers of the minerals to be mined from the seafloor, as opposed to an effort to produce a viable system that would in fact lead to efficient mining for the copper, nickel, cobalt and manganese in the “manganese nodules.” It was widely believed by many developing nations at this time that the benefits from deep seabed mining would come primarily in the form of revenues from royalties to be distributed to developing countries. Economic analysis of deep seabed mining subsequently showed, to the contrary, that the principal economic benefit of seabed mining will be the reduction of the price of the minerals to be used by the consumers of all nations, developed and developing alike. That is, should the price of the minerals from the seabed be higher than production on land, then seabed production will simply not take place, but when production at sea is cheaper, and at some point in time that will happen, then the principal benefit is the cheaper minerals made available to consumers.

Following the first and second oil shocks in 1974 and 1980, and their draconian effect on developing nations, however, the views of developing nations toward the “new economic order” changed dramatically. This was one of the major changes which enabled successful renegotiation of Part XI.

Yes there likely will be a stream of revenues to be distributed to developing countries through the International Seabed Authority, but the benefit will be small compared to the benefit to developing country consumers from the cheaper minerals. Further, economic analysis shows that any effort to protect land-based producers principally assists developed nation producers at the expense of consumers in both developed and developing nations. Not surprisingly, when this reality was understood, the renegotiation of Part XI adopted a realistic system for mining to take place and substituted the GATT non-subsidy approach over the previous effort to protect land-based producers. The renegotiated system, meeting all of the conditions set forth by President Reagan for United States acceptance, is a workable and efficient system for seabed mining.

An associated misperception, also largely generated by the Part XI negotiation and the creation of the new International Seabed Authority, is that the UNCLOS negotiations were all a “third world” scheme to redistribute national incomes, and to turn over the oceans to an international bureaucracy. But nothing could be further from the truth. The reality of UNCLOS is that it has generated the largest transfer to nation states in the history of the world; that is, the massive transfers of the resources of the EEZ and extended shelf to coastal nations. Thus, *UNCLOS has worked a massive transfer of sovereign rights over resources to nation states, not the other way around.* Further, the International Seabed Authority is simply a new functional international agency, along with many already existing before UNCLOS. It is an agency which is necessary for the creation of “property rights” to enable the billion dollar investments needed for deep seabed mining. It is no more a precursor to world government than the Joint Canada/United States functional agency for regulating the water level in the great lakes, or any of the other hundreds of extant international functional agencies.

It is also not true that the core UNCLOS tradeoff was navigational freedom in return for recognition of the “common heritage” principle placing deep seabed mining under an international authority. While there were some in the early days of the negotiations who
advocated such an approach, this asserted “tradeoff” is sheer fantasy for the negotiations as a whole. As early as the final meetings of the Seabeds Committee in 1973, the United States had made it clear that there could be no such “tradeoff,” and that its bottom line requirements for acceptance of the Convention included both straits transit rights and assured access to seabed minerals. Subsequently, virtually all the major participants, including the United States, the Soviet Union and others, urged understanding in the negotiations that the core “tradeoff” was that necessary to resolve the ancient dispute of fisheries versus navigation; that is an extension of coastal state resource jurisdiction to 200 nautical miles in return for full navigational freedom in the zone and a straits transit regime providing access through, over and under the more than 100 straits used for international navigation. Finally, the United States, along with many other developed nations, refused to move forward under the Convention until Part XI had been renegotiated. This alone, showing that the regime for deep seabed mining was also a non-sign issue for many nations, disproves the deep seabed “tradeoff” myth.

H. The Problem of Continuing Violations

The effect of UNCLOS has been so strong that there has been a pattern of increasing compliance with the Convention. This pattern has been steady and will likely continue as more and more nations come into compliance. Unfortunately, however, there is still too much non-compliance. The principal problems are in excessive straight base line claims inconsistent with Article 7 of the Convention, claims that warships must have coastal state consent or provide advance notification for innocent passage through the territorial sea—claims which are inconsistent with Part II, Sections 3(A) & (C), excessive historic waters claims neither justified by history nor by recognition of other states, and claims interfering with navigational and other rights of third states within the economic zone which are not justified by the Article 56 grant of jurisdiction to the coastal state. Enhancing compliance with the Convention should be a continuing priority for the Annual Meeting of States Parties at the United Nations.6

A blatant example of what may be an excessive “historic waters claim” seems to be the “nine-dashed-line” of China in the South China Sea, though China continues to maintain a studied ambiguity as to the meaning of this “dashed-line.” Given China’s enormous interest in global trade, and thus its need for navigational freedom, as well as its increasing blue-water navy supporting the same interest, this “dashed-line,” if an historic waters claim, is not in the long-run interest of China. Nor does it help China in relations with its ASEAN neighbors, or in enabling resolution of the complex South China Sea island and boundary disputes. Nor is the “dashed-line” even remotely plausible under the law of the sea.

It seems likely that China will realize these points and begin a pattern of resolution of the South China Sea disputes through bilateral negotiations where feasible. Where bilateral solutions are not possible because of the myriad of South China Sea features generating an enormously complex pattern of claims, including island sovereignty claims (not governed by the

---

6 For a compilation of excessive claims see J. ASHLEY ROACH AND ROBERT W. SMITH, EXCESSIVE MARITIME CLAIMS, 3rd ed. (Martinus Nijhoff, 2012).
island status claims under Article 121, and unresolved territorial sea, EEZ, shelf and extended shelf overlapping boundary claims under Articles 15, 74 & 83, all complicated by multiple national claimants, then possibly China might pursue a multilateral sharing arrangement among ASEAN nations. In the meantime, this “nine-dashed-line,” and other issues in the complex South China Sea disputes, have generated an UNCLOS Part XV arbitration, brought by the Philippines against China, with the Tribunal having recently decided that it has jurisdiction.

I. The Problem of United States Non-Adherence

The United States was one of the most active and influential participants in the successful negotiations leading to UNCLOS. This is particularly true in the period through the adoption of the SNT, representing the great bulk of the present Convention. The United States was absolutely correct in not accepting the flawed Part XI as originally adopted in 1982, though it bears some responsibility in the ongoing late-stage confusion regarding this Part XI negotiation, particularly in the tenth and eleventh sessions in 1981 and 1982. The United States should also have moved more expeditiously to reopen negotiations on Part XI when that became feasible after the 1982 failure on this Part. But Part XI was fatally flawed in the 1982 version and would not have served the interest of any state, developed or developing, as mining simply would never have taken place. As such, Part XI needed to be changed and United States firmness in this served the world well.

Following the renegotiation of Part XI in 1994, a renegotiation meeting all of President Reagan’s conditions for United States acceptance and then some, the United States strongly supported the Convention, and the President promptly submitted the Convention to the Senate for advice and consent. Subsequently, every American President of both parties has supported United States adherence. Sadly, despite repeated favorable votes and recommendations from the Senate Foreign Relations Committee, for over two decades the Convention has languished in the Senate and has yet to come up for a vote in the full Senate. The reason is opposition from an isolationist faction endlessly repeating a patina of falsehoods about the Convention; a faction which at least has seemed to Senate leadership to have a blocking third in votes and has thus been able to prevent Senate advice and consent under Article II, section 2, of the United States Constitution requiring treaty concurrence by a two-thirds majority.

The United States will at some point fully adhere to the Convention. Nothing will happen, however, prior to the upcoming 2016 Presidential elections. Every oceans industry interest in the United States supports the Convention, from the oil majors to the environmentalists. Indeed, the only opposition is ideologically based, rather than interest based, and even then is senseless unless rooted in inaccuracies about the Convention. In the meantime, the United States accepts

---

7 One way for China to rationalize its “nine-dashed-line” would be to publicly declare that the “line” has relevance only for island sovereignty disputes which, of course, are not governed by the Convention. A slightly broader declaration would add that China asserts relevance, as well, in resolution of overlapping ocean boundaries as an “activity” of China to be taken into account in resolving such disputes. In its own interest, however, China needs to move off any implication that the line has relevance for navigational freedom or that it represents a valid historic waters claim.

8 At least one presidential candidate, Hillary Clinton, is a strong supporter of the Convention. While serving as Secretary of State she oversaw the most effective effort to date to obtain Senate advice and consent.
the normative provisions of the Convention as customary international law, and the United States Navy has one of the best records in the world in careful compliance.

Costs to the United States while the Nation awaits full Convention membership includes inability to participate in the International Seabed Authority, the Commission on the Limits of the Continental Shelf, or the Law of the Sea Tribunal. It also includes inability to move forward to exploration or exploitation of United States designated deep ocean mine sites causing the loss to date of two of the four United States sites with an estimated aggregate value of copper, nickel, cobalt and manganese of half a trillion dollars. You heard correctly, half a trillion dollars. Further, it means loss of effectiveness in the United States ability to assist in resolving oceans disputes such as those in the South China Sea, a slow start in mapping the extended continental margin of the United States, and so many other costs as to preclude their listing here. As Admiral Robert J. Papp, Jr., the Commandant of the Coast Guard, testified before the Senate Foreign Relations Committee in the 2012 hearing on the Convention about United States non-adherence: “It’s almost like having a winning lottery ticket that you don’t cash in.”

J. The Convention as Framework: Looking Forward in the Development of Oceans Law

One of the great strengths of UNCLOS is that it serves as a framework agreement for necessary further agreements to meet new oceans challenges. Thus, because the 200 nautical mile EEZ did not encompass all coastal stocks, even though likely including over 90% of such stocks, it was necessary to work out a management regime for the remaining “straddling” stocks which were within and beyond the EEZ. Similarly, because the ongoing negotiation within UNCLOS on highly migratory species was interrupted when I left the law of the sea process, and was left only partially completed when UNCLOS was finalized in 1982, highly migratory species also were still in need of a more complete regime. Both issues were addressed in a 1995 supplemental agreement, implementing provisions of UNCLOS for straddling and highly migratory stocks. In an interesting irony, the United States Senate quickly approved this 1995 United Nations Fish Stocks Agreement, and the United States became the third party to this Agreement.

Discussions are currently under way in the General Assembly with respect to a possible second implementing agreement, this one concerning conservation and sustainable use of marine biological diversity in areas beyond national jurisdiction (BBNJ). A core issue to be addressed in any such implementing agreement would be protection of biological diversity in sea floor spreading centers beyond national jurisdiction. Part XI of UNCLOS covers only mineral

---

9 Admiral Robert J. Papp, Jr., Commandant of the United States Coast Guard, comment to Senator Webb during testimony on June 14, 2012, before the Senate Foreign Relations Committee urging Senate advice and consent to the Law of the Sea Convention.

resources, so this agreement would address the unique life systems found in these deep ocean vent systems. The specifics of any such agreement have yet to be worked out.

There are at least two other areas in need of implementing agreements—implementing agreements specifically contemplated in UNCLOS. These are pollution from land-based sources, as contemplated by Article 207(4) of UNCLOS, and pollution from sea-bed activities subject to national jurisdiction, as contemplated by Article 208(5) of UNCLOS. During the UNCLOS negotiations it was understood that the complexities of controlling land-based pollution were simply too great to include in the framework agreement, so instead UNCLOS adopted a provision calling for states to address this problem through “competent international organizations or diplomatic conference.” Similarly, it was understood that the specifics of environmental regulation of oil and gas development on the continental shelf would require a specialized venue. So, again UNCLOS adopted a provision calling for states to act through “competent international organizations or diplomatic conference.” Had the shelf environmental provisions been negotiated in the over twenty years since UNCLOS has been in force, quite possibly the huge BP oil spill in the Gulf of Mexico might have been prevented. In any event, going forward these “land-based” and “shelf development” environmental implementing agreements should be an important priority for the international community.11

Because of the enormous success of UNCLOS, as well as its design as a framework agreement permitting consistent implementing agreements, it would be an enormous mistake to seek to renegotiate, or reopen, UNCLOS itself. In UNCLOS the international community has an extraordinary success! Would that were even fractionally as true in most other areas of international law.

K. A Brief Look at the Important Role of the United Nations in the UNCLOS Achievement

The United Nations played an important role in the UNCLOS success. It provided not just physical facilities for the negotiations, but a political foundation encouraging broad global participation. Both developed and developing nations were comfortable with the venue. Further, when the Part XI failure threatened to kill UNCLOS it was the work, and auspices, of the Office of the Under-Secretary-General which overcame the impasse. Without that intervention UNCLOS might today still not be in force, much less provide the basic framework on law of the sea for all nations, as it does. Similarly, the United Nations Fish Stocks Agreement was also enabled through the leadership of Ambassador Nandan and the United Nations.

The United Nations has also provided a service to the rule of law in the world’s oceans through the outstanding day-to-day work of the United Nations Law of the Sea Office (DOALOS). This office has maintained important compilations concerning the status of the

11 Because of the technological complexity of modern deep-ocean drilling for oil and gas on the continental margin, and the relative newness of the technology, I would strongly recommend that any environmental agreement concerning the shelf should incorporate utilization of Probabilistic Risk Assessment (PRA) techniques to isolate, and deal with, weak links in the technology. Elsewhere, PRA has compiled an impressive record in reducing accidents in complex industrial systems.
UNCLOS Convention and its institutions, has published important supplemental materials such as its booklet on baselines, has supported the Hamilton Shirley Amerasinghe Law of the Sea Fellowships, and in countless other ways has served to promote and support the law of the sea. Certainly the United Nations has much to celebrate in the success of its multilateral law-making efforts in the law of the sea.

THANK YOU
BRIEF BIBLIOGRAPHY OF PROFESSOR MOORE

John Norton Moore served as the Chairman of the National Security Council (NSC) Interagency Task Force on Law of the Sea (which coordinated eighteen U.S. Government agencies in developing U.S. oceans policy), Deputy Special Representative of the President for the Law of the Sea, United States Ambassador for the Law of the Sea, and Director of D/LOS, the NSC and State Department office for the Law of the Sea Negotiations. He was a U.S. Representative and Deputy Head of the U.S. Delegation for the Law of the Sea, and he chaired the U.S. Delegation to the 1972 New York session of the Seabeds Committee. He was appointed by President Reagan to the National Advisory Committee on Oceans and Atmosphere and he also served in the Reagan Administration as the first Chairman of the Board of the then newest federal agency, the United States Institute of Peace, and in that capacity set up and ran this new agency for its first five years through forty-nine meetings of the Board. He also served as a four-term Chairman of the American Bar Association Standing Committee on National Security Law and was one of the founders of the field of National Security Law. For over three decades he has served as the Director of the Center for Oceans Law and Policy of the University of Virginia, the preeminent oceans law center in the world. The Virginia Center, among many other engagements on the law of the sea, published the definitive seven-volume article-by-article analysis of the Law of the Sea Convention used by governments and courts all over the world, runs the principal international oceans law conference annually, and established the Rhodes Academy, the top center in the world for training government officials in the law of the sea. Professor Moore also served as Co-Chairman with the Deputy Attorney General of the United States of the first talks between the United States and the USSR on the Rule of Law (Moscow and Leningrad 1990), Consultant to the Arms Control and Disarmament Agency (1987-91), Chairman of the American Bar Association Standing Committee on Law and National Security (1982-86), Counselor on International Law to the Department of State (1972-73), and Chairman of the Governance & Ethics Committee of Freedom house, among other governmental and private sector assignments. He is the initiator and original draftsman for Freedom House of what subsequently became the Community of Democracies. He is also the 2013 recipient of the American Bar Association’s Morris I. Liebman Award in National Security Law for his work in founding the field of National Security Law. Most recently, he won Bronze (third place) as a member of the United States Masters Bench Press team in the 2015 World Championships.
Panel VII - The Arctic: National Security and Ocean’s Law for the New Maritime Frontier

Ms. Julie Gascon, Assistant Commissioner, Central & Arctic Region, Canadian Coast Guard

American Bar Association 27th Annual Review of the Field of National Security Law
Washington DC, November 17th, 2017
Canadian Coast Guard in the Arctic

**Geography**

Approximately 162,000 km² of shoreline

Arctic archipelago roughly 1.4M km²

---

Map adapted from the Atlas of Canada | Carte adaptée de l'Atlas du Canada
Overview

1. Present our Canadian Legislative Framework;

2. Describe the Canadian Coast Guard programs in the Arctic; and

3. Position our Marine Security and situational awareness in the Arctic.
Canada’s Arctic shipping regulatory regime has been in place since 1970 and is founded on the *Arctic Waters Pollution Prevention Act* (AWPPA).


Two primary principles underpin the regime:
1. Prohibition on the discharge of waste; and,
2. Experienced personnel who understand the limits of their vessel and are given adequate information about ice and other conditions will be able to operate safely.

The regulations set out by the AWPPA apply to all vessels of 100 gross tonnage or more, including fishing vessels. The zero-discharge regime, as well as the exceptions to the regime, apply to all vessels, regardless of size.

While the AWPPA and its regulations apply to Canadian Arctic waters only (North of latitude 60 and out to the extent of Canada’s Exclusive Economic Zone), the Canadian Arctic is also subject to legislation found throughout all Canadian waters, including:
- Canada Shipping Act, 2001;
- Marine Liability Act;
- Marine Transportation Security Act; and,
- Oceans Act.
To support the safe operation of vessels in the Canadian Arctic, the regime:

- Requires an experienced ice navigator and additional navigation equipment;
- Has systems in place to prevent ice damage by limiting access to navigation according to a vessel’s capability to operate in ice; and,
- Provides for the issuance of voluntary Arctic Pollution Prevention Certificates.

Under the Canada Shipping Act, the NORDREG requires mandatory vessel reporting to the Canadian Coast Guard.

NORDREG Officers provide vessels with meteorological, navigational, and ice-related information as well as vessel traffic tracking (position, identity, intention, destination).

Having mandatory regulations enhances the safety of vessels, crews and passengers and better safeguards the unique and fragile Arctic marine environment. They are designed to ensure that the most effective services are available to accommodate current and future levels of marine traffic.
Its objective is to address the unique hazards confronted by certain vessels operating in the Arctic and Antarctic (the Polar Regions) through the introduction of a variety of safety and pollution prevention measures, which includes (amongst others) design and equipment, vessel operations and crew training.

Canada played an instrumental role in the development this Code. As a result of this active engagement, the content of the Code — from the hazards addressed, to how a ship is to operate in ice — is influenced significantly by the safety standards contained within the existing Canadian regime.


Although Canada has had its own unique domestic Arctic shipping regime, it contains certain measures that are now outdated and require revision to reflect advancements in ship design and technology.

Canada will become bound by the Polar Code safety-related technical amendments on January 1, 2018, when it will implement these modernized requirements into its *Arctic Shipping Safety and Pollution Prevention Regulations*. 
In the Arctic, there are four comprehensive land claim agreements (CLCA):

- The Inuvialuit Final Agreement (1984);
- The Nunavut Land Claims Agreement (1993);
- The Labrador Inuit Land Agreement (2005); and,
Canadian Coast Guard’s Programs

- Marine Aids to Navigation
- Icebreaking Operations and Escort
- Marine Search & Rescue
- Marine Communications & Traffic Services
- Environmental Response
- Maritime Security
Marine Communications and Traffic Services

- VHF, up to 40 nautical miles
- MF, up to 400 nautical miles
- HF, up to 1200 nautical miles
Coast Guard has 22 equipment depots in the Arctic. These are broken down into three types:

1. Community Packs (x18)
2. Rapid Air Transportable (x1)
3. Major Environmental Response Depots (x3)
Joint Rescue Coordination Center (JRCC) Halifax and JRCC Trenton coordinate SAR response in the Arctic using:

1. Canadian Coast Guard Auxiliary in 12 communities
   • Expansion in 2017
2. Royal Canadian Air Force (RCAF) provides air resources:
   • RCAF bases: Gander, Greenwood, Trenton, Winnipeg, Comox
3. Nunavut and Nunavik SAR groups provide local response for ground search and rescue and limited marine search and rescue
4. All Coast Guard icebreakers and associated helicopters are on 1-hour SAR standby

RCAF Hercules and Cormorant
**Scenarios**

2016 – A fire on a large cruise ship located in the Beaufort Sea has left power only for essential equipment (no heat, water, toilets, food, etc.).

2017 – Cruise ship encounters similar issues 40 nm of Pond Inlet (Nunavut)

**Objectives**

Examine existing SAR capabilities and limitations in emergency responses

Determine operational & logistical requirements for transporting survivors back to the south
Lessons Learned

Limited infrastructure for incidents involving large number of people

All available resources must be directed to incident location

Significant Coast Guard assets should not be expected for first 72 to 96 hours

Lifeboats not designed to hold survivors for long or travel large distances unescorted

Passengers must get into water to be airlifted
Icebreaker escort
Timely assistance
Temporary hotel
No lifeboat crowding
No need to get into water
Command Post

Ernest Shackleton (1A1 Super Icebreaker)
Canadian Coast Guard’s Role

- Enhance Maritime Domain Awareness to support threat identification, monitoring and analysis
- Provide vessels, helicopters and trained personnel to support federal security and enforcement partners
- Develop priorities and policy in collaboration with maritime security community
- Work with partners to analyze marine intelligence
Maritime Security (cont’d)

Coast Guard’s Contributions

- Enhancing Maritime Domain Awareness
- Provision of vessels, helicopters and maritime expertise to security partners
- Development of priorities and policy

Great example of enhanced collaboration between Canadian and U.S. coast guards: **Integrated Border Enforcement Teams (IBET)** (a.k.a. “Shiprider Program”).

Operations in Canadian waters supervised by RCMP officer and operations in American waters supervised by USCG officers.

IBET teams are able to patrol boundary waters of both countries efficiently using fewer vessels.
Marine Security Operation Centres (MSOCs)

- Canada’s maritime expertise contribution
- Inter-agency approach and co-location of representatives from five core federal partners
- Partner resources and expertise leveraged to analyze, generate and disseminate information
- Accurate and timely picture of maritime situational awareness
- MSOC East produces many reports and products to enhance awareness in Northern waters

**MSOC Partners**
- Canadian Coast Guard (DFO)
- Royal Canadian Mounted Police
- Canada Border Services Agency
- Transport Canada
- Department of National Defence

**MSOC West**
Victoria, BC

**GL MSOC**
Niagara, ON

**MSOC East**
Halifax, NS
Coast Guard leverages its vessel traffic monitoring systems and maritime expertise to support awareness of potential on-water threats.

The Coast Guard has many tools to support Maritime Domain Awareness including:

- **Long Range Identification and Tracking** - An international, satellite-based vessel tracking system that uses existing shipborne equipment.

- **Automatic Identification System** - An autonomous broadcast system that enables the identification and tracking of vessels.
Maritime Domain Awareness (cont’d)

Canadian Arctic Shipping
24 October 2017

Vessel Type
- CCG, Canadian Research Vessels
- Merchant Traffic and Resupply Ships
- Fishing Vessels

*Currently no Arctic Adventurers, Cruise Vessels or RCN Ships.
Canada’s Oceans and Protection Plan

$1.5 Billion National Oceans Protection Plan

1. Supports safe and clean marine shipping
2. Builds partnerships with Indigenous and coastal communities
3. Increases economic opportunities for Canadians
4. Improves marine safety
5. Protects the marine environment

canada.ca/oceans-protection-plan
Key Oceans Protection Plan Investments (amongst others) include:

- new CCG infrastructure (e.g., SAR stations);
- training for increased MCTS Centres;
- equipment (i.e. SAR lifeboats),
- actions on derelict vessels to create a polluter-pay approach to clean up future abandoned vessels and funding to support removal of derelict vessels;
- hydrographic map of high-profile ports and key waterways;
- Indigenous engagement in proactive vessel management and leadership in the Arctic CCG Auxiliary and SAR capacity.
Questions?

Thank you!
PANEL VIII:

CURRENT EVENTS IN NATIONAL SECURITY LAW AND CYBER POLICY

DISCUSSANTS:
MONIKA BICKERT
HARVEY RISHIKOF
INTO THE GRAY ZONE
The Private Sector and Active Defense against Cyber Threats

Center for Cyber & Homeland Security
THE GEORGE WASHINGTON UNIVERSITY
# Table of Contents

Foreword and Acknowledgements .................................................................................................................. v
Participants ......................................................................................................................................................... ix
Executive Summary ........................................................................................................................................... xi

**Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats**

1. Background on the Cyber Threat, Responses to the Threat, and Active Defense .............................................. 1

2. The Current Policy, Legal and Technology Context ......................................................................................... 17

3. Genesis of the Framework .................................................................................................................................. 21

4. A Framework for Active Defense Against Cyber Threats ............................................................................... 23

5. Implementing the Framework:
   Key Near-Term Policy Recommendations ...................................................................................................... 31

6. A Call To Action .................................................................................................................................................. 35

7. Active Defense Considerations for the Future .................................................................................................. 37

Appendix I: Additional Views of Nuala O’Connor .............................................................................................. 39

Appendix II: Legal Analysis, Courtesy of Covington & Burling, LLP ................................................................. 41

Appendix III: Global Perspectives on Active Defense .......................................................................................... 45

Appendix IV: Glossary of Terms .......................................................................................................................... 49

Notes...................................................................................................................................................................... 57

Selected Works Consulted ..................................................................................................................................... 67

About the George Washington University
Center for Cyber and Homeland Security ........................................................................................................... 69
PRIVATE SECTOR ENTITIES operate today on the front lines of cyber conflict, targeted by a variety of hostile actors that seek to steal and misappropriate their intellectual property, degrade their infrastructure, and disrupt their business activities. Despite this reality, the options available within the private sector for responding to cyber threats are outdated and constrained. The status quo is reactive in nature and advantages the attacker. The time has come for the private sector, working together with governments, to flip the equation and enhance its ability to counter such cyber threats.

A key element of a cyber strategy for the private sector is active defense, a term that captures a spectrum of proactive strategic and technical cybersecurity measures that are the focus of this report. Such measures—if developed and used within a carefully defined legal and policy framework that accounts for technical risks and companies’ differing capabilities—provide a powerful tool for addressing cyber threats to the private sector.

There are two major challenges for private sector cybersecurity that active defense capabilities would address. The first is related to the cyber threat. Simply put, threats are expanding in persistence and consequence and we cannot solely rely on defensive measures and “firewall” our way out of this problem.

The second challenge has to do with the mismatch between capabilities and authorities between the public and private sectors. While the U.S. government will always play an important role in cybersecurity, it lacks the resources to fully defend the private sector in the digital realm. But the current legal and policy environment for companies to defend themselves is ambiguous, making it risky for businesses to utilize active defense tools that may be effective in addressing malicious cyber attacks. The United States’ efforts to articulate an effective cyber deterrence posture are also constrained by this ambiguity about active defense.

Many American policymakers, recognizing the private sector’s significant role in the nation’s cybersecurity, have led numerous calls for greater public-private partnerships. However, such initiatives have to date been incomplete, focusing on information sharing, best practices, and post-incident investigation. There is a need for government to partner with the private sector in developing and implementing a framework for active defense. Such a framework would allow forward-leaning and technologically advanced private entities to effectively defend their assets in cyberspace, while at the same time ensuring that such actions are embedded within a policy and legal framework that confirms government oversight, ensures that privacy and civil liberties are not infringed, and mitigates technical risks. America cannot accept the cybersecurity risks of a vulnerable private sector or continue to maintain an inadequate cyber deterrence posture.
It is our hope that the framework offered in this report will help to crystallize thoughts, build consensus, and ultimately, spur requisite action related to private sector active defense by the U.S. government and American business executives. In January 2017, the new President and Administration will undoubtedly face a host of challenges that demand priority attention, and the present subject should rank among them given the powerful interplay between national security and economic security.

This report places the current cyber threat in its larger strategic context and then assesses the role of private sector active defense in addressing such threats. With this in mind, the report proposes a framework that defines the most prevalent active defense measures and places them along a spectrum of relative risk and impact, indicating where close coordination with the government becomes necessary for responsible private action. This framework will help actors in the public and private sectors understand and operationalize active defense against cyber threats and is contextualized through careful analysis of relevant policy, technology, and law. The implications of each measure are especially considered in light of the rights and freedoms of Internet users that such a framework should support to the greatest extent. Next, we specify a series of key recommendations that are segmented by target audience (the executive branch, Congress, and the private sector). Finally, the report concludes with a brief discussion of issues for future consideration, followed by standalone appendices that contain, respectively, a deeper dive into the legal dimension, selected global perspectives on active defense (Estonia, France, Israel, and the United Kingdom), and a glossary of relevant terms. The findings and recommendations of this report were distilled by the co-chairs and project staff and do not necessarily represent the views of each member of the Task Force. Co-chair Nuala O’Connor has submitted additional views (Appendix I).

This initiative was made possible by the generous financial support of The William and Flora Hewlett Foundation and the Smith Richardson Foundation. In addition the George Washington University Center for Cyber and Homeland Security and the Task Force co-chairs are grateful for the time, resources, and insights contributed by the Members of the Active Defense Task Force and many other stakeholders—both organizations and individuals—that participated in the workshops, panel discussions, interviews, research, and drafting that helped to shape the ideas contained in this report. To be clear though, it should be noted that this report does not represent a consensus viewpoint of the participants in the task force process.

While it is not practicable to name each and every instrumental contributor to this endeavor we would be remiss if we did not single out at least a few, while at the same time acknowledging the vital expertise that many provided on a not-for-attribution basis across a range of disciplines including technology, security, privacy, law, and business. The law firm of Covington & Burling, LLP and in particular partner Robert Nichols and his team of associates conducted substantial
legal research for this project on a pro bono basis. Orin Kerr, the Fred C. Stevenson Research Professor at the George Washington University Law School also served as a legal consultant.

The Department of Justice’s Computer Crimes and Intellectual Property Section, the United States Secret Service, The Carnegie Endowment for International Peace, Endgame, Johns Hopkins University Applied Physics Laboratory, Microsoft, Mitre, and Novetta provided tailored briefings to the full Task Force. The Johns Hopkins University Applied Physics Laboratory and the William and Flora Hewlett Foundation lent meeting space to the Task Force for two of the four working sessions. Building on the deliberations of the Task Force, this report was primarily drafted by the staff of the Center for Cyber and Homeland Security, including Christian Beckner, Taylor P. Brooks, Sharon Cardash, and Alec Nadeau; Joseph R. Clark and Rhea Siers contributed critical insights. Throughout the life of this project, Alec also worked tirelessly to coordinate the Task Force’s activities and provide logistical support.

The issues discussed in this paper are complex, and attempt to address and balance the views and interests of a diverse group of stakeholders from the U.S. government, various elements of the private sector (notably the tech sector and the financial sector), academia, privacy and civil liberties organizations, and international governments. While we have not proposed a path that reconciles all of the conflicting interests from these different stakeholders, we believe that our proposals can bring them closer together, aligning interests and moving toward productive solutions to common challenges. Our aim was to help chart a constructive course forward through this complicated terrain, and in this, we hope we have succeeded.

Washington, D.C. - October 2016

Task Force Co-Chairs:

Admiral Dennis C. Blair
The Honorable Michael Chertoff
Frank J. Cilluffo
Nuala O’Connor
Participants

Task Force Co-Chairs

Admiral Dennis C. Blair
Former Director of National Intelligence; Chairman and CEO, Sasakawa Peace Foundation USA

Secretary Michael Chertoff
Former Secretary of Homeland Security; Co-Founder and Executive Director, the Chertoff Group

Frank J. Cilluffo
Director, Center for Cyber and Homeland Security; Co-Director of the Project

Nuala O’Connor
President and CEO, Center for Democracy & Technology

Project Staff from the Center for Cyber and Homeland Security

Deputy Director & Co-Director of Project
Christian Beckner

Associate Director & Research Director of Project
Sharon Cardash

Policy Analyst
Taylor P. Brooks

Presidential Administrative Fellow & Project Coordinator
Alec Nadeau

Active Defense Task Force

Stewart Baker
Steptoe & Johnson

David Heyman
Tektonics Global, LLC

Cheri McGuire
Standard Chartered Bank

Christopher Ballister
IBM

Jason Healey
Columbia University, School for International & Public Affairs

Angela McKay
Microsoft Corporation

Robert Chesney
University of Texas School of Law

General Reynold Hoover
National Guard Bureau

James Mulvenon
Defense Group, Inc.

Thomas Corcoran
Zurich Insurance Group

Irving Lachow
Mitre Corporation

Robert Nichols
Covington & Burling, LLP

Rajesh De
Mayer Brown

Peter LaMontagne
Novetta

Michael Papay
Northrop Grumman

Timothy Evans
Johns Hopkins University, Applied Physics Laboratory

Nathan Lesser
National Institute for Standards and Technology

Harvey Rishikof
Crowell & Moring

Nathaniel Fick
Endgame

Ariel Levite
Carnegie Endowment for International Peace

Keenan Skelly
Circadence

Brian Finch
Pillsbury, Winthrop, Shaw, Pittman

Jane Holl Lute
Former Deputy Secretary of Homeland Security

General Kenneth Todorov
Northrop Grumman

Zachary Goldman
Center on Law & Security, New York University School of Law

Matthew McCabe
Marsh

Cory Wilson
Law Enforcement Policy Advisor

Geoff Hancock
Advanced Cybersecurity Group

Michael Zweiback
Alston & Bird, LLP
Executive Summary

OVER THE PAST SEVERAL DECADES, the private sector in the United States has embraced the computer revolution and the growth of the Internet, and migrated its business activities and operations into an information technology environment. This transition to the online domain has provided tremendous benefits to the private sector, enabling business efficiencies, lowering transaction costs, establishing new products and markets, enhancing internal collaboration, and improving the ability of companies to measure and assess their performance. But as the online domain has developed over the past several decades, new risks have accompanied these benefits; companies have become increasingly vulnerable to the theft of online intellectual property or customer data and the disruption of business operations.

These cyber risks and dependencies have grown in recent years due to the activities of hostile state and non-state actors in cyberspace, who have attacked private sector entities for both political and economic reasons. Companies have enhanced their defenses, and the federal government has placed a higher priority on assisting the private sector, but such measures are not commensurate with the nature of the cyber threat today.

This paper examines a set of capabilities that can help to address this gap, collectively defined under the term **active defense**:

*Active defense is a term that captures a spectrum of proactive cybersecurity measures that fall between traditional passive defense and offense. These activities fall into two general categories, the first covering technical interactions between a defender and an attacker. The second category of active defense includes those operations that enable defenders to collect intelligence on threat actors and indicators on the Internet, as well as other policy tools (e.g. sanctions, indictments, trade remedies) that can modify the behavior of malicious actors. The term active defense is not synonymous with “hacking back” and the two should not be used interchangeably.*

The policy discussion on active defense measures in recent years has largely fallen into one of two camps: those who believe that active defense activities are appropriately prohibited under current U.S. law, and those who believe that more active tools should be available to the private sector. What has been missing is a more nuanced discussion of this issue: What measures fall within the scope of active defense, and what are the benefits and risks of each? What measures may be appropriate to use by certain actors, and under what circumstances? What is the role of the federal government in developing a framework and set of norms that can inform such action? And how should policy and law be updated to support private sector active defense in a way that is consistent with both our values and interests, and that can evolve as new technologies are developed?

In other words, how do we move beyond the current policy stalemate of inaction vs. hacking back, and develop appropriate and risk-driven policies for active defense? This paper attempts
to go “into the gray zone” and answer these questions. It proposes a normative framework for operationalizing active defense and puts forward a set of policy recommendations that support the implementation of such a framework.

The initial sections of the report provide background and context to this discussion. It begins with a very brief overview of current cyber threats to the private sector, and what is being done by private entities and government agencies to counter these threats. This discussion of the threat is followed by an articulation of U.S. interests in cyberspace and an explanation of the strategic context of active defense, in particular its relation to the issue of cyber deterrence.

The next section of the report provides a historical perspective on the evolution of the term “active defense,” initially in a general national security context and later with respect to cybersecurity. These historical definitions inform the report’s own definition. The report then discusses the upper and lower boundaries of active defense and examines the spectrum of activities that fall within it, including honeypots, beacons, and sinkholing malicious traffic. It makes clear that certain types of high-risk active defense activity by the private sector should be impermissible due to risks of collateral damage and privacy-related concerns, but pushes for greater clarity on whether and how the private sector can utilize lower-risk active defense measures.

Next, the paper provides additional policy context to the issue of active defense, examining the impact of current U.S. laws (e.g. the Computer Fraud and Abuse Act), assessing the policy impact of evolving technologies such as cloud computing and the Internet of Things, and outlining the nascent international framework for active defense.

The final sections of the report lay out the proposed framework for active defense by the private sector. The core of this framework is the spectrum of active defense measures defined earlier in the report, embedded within a broader set of policy, legal, technical, and governance-related considerations, which provide the basis for risk-driven deliberation and decision-making both within companies and between the government and the private sector on active defense. The framework seeks to maximize the effectiveness of the private sector’s ability to defend its most valuable data and assets. It recognizes that a broad suite of technical and non-technical tools is applicable to the countering of cyber threats to the private sector. And it attempts to balance the need to enable private sector active defense measures with other important considerations such as the protection of individual liberties, privacy, and the risks of collateral damage. An additional key aspect of this framework is a risk-driven methodology that can be used to weigh the risks and benefits of action vs. inaction, and to then choose and utilize appropriate tools if and where action is warranted.

This overview of the framework is followed by a detailed discussion of key actors within the framework and what is needed to operationalize it. After this section, the report puts forward a set of near-term policy recommendations for the U.S. executive branch, Congress, and the private sector that are intended to facilitate the implementation and adoption of this framework.

**Actions for the Executive Branch**

1. The Department of Justice should issue public guidance to the private sector with respect to active defense measures that it interprets to be allowable under current law, indicating that DOJ would not pursue criminal or civil action for such measures assuming that they are related to the security of a company’s own information and systems. Such guidance should be updated on a regular basis consistent with ongoing developments in technology.

2. DOJ and the Federal Trade Commission should update their “Antitrust Policy Statement on Cybersecurity Information Sharing” (2014) to state clearly that antitrust laws should not pose a barrier to intra-industry coordination on active defense against cyber threats.

3. The Department of Homeland Security should coordinate the development of operational procedures for public-private sector coordination.
on active defense measures, utilizing existing mechanisms for cooperation such as the industry-led Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs), and the National Cybersecurity and Communications Integration Center (NCCIC) at DHS.

4. The National Institute for Standards and Technology (NIST) should develop guidelines, best practices, and core capabilities for private sector activity with respect to assessing the risk of and carrying out active defense measures, with 3-5 different levels of technical maturity linked to certification to carry out certain types of measures, or in the case of third-party vendors, to protect other companies. Such guidelines may be distinct for different industry sectors, and this effort at NIST shall be consistent with the work done in 2013-2014 to develop the Cybersecurity Framework.

5. Federal agencies that fund cybersecurity-related research and development, including the Departments of Defense, Homeland Security, the Intelligence Community, and the National Science Foundation, should prioritize R&D on the development of new active defense measures (including capabilities that may improve attribution) and assess efficacy of current active defense measures.

6. The Department of State should engage with foreign partners in developing common standards and procedures for active defense measures. This is particularly relevant given the fact that many of the large companies who are affected by cyber threats operate globally, and thus need to protect information on systems in dozens of countries.

7. The Privacy and Civil Liberties Oversight Board (PCLOB) should carry out a review of current and proposed federal government activities related to active defense activities by the private sector, and release a public report on the results of this review.

8. The White House should develop a policy that provides guidance to federal agencies on when and how they should provide support to the private sector with respect to active defense activities, addressing such factors as the maturity of private sector entities, the nature of the threat actors (if known), and the economic and security-related importance of the infrastructure or information targeted. This latter factor could perhaps be linked to the list of “critical infrastructure at greatest risk” as identified by DHS pursuant to Section 9 of Executive Order 13636. Types of support that are envisioned include information sharing, coordinated planning, intelligence support, and training.

9. The President should issue a directive that codifies the requirements in items 1-6 above and sets clear deadlines for the adoption of them.

Actions for the U.S. Congress

10. Congress should pass legislation to oversee the implementation of the activities in action items 1-7 above, and reinforce the deadlines in statute. Congress should also mandate that the Government Accountability Office review the implementation of this legislation.

11. Congress should reassess language in the CFAA and the Cybersecurity Act of 2015 that constrains private sector activity on active defense, to ensure that low and medium-risk active defense measures are not directly prohibited in statute.

12. Congress should examine whether and how other tools established in law (e.g. indictments, sanctions, trade remedies) can be utilized in support of protecting the private sector against malicious cyber actors. Executive Order 13694 (“Sanctions Related to Significant Malicious Cyber-Enabled Activities”) from 2015 is a good example of this principle in practice, but there are other tools that can be utilized in support of cyber deterrence and active defense.
Actions for the Private Sector

13. Private sector companies should work together and take the lead in developing industry standards and best practices with respect to active defense measures within their sectors and industries. Such efforts should be undertaken on an international basis, involving a broad set of major companies from all regions of the world.

14. Companies should develop policies at the C-Suite level for whether they want to engage in certain types of active defense measures in response to hypothetical future attacks, instead of simply reacting after they have suffered a data breach or other form of cyber attack. Companies should develop an operational template, based upon a thorough risk assessment and analysis of industry standards and best practices, that can be integrated into a broader cyber strategy and incident response protocols. These policies must be incorporated within the companies’ broader commitment to and investment in their own traditional cyber defense programs.

15. Industry groups should examine best practices for coordination between Internet service providers, web hosting services, and cloud service providers and their clients on active defense, leveraging the fact that these service providers often have contractual, pre-authorized access to their clients’ networks for routine business purposes. Such service providers may be well positioned to carry out active defense measures against cyber threats to their clients.

The report concludes with a call to action on this issue and a brief examination of future trends that may impact the evolution and development of active defense policy and procedures. The report includes several appendices that support the report’s core analysis, including a review of U.S. law, vignettes that provide a global perspective on active defense (in the United Kingdom, France, Estonia and Israel), and a glossary of terms.
IN THE PAST SEVERAL YEARS, top national security leaders and executives in the private sector have argued that cybersecurity vulnerabilities are a major threat to their organizations’ missions and to U.S. national security. Indeed cybersecurity is increasingly listed as a top concern for CEOs and other corporate executives. Media outlets are flooded with reports of massive breaches at consumer-facing companies, advanced cyber espionage, and cyber attacks on critical infrastructure. Gone are the days in which the average individual thought about cybersecurity only when his or her credit card was compromised. Instead, a February 2016 Gallup poll found that 73% of Americans considered cyberterrorism to be a critical threat to the United States. These developments are in part the result of the difficulties in deterring malicious cyber activities, something the United States and many other nations have struggled to do.

Recently, observers have noted a significant escalation in the frequency and efficacy of strategic malicious cyber activity. In the private sector, targets have ranged from Sony Pictures to Yahoo, to political organizations. With recent breaches at the Internal Revenue Service, the Office of Personnel Management, and various state agencies, it is clear that government organizations at all levels are also targets of cyber threat actors. The sheer number of successful malicious cyber actions that defenders have faced up to this point has increased the level of frustration many have with traditional cybersecurity measures and has raised the question of what entities can do to adequately defend their interests in cyberspace. As companies collectively lose billions of dollars to intellectual property theft, lose the right to control the use of their most personal information, and generally lose their sense of trust and security online, the feeling that current cyber defenses have failed them is inescapable. In order to preserve public trust in the Internet and its underlying utility, 21st century cybersecurity practices must evolve alongside threats to national security, economic vitality, privacy, and human rights. This report will demonstrate how new cybersecurity practices and strategies can enhance cyber defense in the private sector.

America is at an inflection point in cyberspace. U.S. government agencies and private sector companies have developed and benefited from some of the most advanced capabilities in cyberspace. But these same entities are vulnerable to disruptive cyber incidents, and are under constant threat from a variety of actors. One key element of a broad effort to address this challenge is more clearly defining the private sector’s role in cybersecurity, not only with respect to information sharing and defensive activities, but more broadly with respect to “active defense,” a set of operational, technical, policy, and legal measures that are the subject of this report.
What is the Cyber Threat?

Before turning to a more detailed discussion of active defense later in this paper, we first need to consider and assess the types of cyber threats that are targeting the private sector.

America’s most sophisticated cyber adversaries are the nation-states of Russia, China, Iran, and North Korea. In some instances, these states may use their own military and intelligence services to conduct cyber exploitation, but increasingly states are acting through proxies to whom they may provide funding or other tacit support. Foreign states and their proxies are joined by a variety of other cyber threat actors including criminal enterprises, hacktivists, and terrorists that are engaged in malicious cyber activities against U.S. entities.

Those who use cyber means to exploit or attack computer systems in America and other countries act out of a variety of political, ideological, and geostrategic motivations. Malicious actors may seek power, prestige, money, or some combination of the three. Nation-states may hope to gather intelligence on their adversaries or damage a rival’s critical infrastructure in times of conflict. Criminals tend to be active wherever they can make a profit and where the costs of doing business are low. Terrorist organizations have used the Internet to recruit and radicalize, but undoubtedly aspire to more destructive cyber-enabled attacks. Hacktivists often use cyber capabilities to pursue a political end. Across all cyber threat actor types and motivations, malicious cyber activity is increasing in scale and sophistication, often enabled by advanced and shared capabilities. Regardless of their specific capabilities and motivations, cyber threats undermine the trust and stability of the Internet, corrupting its inherent value.

Cyber Threats to National Security, Economic Security, and Privacy

The effects of cyber threats are not, however, limited to an abstract assault on the Internet as a concept. The cyber threat landscape tends to jeopardize a number of American interests, including national security, economic vitality, human rights, and privacy. National security concerns were raised in 2013 when Iranian hackers gained access to the servers that controlled a dam in Rye, New York. Activities like these are a form of intelligence preparation of the battlefield, tailored to the cyber domain, and could presage attempts to target and disrupt even more significant critical infrastructure in the United States. The disruptive effects of the malicious cyber activities on Ukraine’s electricity grid in 2015 highlight precisely why such attacks must be taken extremely seriously.

Beyond the threat to U.S. national security posed by malicious cyber attacks and espionage is the constant threat against the U.S. private sector. The security of the American economy is of fundamental importance not only to the United States, but to the entire world. Yet cyber espionage, theft, and sabotage against the private sector are rampant. Former NSA Director Gen. Keith Alexander described the cyber theft of American industrial information and intellectual property as the “greatest transfer of wealth in history.” In recent years, the cost to the U.S. economy from malicious cyber activities has increased.

Malicious cyber actors have particularly targeted certain industries, such as the financial sector. In 2012, a disruptive series of Distributed Denial of Service (DDoS) attacks targeted 26 major U.S. banks over a period of four months, causing significant financial losses. In August 2016, Roman Seleznev of Russia was...
convicted for cyber-criminal activities that caused over $169 million in losses to 3,700 financial institutions.\textsuperscript{17} The recent fraudulent manipulations of the SWIFT interbank messaging system led to millions of dollars in losses and fears that the entire global banking system could be at risk of manipulation.\textsuperscript{18}

Malicious cyber actors are frequently targeting valuable intellectual property (IP), the protection of which is necessary to a well-functioning market economy. In 2013, the IP Commission Report found that 20% of American jobs were in IP-intensive industries and that the negative effects of IP theft in one sector can have secondary effects throughout other sectors, threatening U.S. economic security.\textsuperscript{19} This highlights a larger concern that although industrial sectors may have differing cybersecurity capacities, a major vulnerability in one sector could have serious impacts across the board.\textsuperscript{20}

The cyber-related economic threat poses a significant strategic threat to American security. Recent estimates put the cost of cyber attacks against private business to be between 0.64% and 0.9% of the United States’ gross domestic product.\textsuperscript{21} If those estimates are accurate, cyber-attacks did between $120 and $167 billion dollars of damage to the U.S. economy in 2015. Given the ongoing rapid growth in cyber attacks, this trend is likely to continue, if left unchecked.\textsuperscript{22}

Numerous cyber exploitations represent an assault on the individual right to privacy. Recent incursions into the private networks of Target, Sony Pictures, Yahoo, and the Democratic National Committee represent a few of the many particularly threatening cyber operations from a privacy perspective.\textsuperscript{23} In these hacks, malicious cyber actors exploited and released sensitive consumer information, private communications, and intellectual property. In order to preserve public trust in the Internet, 21st century cybersecurity practices must evolve alongside threats to national security, economic vitality, privacy, and human rights.

What is Being Done to Safeguard Against Cyber Threats?

One key aspect that differentiates cybersecurity threats from other security threats is the extent to which the government appears unable to adequeate-
not enough to keep out hackers, and the inherent advantage rests with the attacker. A sophisticated adversary can easily disrupt a service, steal assets, or even destroy data held on private servers. Even non-state malicious actors have increased their sophistication in recent years, at times nearing a level of sophistication previously thought only achievable by the most capable of state actors.

Despite the limitations of defensive measures, it is important to note that private sector companies that implement basic practices of cyber hygiene can prevent the vast majority of malicious cyber activity. Companies are increasingly adopting security controls that will allow them and government partners to focus more resources on countering advanced threats—ones where active defense capabilities come into consideration.

The Anatomy of Exploitation and Attack

Although security policy experts have put much thought into how to preserve and protect U.S. national security, economic security, human rights, and privacy from cyber threats, the nature of evolving technologies make this an ongoing and challenging task. In order to understand why malicious actors have such an advantage in cyberspace, and why defending against them remains so problematic for both the government and the private sector, it is helpful to have a basic understanding of how computer network exploitations and computer network attacks occur.

The Cyber Kill Chain, originally developed by the Department of Defense, can serve as a strong starting point for this type of analysis. The model divides the life cycle of a hack into three major steps: preparation, intrusion, and active breach; and was developed as a guide for gathering intelligence on cyber attacks that would help defenders secure their systems throughout the life-cycle of a hack. This report’s “anatomy of exploitation and attack” outlined in Figure 1, is a slightly modified model that incorporates details included in other analyses of hacker behavior, such as the InfoSec Institute’s Cyber Exploitation Cycle. Critics of the cyber kill chain argue that it relies too heavily on perimeter-based defense techniques and is therefore less helpful when it comes to describing socially engineered attacks, the insider threat, and other modern methods of cyber exploitation. While it was never intended to be operationalized against all types of cyber exploitation, the true weakness in applying the kill chain to cybersecurity is not that the model overemphasizes intrusions at the perimeter, but rather that those who use the model limit themselves to cybersecurity tools that are almost exclusively geared towards perimeter security. This report will frame the anatomy of exploitation and attack in such a way that is directly relevant to the private sector and can begin to guide cybersecurity practitioners away from limiting notions of network defense.

A modified version of the kill chain concept is a useful tool to analyze the stages of a cyber threat at which certain defensive tactics become relevant. Thus, the anatomy of exploitation and attack will serve as a reference point, as this report continues, to demonstrate where emerging cybersecurity practices can disrupt and defeat cyber threat actors. Furthermore, it will help to visually demonstrate how new cybersecurity practices can fill the gaps that intrusion-based cyber defenses currently leave exposed.

Key U.S. Interests In Cyberspace

Although the number and sophistication of cyber threats continues to grow, the United States has thus far escaped a significant cyber attack that has seriously damaged its critical infrastructure or way of life. How long this relative sense of security can last is unclear. Over the past decade, the arsenal of offensive cyber measures has grown unbounded; botnets, DDoS attacks, ransomware, remote access tools, encryption-based exploitation tools, social engineering, and zero-day exploits are the standards of the day. It will only be a matter of time before an adversary successfully capitalizes on these advantages and carries out an attack that damages and disrupts critical infrastructure. This type of asymmetric threat environment requires a carefully calibrated strategic response and calls for a broader cyber deterrence strategy. Not all threats are deterred in the same manner, however,
so the U.S. must develop and implement a clearly articulated strategy tailored to the unique threat against the private sector.

At present, it is unlikely that any state or non-state actor possesses the combination of capabilities and interests necessary to threaten American sovereignty and freedom of action in or through cyberspace. While the recent Russian hacks on U.S. political entities and related information operations have caused a stir this election cycle, the complexities and redundancies of the U.S. electoral system make it relatively resilient to systemic cyber manipulation. While there is some threat that even the doubt created by information warfare campaigns can impact American sovereignty, thought leaders and government officials have so far been able to dispel any type of widespread distrust in America’s electoral system.29

Though the fundamental sovereignty of the United States is not at issue, other key strategic interests, such as U.S. economic security, may be more susceptible to cyber threats. Private sector enterprise, including technological advancement, protects national economic security by fueling economic development, nurturing the growth of military capabilities, and fostering geopolitical influence.30 Over time, unchecked cyber-enabled theft of private sector data and assets could pose a strategic risk and threat to a nation’s economic security. The cyber-enabled misappropriation of private sector assets may occur directly as a result of the immediate transfer of actual wealth from victim to attacker. Alternatively, such misappropriation could be of an indirect nature, from the manipulation of sensitive information that damages a company’s relationships, value, or reputation. The effect of either type of attack would be to give competitors a competitive advantage. Depending on the nature of such an attack and its target, its effects could devastate individual firms, damage whole sectors, or weaken entire economies.

Effective Deterrence and Active Defense
Since U.S. economic security has a unique susceptibility to malicious cyber activities, the U.S. should craft a cyber deterrence policy that is more focused on protecting the private sector. Effective cyber deterrence will require that government and private sector actors have a robust and diverse array of options, including a more permissive policy on the private use of

---

**FIGURE 1. ANATOMY OF EXPLOITATION AND ATTACK**

<table>
<thead>
<tr>
<th>STAGE 1</th>
<th>STAGE 2</th>
<th>STAGE 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="External Preparation of the Attacker" /></td>
<td><img src="image2" alt="The Intrusion" /></td>
<td><img src="image3" alt="The Active Breach" /></td>
</tr>
</tbody>
</table>
active defense measures. The question of objective is straightforward. The U.S. must cut the drain on the economy and private sector caused by malicious cyber activities. Developing a near-term strategic response within such a context requires prioritizing the most pressing threats facing the private sector.

The long-term strategic response must include a cyber deterrence strategy that actually denies benefits and imposes costs. While actors in the public and private sectors currently attempt to deny benefits to attackers using passive and perimeter-centric defense measures, these defenses alone are outmatched by today’s offensive capabilities. Furthermore, while the government has attempted to contribute to such a deterrence posture by imposing costs on malicious actors, this strategy is complicated by the difficulties associated with attribution, the limited resources and tools available to governments seeking to punish international actors, and other geopolitical factors. 31

Historical patterns and modern technology have created a strategic imperative: American policymakers must develop a framework to defend against the misappropriation of wealth from the private sector. The duality of a global economy in which economic partners may simultaneously be geopolitical adversaries makes articulating an effective cyber deterrence posture complex and unique. Flexibility, innovation, and careful cooperation will be key.

Many senior national security officials have argued that if America is to deter aggression in cyberspace, it needs to pursue a whole-of-government approach to cybersecurity that closely involves the private sector. 32 Together, the public and private sectors will need to implement more reliable tools for cyber defense and attribution. This will require increased information sharing to support awareness, cooperation to coordinate responses, and the constant cultivation of private-public partnerships to support decision-making. Cooperation, however, is not the solution in and of itself. In order to ensure that adversaries cannot effectively threaten the strategic interests of the United States in cyberspace, America must move beyond cybersecurity models that focus on outdated passive defense measures. In order for what is truly a whole-of-nation cybersecurity strategy to succeed, the private sector must be allowed and encouraged to build upon its innovative capabilities and advanced resources to pursue a strategy of active cyber defense.

Active Defense: How the Term has Developed and How it Should be Used Going Forward

Active Defense is a term that has been in use within the national security and defense communities for a number of decades. Since its origins in the Department of Defense and its later application to the cyber domain, it has taken on a whole host of meanings. Today, the legacy of its various and evolving interpretations obscures the utility of a term in a sea of conflicting definitions. A brief history of the evolution of the term is helpful to provide some context before this report proposes a recommended definition for consistent future use in the cyber context.

The distinction between active and passive defense was first discussed many decades ago in the context of the military’s traditional physical land, sea, and air defenses. 33 Passive defenses were understood to be those that provided a limited amount of defense against an adversary without requiring military engagement. 34 A traditional passive defense measure might be a hardened bunker or other add-on security measure that depleted an adversary’s resources by requiring extra effort on the part of the adversary to achieve its goal. 35

In the 1970s, the term active defense began to emerge in U.S. Army lexicon during discussions of land warfare tactics. While analyzing the 1973 Arab-Israeli War, U.S. Army General William E. DePuy, Commander of the Army Training and Doctrine Command, used the term to describe a defensive technique based on mobility. 36 The defender would wear down the attacker by “confronting him successively and continuously with strong combined arms teams and task forces fighting from mutually supported battle positions in depth throughout the battle area.” 37

In order to achieve mobility, the defender needed to
leverage “military intelligence, and indicators to identify an attack, respond to the attack or against the capability within the defensive zone or contested area.”

Even at the time, the term was controversial and hotly debated. The use of counterattacks by the defender was restricted to only the “contested area” against the threat itself. Active defense was directed “against the capability, not the adversary.” In its original sense, active defense techniques gave the defender the ability to quickly adapt to the environment in real-time to address attacks in a proactive way. Over time, the definition used by the military was formalized in the Department of Defense Dictionary of Military and Associated Terms as “the employment of limited offensive action and counterattacks to deny a contested area or position to the enemy.”

Active and passive defense definitions were developed separately, and before the term “cyber” was ever incorporated into military doctrine. Experts have struggled to translate the traditional definitions of active and passive defense into perfect analogues in the cyber context. The SANS Institute has crafted a definition based upon the protective nature of passive defenses: “systems added to the architecture to provide consistent protection against or insight into threats without constant human interaction.” A collection of cooperative automated systems such as firewalls, antivirus or anti-malware systems, intrusion detection and prevention systems, and others fall into this category.

It is similarly challenging to translate physical conceptions of active defense into the cyber domain. SANS has defined cyber active defense as “the process of analysts monitoring for, responding to, learning from, and applying their knowledge to threats internal to the network.” The scope of this definition is limited and therefore this report will introduce, in the following section, a robust definition of active defense with clear examples. The SANS definition precludes hacking back and other activities that occur outside the network, focusing instead on dynamic adaptability as a tool to react quickly to threats overcoming passive defenses. Like the traditional definition in land warfare, the activity is confined to the “contested area” of the defender’s internal network.

For the private sector, discussion of the term active defense has been regularly linked with discussions of the Computer Fraud and Abuse Act (CFAA). In 1989, five years after the CFAA became law, Robert Morris Jr., an MIT graduate student, became the first private citizen prosecuted for releasing what was arguably the first major computer virus distributed through the Internet, the Morris Worm.
Since that time, there have been many CFAA prosecutions aimed at those who have gained unauthorized access to computer systems, raising concerns in the private sector over the extent to which private firms may defend themselves using techniques that may involve information or computer systems external to one’s network without express government authorization.

The private sector, faced with escalating losses from malicious cyber threats, has been discussing the idea of active defense for years. Perhaps the first widely known instance of a private use of active defense measures occurred in 1999 when Conxion, Inc., a web service company that hosted the World Trade Organization’s servers, took action against a denial of service (DoS) attack targeting its servers. Tracing the source of the malicious traffic, Conxion reflected the incoming traffic back at the source, flooding the server with its own outgoing traffic; effectively imposing a “reverse” DoS attack on the attacker.47

In 2004, the company Symbiot, Inc. released the first commercially available security platform that could “execute appropriate countermeasures” against a cyber threat. By offering graduated response levels, the system offered a range of options for the user that exceeded the “passive” defenses of other security products. Symbiot’s press release called their new tool, the “Intelligent Security Infrastructure Management System” (iSIMS) the “equivalent of an active missile defense system” that would allow the user to fight “fire with fire.”48 In keeping with their military analogy, the company also issued a paper on the Rules of Engagement that discussed the application of the military principles of necessity, proportionality, and countermeasures, linking the practice of active defense measures with the military’s historic understanding of the term.49 Importantly, the Symbiot product offered a series of graduated responses, not just a “hack back” solution. iSIMS could implement, among other techniques, challenging procedures, honeypots, quarantines, reflection, and blacklisting upstream providers in an escalating series of options.50

Despite this broad array of options, during the time since the release of iSIMS product, there have been many debates over the issue within the private sector, academia, and government. Today, when active defense is discussed, too often the discussion shifts to “hacking back”—offensive cyber measures that are beyond the scope of what we define as permissible activity in this report.51 This report seeks to more clearly articulate the terminology and public dialogue around the topic.

Defining Active Defense for 21st Century Cybersecurity

Given its diverse usage over a number of decades, when security experts, policymakers, and academics use the term active defense in a cybersecurity context, they tend to have in mind a wide variety of definitions. This lack of a common definition complicates discussion surrounding active defense and precludes meaningful progress on developing a commonly understood framework for its implementation. This is especially counterproductive when it comes to developing policy related to cyber active defense in the private sector.

Sound practice related to private sector active defense is also obstructed by businesses’ increasingly common use of third party services to host sensitive data and information outside of their own infrastructure. This development undermines network defense strategies.
that are based on clearly defined network perimeters and areas of direct ownership. Thus, any relevant definition of active defense will need to consider the gray areas in which businesses may be forced to defend their data on a third party’s infrastructure. With this in mind, the report proposes the following characterization of active defense:

**Active defense is a term that captures a spectrum of proactive cybersecurity measures that fall between traditional passive defense and offense. These activities fall into two general categories, the first covering technical interactions between a defender and an attacker. The second category of active defense includes those operations that enable defenders to collect intelligence on threat actors and indicators on the Internet, as well as other policy tools (e.g. sanctions, indictments, trade remedies) that can modify the behavior of malicious actors. The term active defense is not synonymous with “hacking back” and the two should not be used interchangeably.**

**The Upper and Lower Bounds: Passive Defense and Offensive Cyber**

In order to fully contextualize this definition of active defense, it is necessary to define its upper and lower bounds. Cyber activities can produce effects that manifest within the actor’s own network, outside the actor’s own network, or both. The Center’s definition of active defense includes activities that fall across that range, including some activities that manifest effects, whether logical or physical, outside of a particular actor’s own network or systems.

Activities that produce effects solely within an actor’s own networks are often referred to as passive defenses. They primarily involve the use of perimeter-focused tools like firewalls, patch management procedures, and antivirus software. These can be installed and left to function independently. Passive defenses can also include procedures like white or blacklisting and limiting administrative authorities. While passive defenses are necessary for a sound cybersecurity regimen, they are insufficient by themselves to defend against the most advanced cyber-aggressors.

On the other extreme are those activities occurring outside the actor’s network, and that are aimed at coercing action, imposing costs, degrading capabilities, or accessing protected information without authorization; these could be characterized as offensive. “Hacking back” to retrieve or delete stolen data or to gain information about an attacker’s tools, techniques, procedures, and intents fits into this category, as would a retaliatory DDoS attack, the exploitation of a system to extract intellectual property, or the use of malware to damage a system, such as in the case of Stuxnet. As in other domains of conflict, private sector actors should not be authorized to use these types of tools, except in limited circumstances in cooperation with or under the delegated authority of a national government.

**The Spectrum of Active Defense: A Continuum of Activities**

Active defense measures include those which typically fall between these upper and lower definitional boundaries. Such activities may cross the threshold of the actor’s own network borders, and produce effects on the network of another. These activities, taken in pursuit of a variety of objectives that may be either offensive or defensive, affect the confidentiality, integrity, or accessibility of another party’s data. They are no longer passive in nature, and their characterization depends upon the intent or objective of the actor implementing them. Activities aimed at securing one’s own systems, or preserving operational freedom could be characterized as defensive in nature. Disrupting a malicious botnet, sinkholing traffic from a malicious IP address, and other activities that are taken in direct response to an ongoing threat would fall within this category.

Examples of active defense measures can be found in Figure 2, and are ranked according to their relative impact and risk from left to right. (Definitions for each of these active defense measures can be found in Figure 3). The activities towards the far left of Figure 2 are relatively common and low-risk active defense options such as information sharing and the use of honeypots or tarpits. A computer security expert who uses a honeypot on his or her network can, assuming that the decoy fools the attacker, observe attack techniques and use these observations to inform defenses on the defender’s actual network.
While less common, cyber denial and deception is another low-risk defensive technique that can be used to observe attacker behavior, tailor other active defense techniques, and improve incident response capabilities. It can involve concealing and making apparent both real and false information to skew an aggressor’s understanding of the information contained on a computer system, vulnerabilities in that system, and defenses deployed on a network. The process of hunting for and removing threat actors who have already breached fortified perimeter defenses is surprisingly uncommon, yet a relatively impactful cybersecurity measure for its low level of risk. Hunting is as much about having actionable procedures and responses in place for eliminating threats as it is about exposing them, whether they be active or dormant in a network.

Towards the middle of the active defense spectrum are activities that carry more risk, in that they generally involve operations outside of one’s network, and have the potential to lead to minor collateral damage or privacy concerns if used without the requisite level of precision. These activities include beacons, the use of dye packs, and intelligence collection in the deep web and dark net. Beacons are pieces of code that are embedded into files that contain sensitive information. They can be operationalized in two main ways. First, less impactful beacons will simply alert the owner of a file if an unauthorized entity attempts to remove that file from its home network, acting as a built-in burglar alarm. Second, more aggressive beacons are designed to return to the victim information about the internet addresses and network configurations of the computer systems that a stolen document is channeled through, ideally assisting with attribution and forensic evaluation of remote devices.

Increasingly, network defenders are realizing that the information that travels through the dark net can be helpful to inform defensive strategies and alert information security officials of a breach. This realm of the Internet—in which websites are dissociated from traceable servers, user anonymity is common, and information travels between trusted networks of peer groups—is popular for criminal trade in stolen information and malware services, and thus offers a promising trove of human intelligence possibilities for network defenders. For example, a bank’s security team can search through illicit marketplaces and compare the personal or financial information on sale with the information the bank keeps on its custom-
Information Sharing
The sharing of actionable cyber threat indicators, mitigation tools, and resilience strategies between defenders to improve widespread situational awareness and defensive capabilities.

Tarpits, Sandboxes & Honeypots
Technical tools that respectively slow hackers to a halt at a network’s perimeter, test the legitimacy of untrusted code in isolated operating systems, and attract hackers to decoy, segmented servers where they can be monitored to gather intelligence on hacker behavior.

Denial & Deception
Preventing adversaries from being able to reliably access legitimate information by mixing it with false information to sow doubt and create confusion among malicious actors.

Hunting
Rapidly enacted procedures and technical measures that detect and surgically evict adversaries that are present in a defender’s network after having already evaded passive defenses.

Beacons (Notification)
Pieces of software or links that have been hidden in files and send an alert to defenders if an unauthorized user attempts to remove the file from its home network.

Beacons (Information)
Pieces of software or links that have been hidden in files and, when removed from a system without authorization, can establish a connection with and send information to a defender with details on the the structure and location of the foreign computer systems it traverses.

Intelligence Gathering in the Deep Web/Dark Net
The use of human intelligence techniques such as covert observation, impersonation, and misrepresentation of assets in areas of the Internet that typically attract malicious cyber actors in order to gain intelligence on hacker motives, activities, and capabilities.

Botnet Takedowns
Technical actions that identify and disconnect a significant number of malware-infected computers from the command and control infrastructure of a network of compromised computers.

Coordinated Sanctions, Indictments & Trade Remedies
Coordinated action between the private sector and the government to impose costs on known malicious cyber actors by freezing their assets, bringing legal charges against them, and enforcing punitive trade policies that target actors or their state sponsors.

White-hat Ransomware
The legally authorized use of malware to encrypt files on a third party’s computer system that contains stolen information in transit to a malicious actor’s system. Public-private partners then inform affected third parties that they have been compromised and are in possession of stolen property, which they must return in order to regain access to their files.

Rescue Missions to Recover Assets
The use of hacking tools to infiltrate the computer networks of an adversary who has stolen information in an attempt to isolate the degree to which that information is compromised and ultimately recover it. Rarely successful.
ers and their accounts. If the security team discovers a significant match, then it is likely that a hacker breached their network and successfully stole sensitive data without raising the alarm. Defenders, now alerted to the presence of a network vulnerability, can seek to shore up cracks in their security architecture and boot intruders off their system before any more information is compromised.

Those active defense activities that approach the rightmost extreme of the spectrum in Figure 2 are the most aggressive. Private entities should only utilize such measures, as the figure suggests, when working in close cooperation with the government. These activities include sinkholing botnet traffic and taking down the infrastructure of botnets or criminal forums. Botnet takedowns have, up to this point, proven to be some of the most effective partnerships between government and private actors seeking to cooperate on more forward-leaning categories of active defense. The numerous instances of cross-sector and inter-jurisdictional partnerships that have operated under legal authorities to successfully sinkhole botnets provide hope that public-private coordination is possible in cyberspace.60

The group of non-technical actions that appear in Figure 2, coordinated indictments, sanctions, and trade remedies, are not active defense measures in the purest sense, but require mention in this conversation due to the technological underpinnings that facilitate requisite attribution. The investigative tools that are required to confidently attribute malicious cyber activity to an entity can be invasive and thus require close cooperation with the government. The legal and trade implications that follow from such activities would not be possible in many cases without private sector contributions and can contribute significantly to a cyber deterrence posture.

Other active defense measures that are more aggressive and risky include white hat applications of ransomware, and the often discussed and widely inadvisable “rescue mission” for information that has already been stolen from one’s network. While the malicious use of ransomware has become one of the most worrisome trends in cybersecurity over the past year, security experts have considered the possibility of using similar tools to encrypt stolen data that is in transit on a third party’s network. In such a manner, they could inform a third party that hackers had compromised their network and were using it to transmit stolen data. Instead of the warning screen that usually tells victims to pay a ransom in bitcoin, white hat ransomware would inform network administrators that they should contact law enforcement, which can retrieve the stolen information and then remove the ransomware from the third party’s computers. There are legal risks, however, with this approach, as well as a new security risk that such warning notices could be spoofed for phishing attacks that lead to further compromises.

While technically feasible, operations in which defenders attempt to retrieve stolen information from adversary networks, even when the intent is not to alter or destroy any of that adversary’s other legitimate data, are not likely to succeed and are inadvisable. The difference between such “rescue missions” and the much maligned “hack back” is in the intent of the defender: whether he or she is looking to retrieve what was stolen or to inflict damage. Both are high risk and often ill-fated from the start. The moment an advanced adversary captures stolen information, they are likely to protect it by replicating and hiding it within their network or backing it up offline. Due to the low likelihood of achieving a beneficial outcome, even if government partners were to be involved, such operations are again, inadvisable.

Active Defense as it Intervenes in the Anatomy of Exploitation and Attack

Together, these activities make up the current spectrum of private sector active defense measures. Figure 4 demonstrates how active cyber defense strategies can fortify the efforts of security experts to disrupt attacks at various stages within the anatomy of exploitation and attack. The lines in Figure 4 show where certain active defense measures have significant capacity to interdict cyber exploitations and attacks. Many of these measures impact adversary behavior at multiple stages, but for clarity’s sake, Figure 4 explicitly shows only those connections with the highest impact. Passive defense strategies alone usu-
ally focused on preventing and detecting intrusions. Alternatively, active defense techniques allow organizations to potentially interrupt attackers in all three stages of a hack. When defenders fail to implement active defenses, cybersecurity cannot reach its full potential to deny benefits to attackers throughout the entire duration of the hack.

While discussion surrounding specific security technologies or techniques is necessary to illustrate different aspects of active defense, it is important to note that such technologies are likely to have relatively short shelf lives. The key takeaway from this discussion is therefore not the specifics of how a honeypot works or how to sinkhole a botnet. Instead, the goal is to show how such tools and techniques exemplify the concept of a range of active defense activities that can be helpful in addressing current cyber vulnerabilities. Broadly speaking, active defense measures can help to directly inform threat assessments and cybersecurity priorities, protect a business’ “crown jewels” within a network, assist in reliable attribution, recover stolen information, and neutralize threats.

Active Defense Case Studies

Before turning to a broader policy discussion of the private sector and active defense against cyber threats, it is
useful to examine two instances where private entities have used active defense measures (as we have defined them) to mitigate or disrupt cyber threats. Both of these brief vignettes are drawn from open source information, and provide useful insights into the kinds of threat scenarios that necessitate active defense and the ways in which private actors have legally and effectively implemented active defense strategies. With the conclusion of each case study, this report discusses broad takeaways that relate each case to the calculations that today’s executives must make when shaping their approaches to cybersecurity and cyber incident response.

Google’s Response to Operation Aurora

The response of Google to the Chinese-linked hacking campaign that security researchers at McAfee dubbed, “Operation Aurora,” provides a detailed case study of how a particularly skilled private sector actor has used active cyber defense measures to protect its security interests. After Google became aware of a “highly sophisticated and targeted attack” on its networks and corporate infrastructure in late 2009, it decided that a timely response to the breach was necessary. Therefore, internal security teams began a campaign to assess the scope of the breach and investigate the attackers themselves. They found that these attackers had targeted user accounts, many of which were associated with individuals the Chinese government considered to be political dissidents; and Google’s source code, a critical corporate asset and significant piece of intellectual property. If the hackers had been able to alter the source code while remaining undetected, they could have built vulnerabilities directly into Google’s product plans.

As a large technology firm, Google’s leadership decided it had the resources to support a mission to operate outside of its network to track down the attackers. Its search led to a command and control server in Taiwan. Google found that the attacks were likely being controlled from China and that Google was among a group of at least 30 other targeted companies. With this information in hand, Google took the unprecedented step of sharing its findings with law enforcement, the intelligence community, the companies involved, and even the public.

Google’s decision to carry out this type of response and subsequently make it public carried with it legal and reputational risks. Although the details of the Aurora hack on Google are well documented, it remains unclear how exactly Google traced and entered the Taiwanese server. If, as has been reported, it entered the foreign computer without authorization, Google’s actions could be interpreted as a violation of the Computer Fraud and Abuse Act (CFAA), potentially subjecting it to civil or criminal liability. However, U.S. government agencies chose not to take action against Google, and instead admonished China while praising the value of Google’s investigative efforts. To date, the government has not prosecuted a single company for engaging in active defense measures similar to Google’s, although it does warn others of its authority to do so.

The impacts of Google’s response to Operation Aurora on the conversation surrounding active defense are manifold. First, Google’s apparent use of a beaconing technology and its network investigation techniques demonstrate that attribution is not impossible and that the private sector can be a useful partner to the government in this endeavor. Second, this example must be considered in the context of Google’s size, influence, and technical sophistication. Not just any private business could have supported this type of response and not all businesses should consider engaging in such a response.

Third, the lack of an identifiable victim of Google’s countermeasures, whether the intended targets of such
action or innocent third parties, likely contributed to
the fact that the Department of Justice never brought
suit against Google. Had a private company's actions
causation damage on the network of a readily identifiable
victim with commercial interests in America or Asia, they
would have likely led to prosecution, regulatory
action, or civil action under the CFAA or foreign legal
authorities. In such a counterfactual, Google's actions
and the legal fallout could have considerably tarnished
the company's reputation and bottom line. All execu-
tives engaging in active defense must consider these
potential consequences in conjunction with the risk of
taking no action at all. After all, failure to act entirely
could result in even more significant consequences to
a business' reputation and bottom line. C-suite execu-
tives should take each of these considerations into their
risk analysis when developing a cyber strategy.

The Dridex Botnet Takedown

The takedown of the Dridex/Bugat botnet is another
helpful case study of how defenders have successfully
implemented active defense strategies. The partner-
ship between international law enforcement agencies
and private sector actors to dismantle the command
and control (C&C) infrastructure of Dridex illustrates
how multilateral partnerships that draw on diverse
partners with a range of authorities and expertise can
disrupt cybercrime and penalize criminals.66 Dridex
was a banking Trojan that was spread through spam
emails. It would steal online banking credentials that
criminals would use to fraudulently transfer money
into accounts they controlled. This botnet dispropor-
tionately affected small- and medium-sized business-
es in the U.S. and Europe.67

The Dridex botnet, which security researchers first
discovered and significantly analyzed in November
of 2014, breached thousands of organizations across
27 countries and led to losses in the UK of about
$30.5 million and $10 million in the U.S.68 Cyber
criminals used this malware to fill the void left by
the similarly purposed Gameover Zeus botnet and
designed it so that it could avoid common antivirus
software.69 These designs, coupled with its use of a
resilient peer-to-peer C&C structure, made it a chal-
lenging botnet to combat. However, by October of
2015, U.S. and U.K. government officials announced
that the botnet had largely been dismantled through
close cooperation between multiple private sector
entities and other government agencies.70 Together
they had redirected the malicious commands of the
C&C servers to a sinkhole that the Shadowserver
Foundation administered.71 The Dridex takedown
operation did not remove malware from infect-
ed machines, leaving bots vulnerable to re-infec-
tion and future manipulation.72 As in similar bot-
et takedowns, individual users and their security
vendors were responsible for cleaning up their own
computer systems. Coordinating remediation ef-
torts continues to be a major burden to implement-
ing botnet takedowns.73

Significantly, American law enforcement obtained
a court order before taking action against the bot-
net's C&C servers. Coinciding with the takedown
announcement, the US Justice Department indicted
a Moldovan national, Andrey Ghinkul, on a number
of counts related to operating Dridex, which included
“criminal conspiracy, unauthorized computer access
with intent to defraud, damaging a computer, wire
fraud, and bank fraud.”74 In February of 2016, the U.S.
successfully extradited Ghinkul from Cyprus.75

There are three major points to take from this case
that are broadly applicable to discussions surrounding
cyber threats to the private sector and active defense.
First, the fact that Dridex led to significant financial
losses, disproportionately affecting small- and medi-
ium-sized businesses, demonstrates the severity and
ubiquitous nature of the cyber threat to all actors in
an economy. Big banks and giant retailers are not the
only victims in the current threat landscape. Second,
the Dridex takedown exemplifies how public and pri-
ivate entities pool resources in order to tackle a com-
mon threat. Because sinkholing botnet traffic can be
aggressive in the context of computer trespass norms,
law enforcement and the private sector sought legal
approval before taking action. Finally, this case shows
that attribution in cyberspace can be successful and
can lead to significant legal costs for cyber criminals.
Imposing real costs on these criminals is crucial to
removing critical talent from cybercrime circles and
to deterring individuals from engaging in such crime.
The Current Policy, Legal and Technology Context

THE PRIVATE SECTOR TODAY is situated on the equivalent of the front lines of battle: sophisticated and determined actors (“advanced persistent threats”) pose serious threats to U.S. companies. Foreign nation-state security and intelligence forces and their proxies, either actively sponsored or passively sanctioned, increasingly target U.S. businesses for a range of reasons and purposes including computer network exploitation (CNE) and computer network attack (CNA). These actors seek, among other things, to disrupt normal operations, to steal intellectual property, and to map networks that support critical U.S. infrastructure and services such as the electric grid.

Yet the extent to which the private sector can act to thwart these and other cyber threats is limited by policy and law. The current legal framework in the U.S. maintains certain domains of action in this regard as the exclusive preserve of government, which in turn gives rise to interdependencies between the targeted entity and federal authorities. Robust and adaptive partnerships between the public and private sectors are therefore required to meet ongoing evolving and future cyber challenges.

Appendix II to this report identifies and analyzes the legal instruments and common law principles that are most relevant to this study. It includes two U.S. statutes, the CFAA and the Electronic Communications Privacy Act (ECPA), as well as an overview of the common law theories of trespass, self-defense, and necessity. Collectively, these instruments and principles provide a useful starting point for analyzing the legality of accessing a computer that you (the hacker or his target) do not own or have authority to operate. Pursuant to statute, whether (or not) access is “authorized” is pivotal, and is factually determined on a case-by-case basis. The body of law on this issue is ambiguous however, and parties to litigation have invoked (with varying degrees of success) supplemental legal principles and doctrines—such as necessity, defense of property, and implied consent—to make their case before the courts. What is clear is that under U.S. law, there is no explicit right to self-defense (“self-help”) by private companies against cyber threat actors.

Since “authorization” is the key requirement for any actor to access any computer network or system, a victim who wishes to implement offensive measures against an attacker must be authorized to intrude upon or act within the attacker’s network. Since this is unlikely to ever be the case unless previously authorized by contract, U.S. law is commonly understood to prohibit active defense measures that occur outside the victim’s own network. This means that a business cannot legally retrieve its own data from the computer of the thief who took it, at least not without court-ordered authorization. Moreover, measures that originate in your own network—but whose effects may be felt outside your perimeter—may also fall afoul of the law. While the exercise of prosecutorial discretion by the Department of Justice may temper formal legal bounds, it should also be understood that U.S. attorneys will not prioritize the
prosecution of attackers over defenders, meaning that anyone who oversteps places themselves in potential legal jeopardy. 80

Multiple considerations are said to underlie the restrictive nature of the U.S. regime. The law seeks to protect third parties that could suffer significant incidental damage and prevent escalation of the conflict, with possible concomitant effects on U.S. foreign relations. Without concerted de-confliction efforts undertaken in advance, ongoing U.S. law enforcement investigations could be hindered, or security research could be affected. And, to the degree that the activity pursued by the targeted private party reaches into foreign jurisdictions, those (non-U.S.) laws may also be offended raising concerns over the possibility of foreign penalties and extradition requests. The difficulty of attack attribution in the cyber context presents a further risk, giving rise to the possibility of harm to third parties, resulting from mistaken belief in their guilt.

Juxtaposed against this legal framework is an ecosystem of rapidly evolving technology. Advances in machine learning and machine-speed communications have served to propel automated processes for detecting cyber threats, sharing threat-related information, and responding swiftly. These technologies are being used increasingly in both the public and private sectors, and across them. 81 Internet-based cloud technologies, too, will continue to open up options for businesses whose size and accompanying resource level might otherwise constrain their capacity to defend themselves against cyber threats. Cloud computing is a boon to small and medium-sized businesses as it allows them to scale up or down, and pay accordingly, based on their prevailing need for specific services. 82 The point is not academic as threat actors have targeted companies of all sizes. 83

It is also reasonable to expect that, over time, R&D will generate ever-new technologies that can enhance the private sector’s ability to meet and defeat cyber threats. On the other hand, threat actors will also find ways to exploit new technologies to their advantage, such as the Internet of Things, which dramatically expands the potential surface of attack. 84

While technology is a double-edged sword that can serve both to protect and harm, the bounds of the prevailing legal framework can be—and have been—pushed by those with an appetite for risk, fueled by the desire to practice self-help. Companies with substantial resources, for instance, have pursued measures outside the United States in order to secure their assets from cyber threats in a manner that U.S. law would not countenance. 85 The circumstance arises in part because companies are unwilling to passively place their fate in the hands of the U.S. government. This lack of confidence is premised on multiple concerns, including serious doubt that governments possess either sufficient skill or the sustained determination and resources required to pursue perpetrators effectively, and provide adequate remediation—which is essential to deterrence and prevention, moving forward.

These points are well taken in that government cannot be expected to successfully deter cyber attackers targeting U.S. public and private sector interests everywhere, all the time. The challenge is compounded, ironically, by the private sector’s ability to outbid the government for highly skilled cyber experts. A sense of mission is powerful, but the appeal to public service in the national interest (along with other factors that animate individuals to join the civil service) have yet to result in filling the many critical cybersecurity positions and functions in government that remain open. 86 In the longer term, this situation could be redressed by growing the pool of qualified candidates, by deepening and expanding U.S. efforts to encourage our young people to undertake and continue studies in science,
technology, engineering, and mathematics (STEM). But companies need a fix for today, because the existing framework which structures the relationship between the public and private sectors is not sufficiently responsive to the needs of business, given the current cyber threat climate and tempo.

Yet, private sector actors are less engaged than they could be, despite being a potential source of the very resources and expertise that the government lacks. By and large, companies are not pursuing—either independently or in partnership—the actions that are needed to create a strong deterrence posture benefiting from active defense. This disengagement is due to many things: legal ambiguity, risk aversion, limited resources, lack of coordinated leadership, and lack of awareness of active defense.

Legal ambiguity exists at the international level as well, where the framework applicable to the cyber domain remains nascent. The Council of Europe Convention on Cybercrime (the Budapest Convention) includes a definition of “Illegal Access” that may help to define the boundaries of permissible active defense measures. Several countries are developing their own approaches to the question of active defense (see Appendix III). Global norms, though emergent, are at present not sufficiently developed so as to be determinative, which compounds companies’ quandaries.

Those who take bold (and arguably incautious) steps to protect stolen assets will, even if initially successful in practice, achieve but a Pyrrhic victory if a company’s hard-earned goodwill is dissipated by ensuing litigation. Moreover, taking independent action or joining forces with others to frustrate and deter cyber threat actors presumes that businesses have the wherewithal (technical and otherwise) to do so; but this is not a given for many in a tough economy in which many and varied company goals and objectives compete with one another, and there are only so many hands on deck to achieve them. At the senior executive level, furthermore, cyber knowledge and the drive to prioritize measures (e.g., prevention and mitigation) in this domain are uneven. Within and across industry sectors there is significant variation in levels of awareness about active defense, as well as in the level of resources (amount and quality) that are available.

There are a number of current initiatives that illustrate how the private sector can play a lead role in thwarting cyber threat actors. Examples include the Cyber Threat Alliance (CTA), which strives to share “actionable threat intelligence” among its members. Notably, the CTA has acted jointly to expose and counter ransomware attacks that caused damage worldwide, valued at more than $300 million. Without sustained and coordinated leadership though, laudable efforts such as this will re-
main limited in their effects and result only in hit and miss rates of success.

The upshot is that private entities, which did not get into business to defend their information and infrastructures against sophisticated cyber actors, are forced to do just that. This is an unsustainable position.

In the remainder of this report, we put forward a new framework that attempts to addresses the challenges outlined here—most fundamentally, that the status quo leaves America vulnerable to significant cyber threats. With the private sector often looking to be more aggressive, but hamstrung by the potential for serious risks and unintended consequences, U.S. companies need clarity on what they can and cannot do. These parameters should be defined in advance, as the product of a careful deliberative process—rather than in the heat of the moment, when a mindset to avenge may exist, or a cycle of regression may take hold due to a hack that has unintended consequences.
TO GENERATE THE FRAMEWORK contained in this report, the Center brought together a diverse group of expert stakeholders, convening a Task Force whose members have backgrounds in the private and public sectors, and are thought leaders in the areas of technology, security, privacy, law, and business. Led by the four Task Force co-chairs, the Active Defense Task Force on four separate occasions for working sessions. The meetings addressed a range of fundamental themes and challenges, including: the policies and laws governing active defense against cyber threats both inside and outside the United States; existing and emerging technologies for protecting against cyber threats targeting the private sector; and corporate best practices for protecting and defending systems.

Task Force co-chairs and Center staff also consulted widely with stakeholders across the country, including financial sector executives in New York City, senior U.S. government officials in Washington, D.C., and a range of Silicon Valley technologists, through interviews conducted either in person or by telephone. The majority of these interactions and exchanges took place under the Chatham House Rule in order to encourage free and full discussions of the issues under study.

Ultimately, the many findings produced by these expert conversations were distilled and developed into key principles that were debated, refined, and placed in context in this report. While the members of the Task Force found common ground and reached agreement on many aspects of this discussion, they did not reach a consensus opinion on all issues discussed below. The findings and recommendations of this report, as informed by the deliberations of the Task Force, were therefore produced and refined by the co-chairs, and should be interpreted in the context of the additional views of Nuala O’Connor, as expressed in Appendix I.
AFTER THIS EXTENSIVE PROCESS of consultation and review, the report offers a risk-based framework for private sector active defense that strikes a balance between the risk of inaction in the face of escalating cyber intrusions, versus the risk of overly aggressive responses that could escalate, backfire, or harm innocent third parties.

The core of this framework is the spectrum of active defense measures defined in Figures 2 and 4 of this report. These measures are embedded within a broader set of policy, legal, technical, and governance-related considerations, which provide the basis for risk-driven deliberation and decision-making, both within companies and between the government and the private sector, on active defense. This framework can guide and influence both short-run decision-making (i.e. how to respond now to an attack), as well as longer-term investment and capacity-building.

The framework seeks to maximize the effectiveness of the private sector’s ability to defend its most valuable data and assets. We propose to expand the private sector’s latitude for action, so that companies may take limited yet appropriate actions to protect themselves against various types of cyber threats, including the theft and exfiltration of data. But we also propose to embed these authorities to act within a policy and legal framework that is risk-driven and accounts for companies’ relative capabilities to engage in such actions. We propose that such private sector actions should be considered within a broader framework of public-private cooperation on cyber threats, so that government legal authorities and investigative capabilities can be used in concert with private sector action, and to ensure de-confliction of efforts. The implementation of such a framework will raise costs for and reduce benefits to attackers, dissuading and deterring threats over time. It will also ensure that measures are proportional to the threat and will restrain harmful or unlawful actions. For those actors already engaged in active defense measures, it will provide guidance to ensure their measures fall within the bounds of the law.

This framework recognizes that a broad suite of technical and non-technical tools is applicable to the countering of cyber threats to the private sector. In addition to purely technical active defense measures, this includes such activities as information sharing, and intelligence collection, as well as broader policy tools such as sanctions, naming and shaming through technical attribution, indictments, and trade remedies. These non-technical activities and tools are informed by technical approaches to cybersecurity and cannot be excluded from conversations on active defense and cyber deterrence. While such actions are typically the purview of government actors, the resources of the private sector are valuable when implementing such policies in cyberspace due to the Internet’s dispersed and bottom-up design. Closer cooperation between domestic, private actors and government agencies that implement such policies is thus desirable. In fact, coordination between government and business
is required in most realms of active defense. A strong framework will help to alleviate the advantage that malicious actors gain from current ambiguity in terms of who takes the lead in defending businesses in cyberspace. The framework would also provide for greater transparency and accountability in private sector active defense.

The framework also balances the need to enable private sector active defense measures with other important considerations such as the protection of individual liberties, privacy, and the risks of collateral damage. While a strong framework for responsible active defense will bolster the tools that the private sector can employ to safeguard the privacy of their customers' sensitive personal information, the importance of guaranteeing the responsible use of active defense measures cannot be overstated. Activities that extend beyond the networks that a company is authorized to access raise legitimate privacy concerns (among other issues) for innocent third parties, so the framework must ensure that any measures taken by the private sector are proportion- al to the threat and limited in scale, scope, duration, and effect. By providing a clear framework for these activities, practices that exceed or circumvent the framework’s carefully crafted best prac- tices may be curtailed before undue infringement on the privacy rights of innocent parties can occur. There are a variety of oversight mechanisms and legal reporting requirements that could be utilized to ensure that such consider- ations are integrated into the framework.

A key aspect of this framework is a risk-driven methodology that can be used to weigh the risks and benefits of action vs. inaction, and to then choose and utilize appropriate tools if and where actions is warranted. As discussed later in the paper, government should work with the private sector to establish such a risk-driven methodology, developing it through an open, consultative process.

Key Actors in the Active Defense Framework

Before looking at how this framework can be used, we need first to understand the capabilities and interests of the key actors within it. The framework’s first relevant set of actors includes the various businesses that make up the U.S. private sector. The Task Force quickly recognized that due to the enormous diversity of private entities operating in the United States, not all sectors operate at the same level of sophistication. Referring only to the capacity of the “private sector” as a whole is an overgeneralization. Indeed, there is no “single” private sector. While many “mom-and-pop” shops operate with only the most basic firewalls installed on their computers, others, like the defense, technology, finance, and energy sectors, have developed and actually employed comparatively advanced cyber defense capabilities to protect their networks.

Many large companies utilize advanced cyber capabilities that cross into a “gray area” of activities that fall below the level of hacking back but still push the limits of current U.S. law. In 2013, the FBI investigated whether a number of U.S. banks had used active defense techniques to disable servers in Iran that were conducting malicious attacks against their networks. No charges were brought, but major banks reportedly advocated strongly for such activities. The next year, an industry coalition including Microsoft, Symantec, and Cisco dismantled a sophisticated, allegedly Chinese-backed APT known as Axiom, removing the group’s malware from 43,000 computers around the world. Today, companies in the United States and Israel are selling increasingly advanced cybersecurity solutions to top financial and defense firms that push the limits of measures that can be fairly called “passive defenses.”

Many private sector actors are increasingly implement- ing their own progressively aggressive defensive
measures because they believe the government has failed to offer adequate protection. Advanced actors within the private sector often believe their own abilities to react quickly to defend their networks make them more effective defenders of their data than law enforcement or other government entities. For private entities operating in a market where safeguarding customer privacy is a top concern and reaction times are often measured in nanoseconds, waiting for the government to come to the rescue is not enough. If a proper balance is struck that allows the private sector to react to threats to its networks without overly burdensome laws and policies, the private sector can be a vital player in ensuring the nation’s economic security.

The other key actors incorporated into the active defense framework are the various executive branch agencies (including law enforcement and regulatory agencies) that have cybersecurity responsibilities and Congress. Although the state has historically been responsible for protecting its citizens and private sector from external threats, due to limited resources and available personnel, it is unlikely the government will ever be able to fully respond to cyber threats that do not directly and substantially threaten the national interest. Protection of public networks alone already consumes much of the government’s cybersecurity bandwidth. At the current rate, the government is failing to address the most common and widespread threats to the private sector: those that can overcome firewalls and other passive security measures, but fail by themselves to rise to the level of national security threats. Unfortunately, while such malicious activities do not garner the full attention of the government, the sum of their impacts can grow to such a degree that they do collectively pose a major threat to economic and national security. This dangerous reality will only intensify in coming years. As the rapid development of the “Internet of Things” suggests, the private sector faces a growing attack surface and an increasing array of vulnerabilities inherent in their products, services, and operating procedures.

Despite the growing security gap, the government is the sole actor with the prerogative to engage in techniques like “hacking back” that involve accessing a system outside a defender’s networks with the intent to disrupt or destroy parts of a computer system. Though the CFAA prohibits “unauthorized access” to a computer, Congress specifically excluded from coverage “lawfully authorized investigative, protective, or intelligence activity” of law enforcement and intelligence agencies. The Department of Justice is clear...
that without law enforcement authorization and outside of direct cooperation, hacking back is a violation of the CFAA, subject to civil and criminal penalties. Conspicuously absent from the legality discussion by DOJ officials are those active defense activities that fall below the level of hacking back, such as intelligence gathering, beaconing, and sinkholes.

Operationalizing the Active Defense Framework

The first step necessary in creating an effective environment for the use of active defense techniques by the private sector is for the government to eliminate the legal “gray areas” by more clearly and explicitly defining which types of techniques fall within the bounds of the law. This can be accomplished by assigning a legal or other categorical status to certain characteristics of an active defense technique. There are a number of relevant characteristics that could be considered in such an analysis, including temporal, functional, effects-based, and location-based factors.

A first consideration is the point during the attack at which the defender utilizes the active defense measure. Is the technique used preemptively, during, or after an attack? Stopping an ongoing attack is likely to be considered more legitimate than a retaliatory or otherwise post hoc attempt to recover or deny the attacker the benefits of their attack. A second useful consideration is the technique’s intended function. Is the purpose to collect intelligence on a threat, to prevent an attack from ever occurring, to end a network attack, to mitigate damage, retrieve stolen assets, or impose costs on the attacker? A corollary consideration is how the technique affects the confidentiality, integrity, or accessibility of data. Society may find some effects, such as “observation” or “access” more acceptable than the “disruption” or “destruction” of data.

A cyber activity may also be categorized based on its effects and location. Is the effect felt purely within the defender’s network, or on outside networks such as on the attacker’s or that of some third party? Though such activities are at times desirable, such as the automatic removal of malware or patching of a vulnerability, any damage to the data or networks of an innocent third party would need to be remedied.

Cloud computing and the distributed architecture of the Internet itself make identifying specific individuals difficult, particularly if malicious actors are using proxies to carry out their activities.

Next, is the active defense measure authorized, whether by an oversight body, law enforcement, or the owner of the affected network? As discussed before, botnet takedowns have become a common mechanism for the government and private sector to cooperatively address cyber threats. These operations have primarily been conducted in a partnership with law enforcement, bolstered by the authority of a court order. Law enforcement and other public sector entities are likely to view a defender’s defensive measures in a more favorable light if they are given a cooperative role or otherwise have some oversight authority.

Finally, is the entity that is carrying out the measure capable of doing so in a way that maximizes its efficacy and minimizes the risk of negative consequences, such as collateral damage to other systems or networks or potential escalation?

Both the government and the private sector can benefit from careful consideration of these factors. The government should institute a strong declaratory policy detailing the characteristics of active defense techniques it believes fall within the bounds of the
The existence of such a declaratory policy would encourage the private sector to carefully consider these factors whenever engaging in active defense measures. With a clear characteristics-based legal framework, it would be possible for a private actor to assess the legality of a particular activity or technique on a case-by-case basis.

The characteristics-based analysis would not be complete without a strong risk assessment process that weighs the risks of using a particular active defense technique against the risk of failing to do so. Such an analysis must be broad and consider not just primary consequences to the information systems involved, but also second and third order consequences such as the privacy rights of those potentially affected. Any newly developed techniques must undergo careful consideration before being implemented to ensure they fall within the bounds of the law and sound policy.

This type of analysis will be useful in expanding the range of options open to the private sector when faced with attacks against their most valuable assets and data. Although flexibility and adaptability in the face of technological change are hallmarks of this type of characteristics-based analysis, there are certain principles that should serve as bright lines for the extreme ends of the spectrum of acceptable cyber defensive measures.

First, “hacking back” by the private sector to intentionally cause substantial harm and destroy other parties’ data is clearly unauthorized and rightly prohibited. These types of activities clearly fall within the type of behavior prohibited by the CFAA and other relevant U.S. laws like the Cybersecurity Act of 2015 and the Federal Wiretap Act. From a policy standpoint, these techniques are likely to escalate incidents because they are likely to be disproportionate, difficult to adequately contain, often retributive, and imprecise. Activities such as hacking back to retrieve stolen data or infecting the attacker’s own systems with malware are likely to be ineffective. Stolen data likely exists in a multitude of locations both inside and outside of the attacker’s networks. It is unlikely that an attempt to retrieve stolen data would remove it from every location where it is stored; the risk of escalation in exchange for uncertain gains is simply too high. These types of cyber defense activities should continue to be prohibited.

On the other side of the spectrum are activities such as firewalls, internal traffic monitoring, intrusion detection, hunting, and information sharing systems that identify and target threat signatures and indicators of compromise. These activities primarily involve analysis of the defender’s own logs and traffic data to search for malware or other irregularities. Automation of these processes along with vigilant adherence to other cyber hygiene best practices will continue to provide a minimal layer of defensive protection against an onslaught of malicious threats. These activities occur primarily within the defender’s own network, and do not intrude on the data or networks of any other party. They are both legal and fundamental to a strong cybersecurity regimen.

Other activities, such as the use of beacons, honeypots or tarpits, remote intelligence gathering, and denial by deception, which may have traditionally fallen within the legal “gray areas,” should be analyzed using the proposed characteristic-based approach recommended by the Task Force. As new technologies and defensive techniques emerge, they too should be analyzed on a case-by-case basis in order to ensure they are compatible with the principles outlined above. Any activity must be necessary, proportional, and capable of being minimized to contain potential unanticipated consequences. Before any defensive mea-
sure is implemented, a defender should be required to assert a positive identification of the hostile actor with near certainty, relying on multiple credible attribution methods. These types of considerations, if undertaken by C-suite executives, attorneys, CISOs, and IT professionals allow for the use of a rapid and flexible roadmap for approving defensive measures.

Even without a change in the laws, the Department of Justice and other law enforcement agencies should exercise greater discretion in choosing when to enforce the CFAA and other relevant laws, and should provide clarity about how it intends to exercise such discretion. Companies engaging in activities that may push the limits of the law, but are intended to defend corporate data or end a malicious attack against a private server should not be prioritized for investigation or prosecution. Instead, only the most serious threats deserve prioritized attention. The government has a real role to play when it comes to private sector cybersecurity, but it should use its limited resources to first address corporate espionage, organized crime, and malicious activities sponsored by foreign governments.

To date, the government has refrained from prosecuting any of the firms that have engaged in active defense, even those that purportedly did so without authorization from law enforcement. However, those pioneering the use of active defense techniques have primarily been well-known titans of their industries, such as Google and Facebook, with myriad connections to U.S. government sources. As the number of firms using active defense techniques increases, without significant legal and policy changes and increased clarity and transparency of prosecutorial discretion, the government will likely feel pressured to prosecute defending firms more often.

This pressure can be resisted. In the past, federal agencies have offered guidance on interpreting federal statutes that could impose liability on individuals and companies engaging in cybersecurity efforts. In 2014, the Department of Justice and Federal Trade Commission issued a policy statement declaring that reasonable information sharing for cybersecurity purposes would not be considered a violation of antitrust law. This assurance was codified by the Cybersecurity Act of 2015. Just as prosecutors avoid stifling legitimate cybersecurity research and refrain from overly aggressive enforcement of antitrust law, the government should avoid blocking private defensive measures through an overzealous use of the CFAA’s criminal provisions.

The framework also recommends strengthening existing public-private partnerships and creating new processes to facilitate private sector entities’ ability to respond to threats to their networks. As discussed above, in recent years, companies have been working hand-in-hand with law enforcement entities to dismantle giant networks of remotely controlled computers used for malicious attacks, called botnets. Botnet takedowns have largely been conducted by major private sector actors working jointly with law enforcement to employ advanced active defense measures against the botnet’s command and control servers. In 2013, Microsoft, in cooperation with international law enforcement partners and facilitated by the FBI, successfully dismantled 1,000 networks used by the Citadel Botnet to target a number of major financial institutions. Since 2013, law enforcement and engaged members of the private sector have worked in cooperation based upon the Citadel model of public-private cooperation.

Although botnets will continue to be a problem, these takedowns illustrate just how effective private sector actors can be in defending their own networks from malicious activities while operating within the bounds of the law. Without the fear of legal consequences, security experts were able to implement robust measures to shut down the botnets and remove harmful malware from computers and networks worldwide. This report recommends streamlining this type of process to make the legal procedures necessary to obtain authorization to engage in active defense techniques easier, speedier, and more transparent. Every process should be tailored as narrowly as possible, and draw from lessons learned from previous cooperative efforts.

One tactic to implement this framework may be to grant licenses to certain cybersecurity companies that would allow them to engage in limited active defense techniques. A federally licensed cybersecurity...
firm could gather intelligence about a threat at the request of a private company, and either turn it over to law enforcement, “name and shame” the perpetrators publicly, or share the intelligence privately with other relevant parties. Doing so could address certain domestic statutory issues, since these firms might be considered “lawfully authorized” to operate, in compliance with the law enforcement and intelligence exceptions to the CFAA. Analogous to private detectives, security firms, or specialized police used by the private sector and even the U.S. government today, firms like Crowdstrike, Mandiant, and FireEye have already proven to be adept at this type of information gathering. As Jeremy and Ariel Rabkin note, the United States routinely relies on reporting conducted by private firms that may be unlawful in the country where it is conducted. The firms would be liable for any mistakes in attribution causing damage to third parties, incentivizing prudence and caution. Relying upon private actors to act in an authorized manner on behalf of law enforcement or other elements of government, however, could well raise issues under the state action doctrine and Fourth Amendment jurisprudence that would need to be addressed.

Another necessary aspect of an operational active defense framework is a consultative group or process that can facilitate decision-making between the federal government and the private sector. This could either be a formally established federal advisory committee (similar to the Critical Infrastructure Partnership Advisory Council or the National Security Telecommunications Advisory Committee) or a more ad hoc set of processes for public-private consultation on active defense, consistent with the Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government (established pursuant to the Cybersecurity Act of 2015), the National Cyber Incident Response Plan and other operational plans and procedures.

It is also vital to continue to strengthen the existing diplomatic processes of building global norms of responsible state behavior in cyberspace. During the past few years the international diplomatic community has made a number of significant advances in building consensus on what laws, rules, and norms should govern in cyberspace. In 2013 a group of experts representing fifteen countries at the United Nations (UN), including countries like the U.S., China, and Russia, agreed in a consensus report (the GGE 2013) that international law and the UN Charter apply in cyberspace. A follow-on report from an expanded group of UN experts in 2015 (GGE 2015) outlined specific norms, confidence-building measures, and procedures for international cooperation and capacity building. In 2013, another group of experts released the Tallinn Manual, the most detailed study of the applicability of international law to cyberspace, with particular attention to the jus ad bellum (right to war) and law of armed conflict.

These are welcomed developments in the international discussion and consideration of active defense, but fall short of answering the ultimate question of which active defense techniques are acceptable and which become prohibited without express authorization. There is scarce international law on the matter. The Council of Europe Convention on Cybercrime (the Budapest Convention) criminalizes computer crimes similarly to the CFAA, but has not been ratified by a few of the most advanced cyber powers, including Russia and China. Generally, international law ap-
plies primarily to states, and therefore has little effect on private sector actors engaging in active defense. Absent an international treaty to clarify the matter, and without a harmonized understanding of which active defense techniques are considered acceptable, those who do engage in active defense may be subject to violations of the law of the country hosting the target servers.

Therefore, it is important for such norms of responsible state behavior to develop in cyberspace. A growing consensus on the responsibility of states to stop malicious cyber activities originating from within their territory has been promoted broadly through acceptance of the GGE 2015. An agreement to prohibit cyber-enabled theft of intellectual property was undertaken by China, the U.S., Russia, and the other members of the G20. These agreements strengthen the case for providing private actors with the leeway to defend themselves when governments fail to meet their commitments.

Diplomats, industry leaders, and other experts should capitalize on this progress to build a global set of norms regulating the use of active defense techniques. These norms will be required to complement existing domestic and international legal regimes that exist to regulate consumer privacy, such as regulations promulgated by the U.S. Federal Trade Commission, and major international data privacy agreements such as the E.U.-U.S. data Privacy Shield agreement.

Beyond the development of international norms, governments must continue to play an active role in protecting domestic entities from cyber threats. While this report primarily focuses on the part that a more proactive private sector can play in denying benefits to malicious actors and bolstering America’s cyber deterrence posture, imposing costs on aggressors in cyberspace tends to require state involvement. Furthermore, even companies with massive cybersecurity budgets, such as large financial institutions, do not have the capacity or interest to square off against a state-sponsored adversary in a way that encourages escalation or sustained cyber conflict. Therefore, the government must begin issuing consistent and clear statements detailing which malicious cyber activities will warrant American responses, and how such responses will progress in severity. Demonstrating the capacity and willingness to act in accordance with such statements are also crucial to cyber deterrence. Such progress would help to address some of the more significant threats in cyberspace, allowing private sector efforts, including the responsible use of active defense, to focus on more manageable threats.
THE ESTABLISHMENT of such a framework for active defense against cyber threats is unlikely to emerge quickly or efficiently; it is unlikely in the near-term that there will be a single event that will realign private and public sector incentives and catalyze the development of such a framework. However, there are a number of specific actions that can be undertaken by government agencies and by key private sector companies to shift the policy and legal context for active defense. This section recommends a set of actions which taken together, will shift the policy environment more closely toward one that integrates active defense measures as useful, risk-based tools to counter cyber threats.

**Actions for the Executive Branch**

1. The Department of Justice should issue public guidance to the private sector with respect to active defense measures that it interprets to be allowable under current law, indicating that DOJ would not pursue criminal or civil action for such measures assuming that they are related to the security of a company’s own information and systems. Such guidance should be updated on a regular basis consistent with ongoing developments in technology.

2. DOJ and the Federal Trade Commission should update their "Antitrust Policy Statement on Cybersecurity Information Sharing" (2014) to state clearly that antitrust laws should not pose a barrier to intra-industry coordination on active defense against cyber threats.

3. The Department of Homeland Security should coordinate the development of operational procedures for public-private sector coordination on active defense measures, utilizing existing mechanisms for cooperation such as the industry-led Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs), and the National Cybersecurity and Communications Integration Center (NCCIC) at DHS.

4. The National Institute for Standards and Technology (NIST) should develop guidelines, best practices, and core capabilities for private sector activity with respect to assessing the risk of and carrying out active defense measures, with 3-5 different levels of technical maturity linked to certification to carry out certain types of measures, or in the case of third-party vendors, to protect other companies. Such guidelines may be distinct for different industry sectors, and this effort at NIST shall be consistent with the work done in 2013-2014 to develop the Cybersecurity Framework.

5. Federal agencies that fund cybersecurity-related research and development, including the Departments of Defense, Homeland Security, the Intelligence Community, and the National Science Foundation, should prioritize R&D on the development of new active defense measures (including capabilities that may improve attribution) and assess efficacy of current active defense measures.
6. The Department of State should engage with foreign partners in developing common standards and procedures for active defense measures. This is particularly relevant given the fact that many of the large companies who are affected by cyber threats operate globally, and thus need to protect information on systems in dozens of countries.

7. The Privacy and Civil Liberties Oversight Board (PCLOB) should carry out a review of current and proposed federal government activities related to active defense activities by the private sector, and release a public report on the results of this review.

8. The White House should develop a policy that provides guidance to federal agencies on when and how they should provide support to the private sector with respect to active defense activities, addressing such factors such as the maturity of private sector entities, the nature of the threat actors (if known), and the economic and security-related importance of the infrastructure or information targeted. This latter factor could perhaps be linked to the list of “critical infrastructure at greatest risk” as identified by DHS pursuant to Section 9 of Executive Order 13636. Types of support that are envisioned include information sharing, coordinated planning, intelligence support, and training.

9. The President should issue a directive that codifies the requirements in items 1-6 above and sets clear deadlines for the adoption of them.

Actions for the U.S. Congress

10. Congress should pass legislation to oversee the implementation of the activities in action items 1-7 above, and reinforce the deadlines in statute. Congress should also mandate that the Government Accountability Office review the implementation of this legislation.

11. Congress should reassess language in the CFAA and the Cybersecurity Act of 2015 that constrains private sector activity on active defense, to ensure that low and medium-risk active defense measures are not directly prohibited in statute.

12. Congress should examine whether and how other tools established in law (e.g. indictments, sanctions, trade remedies) can be utilized in support of protecting the private sector against malicious cyber actors. Executive Order 13694 (“Sanctions Related to Significant Malicious Cyber-Enabled Activities”) from 2015 is a good example of this principle in practice, but there are other tools that can be utilized in support of cyber deterrence and active defense.

Actions for the Private Sector

13. Private sector companies should work together and take the lead in developing industry standards and best practices with respect to active defense measures within their sectors and industries. Such efforts should be undertaken on an international basis, involving a broad set of major companies from all regions of the world.

14. Companies should develop policies at the C-Suite level for whether they want to engage in certain types of active defense measures in response to hypothetical future attacks, instead of simply reacting after they have suffered a data breach or other form of cyber attack. Companies should develop an operational template, based upon a thorough risk
assessment and analysis of industry standards and best practices, that can be integrated into a broader cyber strategy and incident response protocols. These policies must be incorporated within the companies’ broader commitment to and investment in their own traditional cyber defense programs.

15. Industry groups should examine best practices for coordination between Internet service providers, web hosting services, and cloud service providers and their clients on active defense, leveraging the fact that these service providers often have contractual, pre-authorized access to their clients’ networks for routine business purposes. Such service providers may be well positioned to carry out active defense measures against cyber threats to their clients.

Collectively, these fifteen recommendations will move the U.S. government and key private sector stakeholders closer to the adoption of the active defense framework envisioned in the last section.
THE TIME FOR ACTION on the issue of active defense is long overdue, and the private sector will continue to be exposed to theft, exfiltration of data, and other attacks in the absence of a robust deterrent. When private sector companies have a capability to engage in active defense measures, they are building such a deterrent, which will reduce risks to these companies, protect the privacy and integrity of their data, and decrease the risks of economic and societal harm from large-scale cyber attacks. We cannot afford to wait any longer on these issues; instead, public and private sector actors need to work together to clarify the gray zone between doing nothing and hacking back, and then utilize available tools effectively and responsibly. Such efforts will shift risk back to our cyber adversaries, and ultimately serve as a deterrent to further action and the basis for multilateral coordination between and among the public and private sectors, leading to enhanced cooperation and mutual protection against cyber threats.
7

Active Defense Considerations for the Future

THIS REPORT IS A SNAPSHOT of active defense and its broader implications as they exist today. However, it is important to recognize that this field will be constantly evolving—including from the standpoint of technology and law. With respect to technology, key questions for the future include: how active defense will be impacted by the Internet of Things (IOT), cloud computing, increasingly distributed enterprises, and the changing capabilities and intentions of threat actors? Certainly the IOT will expand exponentially the opportunities for adversaries to attack. At the same time, from the defender’s perspective, the task of identifying potential vulnerabilities and acting to mitigate them before and after breach will become more complex and more resource-intensive. The tradeoff is that the IOT will bring increased convenience and functionality for both business and consumers; but it will come at a price.

Cloud computing also cuts two ways. On the one hand, it opens up avenues for a wider range of enterprises to obtain services for cybersecurity and other purposes. On the other hand, the cloud also changes the landscape in which adversaries operate by providing a tempting target, rich in assets for attack. Whereas potential targets may currently be more dispersed, the cloud concentrates them to a greater degree—although the owners and operators of Internet-based cloud technologies and services may be comparatively well-placed to defend the valuable constellations of data and other assets that are effectively entrusted to them. Another trend, in the form of increasingly distributed enterprises, also alters the cybersecurity ecosystem for network defenders and network attackers at once. Here again, the evolution in practice brings with it new challenges for the in-house security practitioner, including “more places where it [data] must be protected.”

As technology continues to change so too will the capabilities—and accompanying intentions—of threat actors. However, the counterforces they face will not remain static either: new elements will enter the fray, and the capacities and roles of existing actors will develop as well. For example, what is the role for state and local governments when it comes to active defense? Just as these authorities have become ever-more involved over time in matters of cybersecurity more generally, one might expect state and local officials to participate (eventually) in the domain of active defense in particular.

Another important question for the future is: how will international norms develop in this area? The answer depends upon individual actors (state and non-state) as well as the totality of their conduct. These practices and the statements made in support of—or in protest to—them will constitute evidence of emerging global parameters of acceptable behavior. Formal international instruments such as global treaties are, admittedly, generally difficult to draft and bring into force given the wide variety of competing viewpoints that must be accommodated and reconciled. Therefore, it may prove constructive in the shorter term to work towards a more informal international understanding of what should be the core body of
principles governing active defense—perhaps in the form of a voluntary code of conduct. In contrast to a multilateral (interstate official) agreement such a tool is by definition non-binding, though it could still reflect the consensus opinion of a range of key participants in active defense worldwide, and thereby serve as a building block for the creation of more embedded international norms in the future.

The Center for Cyber and Homeland Security and the Task Force co-chairs look forward to continuing to work on these and related issues as they continue to engage on these and associated cyber policy matters in the years ahead.
This report is a necessary contribution to the important conversation around the appropriate cybersecurity defensive measures that companies can take to respond to and prevent attacks. The George Washington Center for Cyber and Homeland Security and the members of the Task Force are to be commended for their efforts to further a constructive dialogue and contribute to the scholarship on these issues. If policy makers draw only one lesson from the report, it should be that the “gray zone” between lawful and unlawful defensive measures must shrink. The current level of ambiguity between lawful and unlawful defensive measures poorly serves corporate, privacy, data security, national security, and law enforcement interests. I write separately to express my concern that the report advocates a more aggressive posture than I believe appropriate, and does not give adequate weight to security and privacy risks of some of the techniques it favors.

I appreciate the willingness of the Task Force, and in particular, my colleague Frank Cilluffo, to consider and provide space in the dialogue for these views. I also want to recognize our team at the Center for Democracy & Technology—especially Chris Calabrese, Joseph Lorenzo Hall, Greg Nojeim and Gabe Rottman—for their insights and contribution to these comments.

The report draws a line between “active defense” measures that Congress and the executive branch should make lawful or consider lawful, and “hacking back” which would remain unlawful. I believe that the line between them, consistent with the line drawn in the Computer Fraud and Abuse Act (CFAA) and the Cybersecurity Information Sharing Act, should be the act of gaining unauthorized access to another’s computer or network, as recognized by the US Department of Justice (DOJ) and the US Department of Homeland Security.130 The unauthorized access bar should be raised by amending the CFAA to add a requirement that to be unlawful, the act of gaining unauthorized access must involve circumventing a technical access control. This would ensure that mere “terms of service” violations do not trigger CFAA civil and criminal liability.

Instead, the report invites companies to engage in active defense measures that involve gaining unauthorized access to another’s computer or network, so long as the entity engaging in this activity does not do so with intent to cause harm. For example the report discusses the use of “dye packs” and “white hat ransomware”—both of which involve gaining unauthorized access to another’s computer or network and placing malware on those systems—as more aggressive active defense measures that might become lawful based on considerations like whether they were conducted in conjunction with the government and the intent of the actor.

I believe these types of measures should remain unlawful. Intent can be difficult to measure, particularly when on the receiving end of an effort to gain access. Because attacks are often launched through the computers of innocent people, and because attack attribution is at best an inexact science, the risk of harm in these methods that gain unauthorized access can fall upon other victims of the attack and on innocent bystanders.

The risks of collateral damage to innocent internet users, to data security, and to national security that can result from overly aggressive defensive efforts needs to be better accounted for. There are examples of defensive measures that had unintended consequences, and lessons can be learned from those cases. For example, Microsoft’s efforts to take down two botnets associated with the dynamic DNS service offered by no-ip.com had the effect of temporarily denying DNS service to 5 million people, effectively causing 99.8%
collateral damage to users of no-ip’s service, and causing those domains to be completely inaccessible to their users and customers for two days. Instead, as an example of active defense measures companies could take, the report mentions Google’s response to operation Aurora. Based on existing evidence it seems likely that response involved gaining unauthorized access to computers in Taiwan that were believed to be under the control of entities in China and inspecting data on those computers—serious conduct with national security and foreign law implications that must be more thoroughly addressed.

Some of the more aggressive defensive measures the report mentions, if permitted at all, should be engaged in by law enforcement or under the direction of a law enforcement agency. “Coordination” with law enforcement may not be enough. Moreover, the report only briefly dwells on the risks of government hacking or of the myriad controls that should be imposed to prevent or ameliorate harm. Just a few of the unanswered questions include: What kind of court order would be required to permit such government conduct? How would it constrain that conduct, and when? How and when would the government give notice to the targets of these defensive measures, when those targets will invariably perceive this conduct as attacks? Further, since, as the report does note, government notice in these contexts could be spoofed and, if the conduct becomes normalized, could become an additional vector of attack, what steps will be taken to authenticate the sender or prevent such abuse?

There is also an ongoing and active debate regarding the scope of law enforcement hacking in criminal investigations under a revised Rule 41—the authority DOJ would likely use in some of the contemplated active defense scenarios. Those actions are certain to result in overbroad searches and possibly damage to the computers of many innocent people who have already been the victims of hacking.

When it comes to risky defensive conduct that may cross the line and be unlawful, the report makes two observations that give me pause. First, that some cybersecurity firms might be given a license to operate as agents of the federal government and engage in conduct that would be unlawful for other private parties. Second, that the Department of Justice forbear prosecution of companies that engage in unlawful active defense measures. The first may be unwise and would be difficult to implement. The report does not address any limits and controls under which the licensed firm would operate, or the qualifications that would be required of licensees, or how they themselves and consequences of their actions will be overseen. The second—possible DOJ forbearance—would grow rather than shrink “the gray zone” of permissible conduct. And, in some cases, forbearance may be appropriate, but in instances where an entity actually circumvents a technical access control, prosecution may indeed be warranted. A call for DOJ forbearance must better account for the computer crimes laws of other countries that would be implicated in many active defense scenarios where the affected system is located in another country.

I recognize the Task Force’s efforts to accommodate many of my concerns. Ultimately though, I would have preferred a more moderate approach. As this discussion progresses, I urge greater outreach to privacy and civil liberties groups beyond the experts whose views were sought. Hopefully the report will put active defense higher on the agenda of more stakeholders. We look forward to continuing to participate in this discourse, and to ensuring that active defense measures include protections for civil liberties while not undermining the integrity of the architecture of computer and networked systems.
Appendix II: Legal Analysis
Courtesy of Covington & Burling, LLP

I. Most Relevant U.S. Statutes
   A. Computer Fraud and Abuse Act (18 U.S.C. § 1030 et seq)
      1. Main Restrictions—it is illegal for anyone who:
         a) Accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer;
         b) Knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
         c) Intentionally access a protected computer without authorization, and as a result of such conduct, recklessly cause damage; or
         d) Intentionally access a protected computer without authorization, and as a result of such conduct, cause damage and loss.
   2. Practical Effect/Examples
      a) Most of the aggressive cyber defense measures (and perhaps some of the more intermediate) likely would violate this law.
         (1) For example, any measure that would recover, erase, or alter stolen data or send malware to disrupt an attack likely would require unauthorized access to a computer and would obtain data from or cause damage to that computer.
         (2) Less clear are intermediate measures such as observation and monitoring outside a company’s network or beaconing. While these may require access to a computer, they may not involve obtaining information or causing damage.
      b) The statute has been interpreted very broadly (e.g., a protected computer is any computer connected to the internet, United States v. Trotter, 478 F.3d 918 (8th Cir. 2007)) but there is also some ambiguity about the meaning of “authorization” and therefore the meaning of “without authorization” or “exceeds authorized access.” LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1132-33 (9th Cir. 2009), United States v. Valle, No. 14-2710 et al. (2d. Cir. 2015).
         (1) Nevertheless, active cyber defense measures that involve accessing an attacker’s computer or network to obtain or destroy data likely would qualify as “without authorization” or “exceeds authorized access.”
   3. Potential Amendments?
      1. Main Restrictions—It is illegal for anyone to:
a) Intentionally or purposefully intercept (or endeavor to intercept), disclose or use the contents of any wire, oral, or electronic communication;

b) Intentionally or purposefully use (or endeavor to use) a device to intercept oral communication.

c) A “device” is any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than a telephone or telegraphy equipment given to the user by a provider of wire or electronic communication and used in the ordinary course of business, or a hearing aid or similar device.

2. Practical Effect/Examples

a) While most of the analysis centers on the CFAA, some cyber defense tactics may also violate the Wiretap Act. For example, practices such as sinkholing may violate the Wiretap Act to the extent that intercepting malicious traffic would be considered an intercept of an electronic communication. See Sean L. Harrington, Cyber Security Active Defense: Playing with Fire or Sound Risk Management?, 20 Rich. J.L. & Tech. 17 (2014).

3. Potential Amendments?

a) The Wiretap Act has an exception that allows law enforcement officials to monitor activity of hackers when certain limited criteria are met (including when the owner or operator of the network authorizes the interception and when there is a lawful investigation). See 18 U.S.C. § 2511(2)(i)(I)-(IV); see also Harrington, 20 Rich. J.L. & Tech. 12. There could be some potential to expand on this exception or add to the criteria circumstances involving cyber defense or stolen data.


1. Main Restrictions—prohibits anyone from:

a) Installing a pen register or trap and trace device without obtaining a court order

b) A “pen register” is “a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication…” 18 U.S.C. § 3127(3).

c) A “trap and trace device” is a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication…” 18 U.S.C. § 3127(4).

2. Practical Effect/Examples

a) Prohibition on “trap and trace” devices may apply to intermediate cyber defense measures such as honeypots or sinkholes that operate to capture incoming data and identify the source of intrusion or attack.

b) Emphasis here is really demonstrating the role that the government would play in cyber defense measures, i.e., the need to obtain a court order to install a pen register or trap and trace device.

II. Common Law Theories

A. Trespass to Chattels

1. Elements

a) Trespass to chattels is “intentionally...dispossessing another of the chattel, or using or intermeddling with a chattel in the possession of another.” Restatement (Second) of Torts § 217.
b) Accordingly, one needs to prove (1) intent, (2) interference with the chattel, and (3) actual harm. See T. Luis de Guzman, *Unleashing a Cure for the Botnet Zombie Plague: Cybertorts, Counterstrikes, and Privileges*, 59 Catholic U L Rev. 527 (2010).

2. Examples

   a) Courts have found that spam email interfered with an email server enough to amount to an action for trespass to chattels. *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1021 (S.D. Ohio 1997); see also Huang, 82 Geo. Wash. L. Rev. at 1242.

   b) A trespass to chattels action could also arise due to unwanted computer access. *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393 (2d Cir. 2004) (finding that continued, automated behavior consumed capacity of Register.com’s computer system and impaired their quality and value); see also Huang, 82 Geo. Wash. L. Rev. at 1242, 43.

   c) Ultimately, trespass to chattels may require repeated access that causes some harm to computer performance. Huang, 82 Geo. Wash. L. Rev. at 1242, 43.


3. Practical Effect

   a) Under certain circumstances, one can interfere with another’s chattels to defend his or her own chattels. See de Guzman, 59 Catholic U L Rev. at 542. The Restatement (Second) of Torts recognizes this privilege: “one is privileged to commit an act which would otherwise be a trespass to a chattel or a conversion if the act is, or is reasonably believed to be, necessary to protect the actor’s land or chattels or his possession of them, and the harm inflicted is not unreasonable as compared with the harm threatened.” Restatement (Second) of Torts § 260(1).

   b) A company might be able to use this concept to shield itself from liability for cyber defense measures. However, such measures could include other actions that could be found tortious, or even in violation of the CFAA. See de Guzman, 59 Catholic U L Rev. at 542.

B. Negligence

   1. Elements

      a) Duty of care, breach, causation, and damages.

   2. Practical Effect/Examples

      a) Commentators have proposed holding intermediary parties responsible for failure to secure their systems. Kesan & Hayes, 25 Harv. J.L. & Tech. at 498; see de Guzman, 59 Catholic U L Rev. at 548.

      b) For example, a “zombie” computer owner, ISP, or software manufacturer could all be held liable for failing to safeguard their own devices which in turn were used to launch an attack on the ultimate victim. See Kesan & Hayes, 25 Harv. J.L. & Tech. at 498.

   3. Limitations

      a) It could be challenging to establish a duty of care and show causation in many cases. See Kesan & Hayes, 25 Harv. J.L. & Tech. at 499. ISPs and other service providers could avoid liability through contractual terms. See id. at 499-500.

      b) No recourse for companies to retrieve stolen data or to fix damages to network or computer caused by attack.
III. International Law

A. No Overarching International Law for Private Actors

1. There is no overarching international law that specifically addresses active cyber defense by private actors. See Paul Rosenzweig, International Law and Private Actor Active Cyber Defensive Measures, 50 Stan. J. Int’l L. 103 (2014).

B. International Law Focuses on Nation-States

1. Most of the applicable international law focuses on the actions of nation-states
2. This includes the UN Charter and other laws governing nations’ right to self-defense. See Michael N. Schmitt, In Defense of Due Diligence in Cyberspace, 125 Yale L. J. (2015); see also Tallinn Manual.

C. Countries’ Own Domestic Laws

1. Some countries have enacted laws that address active cyber defense. For example:
   a) Germany has made hacking back illegal (although anecdotal evidence suggests that private entities in Germany engage in this tactic anyway). Rosenzweig, 50 Stan. J. Int’l L. 103
   b) Netherlands proposed law allowing enforcement officials to hack back internationally. Id.
   c) Israeli Defense Forces reserve right to use offensive cyber operations but law is silent on ability of private actors to do the same. Id.
2. Private companies may be liable for active cyber defense actions that are taken against a computer or a network in a country with a domestic law prohibiting such actions. Id. (hypothesizing that “when a private sector hack back has collateral effects in an allied country . . . we can imagine that U.S. legal authorities would generally honor an appropriately couched extradition request from the affected nation.”).

D. Analogous International Laws

1. Certain laws such as the Budapest Convention, Rome Statute, International Criminal Tribunal provide opportunities to analyze whether the self-defense provisions under these laws could be extrapolated to cyber activities. Id. Most allow some sort of self-defense, even if it is limited.
2. Law of piracy would allow for self-defense but not active pursuit (which would be left only to states and only within their own territorial waters). Id.
3. Letters of marque would suggest a state’s explicit acceptance and/or direction of action to retaliate against malicious cyber activity. Id.
IN A GLOBALIZED WORLD, corporations, threat actors, and computer networks are unrestricted by political boundaries. While this report’s focus is on private sector active defense in the context of U.S. policy and law, it is worthwhile to briefly summarize the active defense “climates” in four foreign countries that are relevant in the realm of cybersecurity. As is seen in the following examples, every country creates unique architectures to deal with cyber threats, enacts different computer trespass laws, and socializes different cybersecurity norms. These factors all influence the level to which countries consider implementing policies conducive to private sector active defense. The following section details the active defense climates of the United Kingdom, France, Estonia, and Israel.

The United Kingdom

The 2010 UK National Security Strategy characterized cyber-attacks as a “Tier One” (“highest priority”) threat and, since then, the government has been working with the private sector to share threat-related information. Against this background, the UK security and intelligence agency, Government Communications Headquarters (GCHQ), has been helping to build awareness of—and resilience to—the cyber threat in the critical financial services sector, by supporting efforts to test, train, and exercise capabilities in this area. The country’s new National Cyber Security Centre (NCSC) is intended to reinforce and expand the effort to inform and support against cyber threats to the business community and beyond. The country’s new National Cyber Security Centre (NCSC) is intended to reinforce and expand the effort to inform and support against cyber threats to the business community and beyond. The country’s new National Cyber Security Centre (NCSC) is intended to reinforce and expand the effort to inform and support against cyber threats to the business community and beyond. The country’s new National Cyber Security Centre (NCSC) is intended to reinforce and expand the effort to inform and support against cyber threats to the business community and beyond. Hackers have hit Britain’s biggest banks—from HSBC to Standard Chartered to Barclays—repeatedly in recent years. Analysts have emphasized the major banks’ vulnerabilities, introduced by “their complex and ageing web of overlapping computer systems.”

France

The larger context of a company’s position in the marketplace shapes the need for—and manner of implementation of—private sector active defense against cyber threats. In the case of France, government ownership (even if partial) persists in diverse domains from banking to energy to telecommunications. This stands in contrast to the United States and the United Kingdom, where privatization levels are much more extensive. Against the background of this greater blurring of the line between the state and enterprise, France has engaged actively in industrial espionage (despite protestations to the contrary) to the benefit of French economic interests. At the same time, French companies have been targeted. Yet, according to the former head of DCRI (the predecessor to the French internal intelligence agency DGSI):
“Companies rarely admit security breaches or seek the help of the state.”

Under current French law, however, operators of “essential services” are required to report cyber breaches; and the European Union framework now obliges the same. In 2015, France also introduced legislation that explicitly empowers the country’s intelligence entities to conduct surveillance for specified areas and purposes—including “essential industrial and scientific interests.” A new dedicated entity for strategic intelligence and economic security stood up earlier this year. In addition, legislation intended to frustrate threat actors who use encryption continues to advance domestically; and at the international level, France is working in parallel to spur a global effort to achieve similar effect. Increasingly, therefore, French officials are focusing on the points of intersection between economic security and national security.

**Estonia**

In order to protect its rapidly developing e-govern ment infrastructure, Estonia began to promote cybersecurity through national policy in the early 2000’s. It adopted its first national cybersecurity strategy in 2008 after the well-known DDoS attacks of 2007. Following several years of active institutional development, including the establishment of the NATO Cyber Defence Center in Tallinn, the incorporation of the Estonian Information Systems Authority, and the creation of a national cyber security council, Estonia became one of a few countries to adopt a second national strategy in 2014.

Despite these developments, Estonia has no overarching national legal framework that governs cybersecurity and cyber defense. This is not to say that Estonian law has nothing to say about cyber. The Penal Code defines certain computer crimes, including unauthorized access to computer systems, and the Emergency Act governs organizational and governmental cybersecurity. Estonia is also a signatory to the Council of Europe’s Convention on Cybercrime and is subject to EU directives, such as the recent directive on security of network and information systems.

The topic of active defense is rarely an explicit part of Estonian public discourse on cybersecurity, especially within the private sector. However, public and private entities engage in certain activities that fall under its remit. Among other initiatives, Estonian intelligence agencies, the national CERT, and the Information System Authority share information among themselves, with the private sector, and with international counterparts to facilitate rapid response to emerging cyber threats and improve critical infrastructure cybersecurity. Government agencies also conduct penetration tests of critical infrastructure companies hold regular public-private cyber defense exercises, and collaborate with international partners in takedown operations.

Ultimately, there is no discernible momentum in Estonia for policy changes in the field of private sector active defense, nor are there particularly loud calls for such changes from company executives. This may be due to the lack of an overarching legal framework for cybersecurity in Estonia—the development of which is a priority under the most recent national cybersecurity strategy—or by the fact that private sector leaders do not publicly discuss active defense measures. However, it is more likely that Estonia’s small size and intensive public-private cooperation provide its private sector entities with greater access to governmental attention and resources, an advantage that may be unavailable to private entities in larger European or North American countries. Barring major political or external pressure, this arrangement is unlikely to change in the near future.

**Israel**

Out of necessity, Israel has developed advanced cybersecurity capabilities that include Unit 8200 of the Israel Defense Forces (IDF). The country’s private sector too, has had to develop operational strategies to counter sustained cyber-attacks and industrial espionage. Notably, Israel’s cybersecurity industry is a major player in the global market, and continues to attract capital and investors. The sector also benefits from the skills and experience that former mem-
bers of IDF Unit 8200 have brought to Israel’s vibrant “tech startup” community.158

The tenor of the national dialogue in Israel, spanning both the public and private sectors, is supportive of a forward-leaning and robust posture on matters of cybersecurity.159 The country’s legal framework in this area is comparatively relaxed relative to that of the United States.160 (Indeed, anecdotal evidence suggests that U.S. firms wishing to take a more active posture on cybersecurity have contracted with Israeli firms in order to circumvent U.S. strictures in this area).161

From a government standpoint, Israel’s National Cyber Bureau (NCB) coordinates the country’s cybersecurity initiatives while supporting the private sector. As part of the Prime Minister’s Office, the NCB funds research and development, and works to improve public-private sector collaboration in accordance with the government’s “Digital Israel” initiative.162 Furthermore, since its establishment in 2002, Israel’s National Information Security Authority has directly advised owners of critical infrastructure situated in the private sector, on cybersecurity issues.163
### Appendix IV: Glossary of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition and Source</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advanced Persistent Threat (APT)</strong></td>
<td>“An adversary that possesses sophisticated levels of expertise and significant resources which allow it to achieve its objectives using multiple attack vectors. (NIST SP 800-61).”  &lt;br&gt;  “An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders’ efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.” SP 800-39.  &lt;br&gt;  <a href="http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf">http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf</a></td>
</tr>
<tr>
<td>Term</td>
<td>Definition and Source</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Blacklisting</td>
<td>“The process of the system invalidating a user ID based on the user’s inappropriate actions. A blacklisted ID cannot be used to log on to the system, even with the correct authenticator. Blacklisting and lifting of a blacklisting are both security-relevant events. Blacklisting also applies to blocks placed against IP addresses to prevent inappropriate or unauthorized use of Internet resources.” CNSSI-4009. “A list of email senders who have previously sent spam to a user.” SP 800-114. “A list of discrete entities, such as hosts or applications, that have been previously determined to be associated with malicious activity.” SP 800-94. <a href="http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf">http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf</a></td>
</tr>
<tr>
<td>Botnet</td>
<td>“A term derived from ‘robot network,’ is a large automated and distributed network of previously compromised computers that can be simultaneously controlled to launch large-scale attacks such as a denial-of-service attack on selected victims.” <a href="http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf">http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf</a></td>
</tr>
<tr>
<td>Botnet takedown</td>
<td>“Actions taken to identify and disrupt a botnet’s command and control infrastructure.” <a href="http://timreview.ca/article/862">http://timreview.ca/article/862</a></td>
</tr>
<tr>
<td>Computer Network Attack</td>
<td>“Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.” CNSSI-4009. <a href="http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf">http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf</a></td>
</tr>
<tr>
<td>Computer Network Defense</td>
<td>“Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities.” CNSSI-4009. <a href="http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf">http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf</a></td>
</tr>
<tr>
<td>Term</td>
<td>Definition and Source</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Computer Network Exploitation</td>
<td>“Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary information systems or networks.” CNSSI-4009.</td>
</tr>
<tr>
<td>Critical infrastructure</td>
<td>“System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. [Critical Infrastructures Protection Act of 2001, 42 U.S.C. 5195c(e)]” CNSSI-4009.</td>
</tr>
<tr>
<td>Cyber attack</td>
<td>“An attack that alters a system or data.” CNSSI-4009. “An attack on the authentication protocol where the Attacker transmits data to the Claimant, Credential Service Provider, Verifier, or Relying Party. Examples of active attacks include man-in-the-middle, impersonation, and session hijacking.” SP 800-63. “An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.” SP 800-32. “Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.” CNSSI-4009.</td>
</tr>
</tbody>
</table>
| Cyber deterrence by denial   | “Reducing the incentive of potential adversaries to use cyber capabilities against the United States by persuading them that the United States can deny their objectives . . . The President has at his disposal a number of tools to carry out deterrence by denial. These include a range of policies, regulations, and voluntary standards aimed at increasing the security and resiliency of U.S. government and private sector computer systems. They also include incident response capabilities and certain law enforcement authorities, such as those used by the Department of Justice to take down criminal botnets. They include cyber threat information sharing mechanisms, as well as public-private partnerships.”

“efforts . . . to persuade adversaries that the United States can thwart malicious cyber activity, thereby reducing the incentive to conduct such activities. To make these deterrence efforts credible, we must deploy strong defenses and architect resilient systems that recover quickly from attacks or other disruptions.”

Continued on the next page
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition and Source</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cyber deterrence by denial (continued)</strong></td>
<td>“Pursuing defense, resiliency, and reconstitution initiatives to provide critical networks with a greater capability to prevent or minimize the impact of cyber attacks or other malicious activity, and reconstitute rapidly if attacks succeed. Building strong partnerships with the private sector to promote cybersecurity best practices; assist in building public confidence in cybersecurity measures; and lend credibility to national efforts to increase network resiliency.”&lt;br&gt;Department of State International Cyberspace Policy Strategy, Public Law 114-113, Division N, Title IV, §402 (March 2016), <a href="https://www.state.gov/documents/organization/255732.pdf">https://www.state.gov/documents/organization/255732.pdf</a></td>
</tr>
<tr>
<td><strong>Cyber espionage</strong></td>
<td>“Activities conducted in the name of security, business, politics, or technology to find information that ought to remain secret. It is not inherently military.”&lt;br&gt;<a href="http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf">http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf</a></td>
</tr>
<tr>
<td><strong>Cyber Infrastructure</strong></td>
<td>“Includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of other media types. Communications include sharing and distribution of information. For example: computer systems; control systems (e.g., supervisory control and data acquisition-SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure.” NISTIR 7628.&lt;br&gt;<a href="http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf">http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf</a></td>
</tr>
<tr>
<td><strong>Cyberspace</strong></td>
<td>“A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.” CNSSI-4009.&lt;br&gt;<a href="http://www.globaltimes.cn/content/1010409.shtml">http://www.globaltimes.cn/content/1010409.shtml</a></td>
</tr>
</tbody>
</table>
Term | Definition and Source
--- | ---
**Dark Net** | “A collection of websites that are publicly visible but hide the Internet Protocol addresses of the servers that run these sites.” “The Dark Web relies on darknets or networks that are made between trusted peers. Examples of Dark Web systems include TOR, Freenet, or the Invisible Internet Project (I2P).” Vincenzo Ciancaglini et al., Below the Surface: Exploring the Deep Web, TrendLabs Research Paper, TrendMicro (2016) [https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf](https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf).

**Deep Web** | “Any Internet content that, for various reasons, can’t be or isn’t indexed by search engines like Google. This definition thus includes dynamic web pages, blocked sites (like those that ask you to answer a CAPTCHA to access), unlinked sites, private sites (like those that require login credentials), non-HTML/-contextual/-scripted content), and limited-access networks.” Vincenzo Ciancaglini et al., Below the Surface: Exploring the Deep Web, TrendLabs Research Paper, TrendMicro (2016) [https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf](https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf).

**Denial of Service (DoS)** | “The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.). CNSSI-4009. [http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf](http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf)

**Distributed Denial of Service Attack (DDoS)** | “A Denial of Service technique that uses numerous hosts to perform the attack.” CNSSI-4009. [http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf](http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf)

**Dye pack** | See beaconing. In the cybersecurity context, the terms beacon and dye pack are often used interchangeably. However, with the term's physical namesake being the dye packs used to identify bank robbers, the cybersecurity tool sometimes takes on a more aggressive connotation. Where, in bank robberies, dye packs explode and contaminate the stolen money and their environment with a recognizable dye, cyber dye packs are often thought to not only be able to collect information on a hacker’s computer (similar to a beacon) but also to be able to have a destructive impact on their surrounding environment.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition and Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>“A system or combination of systems that enforces a boundary between two or more networks, typically forming a barrier between a secure and an open environment such as the Internet.” “A gateway that limits access between networks in accordance with local security policy.” SP 800-32. “A hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy.” CNS- SI-4009. “A device or program that controls the flow of network traffic between networks or hosts that employ differing security postures.” SP 800-41.</td>
</tr>
<tr>
<td>Honeypot</td>
<td>“A specially configured server, also known as a decoy server, designed to attract and monitor intruders in a manner such that their actions do not affect production systems.” “A system (e.g., a Web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders and has no authorized users other than its administrators. CNSSI-4009.</td>
</tr>
<tr>
<td>Information Sharing and Analysis Center</td>
<td>“ISACs help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards. ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency . . . ISACs are trusted entities established by critical infrastructure owners and operators to foster information sharing and best practices about physical and cyber threats and mitigation. About ISACs, National Council of ISACs (Accessed Oct. 14, 2016), <a href="http://www.isaccouncil.org">http://www.isaccouncil.org</a>.</td>
</tr>
<tr>
<td>Patching</td>
<td>“Fixes to software programming errors and vulnerabilities.” The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.” CNSSI-4009.</td>
</tr>
<tr>
<td>Quarantine</td>
<td>“Store files containing malware in isolation for future disinfection or examination.” SP 800-69.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition and Source</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Ransomware                | “Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system’s screen or by locking the users’ files unless a ransom is paid. More modern ransomware families, collectively called crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key.”  
| Remote Access Tools (RATs)| Tools that allow either authorized or unauthorized remote access, i.e., “access to an organizational information system by a user (or an information system acting on behalf of a user) communicating through an external network (e.g., the Internet).” SP 800-53. “Access by users (or information systems) communicating external to an information system security perimeter.” SP 800-17. “The ability for an organization’s users to access its nonpublic computing resources from external locations other than the organization’s facilities.” SP 800-46. “Access to an organization’s nonpublic information system by an authorized user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).” CNSSI-4009.  
| Sinkholing                | “A mechanism aimed at protecting users by intercepting DNS requests attempting to connect to known malicious or unwanted domains and returning a false, or rather controlled IP address. The controlled IP address points to a sinkhole server defined by the DNS sinkhole administrator. This technique can be used to prevent hosts from connecting to or communicating with known malicious destinations such as a botnet C&C server.”  
| Social engineering       | “An attack based on deceiving users or administrators at the target site into revealing confidential or sensitive information.”  
| Spyware                   | “Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.” SP 800-53, CNSSI-4009.  
http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf |
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition and Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tarpits</td>
<td>“Allowing a tarpitted port to accept any incoming TCP connection. When data transfer begins to occur, the TCP window size is set to zero, so no data can be transferred within the session. The connection is then held open, and any requests by the remote side to close the session are ignored. This means that the attacker must wait for the connection to timeout in order to disconnect.” <a href="http://csrc.nist.gov/cyberframework/framework_comments/20131213_charles_alsup_insa_part3.pdf">http://csrc.nist.gov/cyberframework/framework_comments/20131213_charles_alsup_insa_part3.pdf</a></td>
</tr>
<tr>
<td>White hat</td>
<td>“White hats are security researchers or hackers who, when they discover a vulnerability in software, notify the vendor so that the hole can be patched.” Kim Zetter, Hacker Lexicon: What are White Hat, Gray Hat, and Black Hat Hackers?, Wired (April 13, 2016), <a href="http://docs.house.gov/meetings/IF/IF17/20150324/103226/HHRG-114-IF17-Wstate-SchoolerR-20150324.pdf">http://docs.house.gov/meetings/IF/IF17/20150324/103226/HHRG-114-IF17-Wstate-SchoolerR-20150324.pdf</a>.</td>
</tr>
<tr>
<td>Whitelisting</td>
<td>“A list of discrete entities, such as hosts or applications that are known to be benign and are approved for use within an organization and/or information system.” SP 800-128. <a href="http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf">http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf</a></td>
</tr>
<tr>
<td>Zero-day exploits</td>
<td>“A vulnerability that is exploited before the software creator/vendor is even aware of its existence.” <a href="http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf">http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf</a></td>
</tr>
</tbody>
</table>
Notes


4. Justin McCarthy, “Americans Cite Cyberterrorism Among Top Three Threats to US,” Gallup (2016), http://www.gallup.com/poll/189161/americans-cite-cyberterrorism-among-top-three-threats.aspx. The percentage of Americans responding that Cyberterrorism was a critical threat (73%) was the third highest of all threats included in the poll and received the most bipartisan agreement.


29. Press Release, Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence

31. While law enforcement organizations are also confronted with the challenges of limited resources when combating traditional crimes, they benefit from the ability to periodically and visibly "flex" their enforcement muscles in ways that remind threat actors that their actions will not go unnoticed or unchecked. Such visible deterrence can play a significant role in affecting the risk calculations of malicious actors. However, in the digital world, those who combat cybercrime have yet to develop or implement this type of enforcement model. When private actors report cyber incidents, they may or may not be investigated depending on enforcement priorities. Where investigations do take place, they often are completed in a less visible manner, or worse, lead to penalties on the victims.


35. Ibid.


39. Ibid.


43. Ibid.


45. Ibid.


50. Ibid, 4.


52. Ibid.


54. It is important to note that while hacking back is offensive in nature, military and intelligence officers tend to place it in a category of action that is distinct from the sophisticated and tailored approaches that they consider "cyber offense." While the intelligence collection potentials of hacking back may appear attractive to private companies, there are other less risky methods to gather such information that should always be prioritized.


56. Ibid.

57. Impact is measuring the effectiveness of such techniques at deterring cyber threats, and risk is the level of exposure a defender assumes to potential adverse effects such as escalation, unintended consequences, misattribution, and civil or criminal liability.


59. Dye packs are an inherently riskier measure than beacons from a legal standpoint, given that they install malware on an attacker’s system after data exfiltration.


66. DOJ Press Release - Partners involved in the Dridex/Bugat takedown include the FBI, DHS' US-CERT, the UK National Crime Agency, Europol's EC3, Germany's Bundeskriminalamt, Dell SecureWorks, Trend Micro, Fox-IT, S21sec, Abuse.ch, the Shadowserver Foundation, Spamhaus, and the Moldovan General Inspectorate of Police Centre for Combating Cybercrime, the Prosecutor General Office Cyber Crimes Unit, and the Ministry of Interior Forensics Unit.


arrested-and-malware-disabled.


78. See infra Appendix II: Legal Analysis at 44.


80. Ibid.


87. Article 2—Illegal Access. Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offenses under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system. Convention on Cybercrime, Council of Europe, November 23, 2011, T.S. No. 185, [http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=185](http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=185).
88. See infra Appendix II: Legal Analysis at 44.
94. Ibid.
104. Ibid.
107. Ibid.
109. Ibid, 4. “[…]such a typology then helps us identify the appropriate legal régimes that would apply in various domains. We can ask a sensible question like ‘what should be the legal limits of a private sector actors [sic] off-network attribution efforts that have no appreciable effect?’ and mean something that actually says ‘is this beaconing technique legal?’” (emphasis original).


112. Companies conducting "lawfully authorized investigative, protective, or intelligence activit[ies]" are excluded from the CFAA's criminal provisions under Computer Fraud and Abuse Act, U.S. Code 18 (2012), §1030(f).

113. Jeffery Meisner, "Microsoft Works with Financial Services Industry Leaders, Law Enforcement and Others to Disrupt Massive Financial Cybercrime Ring," The Official Microsoft Blog, June 5, 2013, https://blogs.technet.microsoft.com/microsoft_blog/2013/06/05/microsoft-works-with-financial-services-industry-leaders-law-enforcement-and-others-to-disrupt-massive-financial-cybercrime-ring (others involved included the Financial Services-Information Sharing and Analysis Center, the American Bankers Association, and foreign Computer Emergency Response Teams). Though the Citadel takedown made a substantial impact on the botnet's operation, it is extremely difficult to totally eliminate a botnet since it can so easily be reconstructed and redirected. Law enforcement continues to work to prosecute the operators of the botnets in order to address the problem at its source instead of just treating the symptoms. See ibid.


117. William Roth, “Cyber Attacks Against the U.S.: Deputizing the Private Sector to Assist,” (2016). Drawing an analogy between licensed cybersecurity firms authorized to engage in limited intelligence gathering techniques on external networks and U.S. State licensure of railroad police of limited powers “in situations where government is incapable” of keeping the peace.


119. Ibid, 10.

120. Ibid, 11.

121. For an overview of various legal regimes applicable to Active Defense techniques, see Appendix II: Legal Analysis at 44.


129. "Distributed environments face a variety of unique challenges that make security administrators' tasks even harder. Not only do they often have access rules that vary by business unit, but their traditional firewall rules are frequently complex and
unmanageable as well. In addition, distributed environments usually have federated, if not chaotic, endpoint governance. Data is further exposed because more copies of data create more places where it needs to be protected.” John Pescatore, “Conquering Network Security Challenges in Distributed Enterprises,” SANS Institute, InfoSec Reading Room, June 2015, https://www.sans.org/reading-room/whitepapers/analyst/conquering-network-security-challenges-distributed-enterprises-36007.


140. Ibid.


150. The Center for Cyber and Homeland Security would like to thank Patrik Maldre and Sander Retel of Retel Partners for sharing their insights into the active defense climate of Estonia.


159. Ibid.

160. Lewis, “Advanced Experiences.”


163. Lewis, “Advanced Experiences.”


Denning, Dorothy. “Rethinking the Cyber Domain and Deterrence.” *Joint Force Quarterly 77.* 2nd Quarter. 2015.


About the George Washington University Center for Cyber & Homeland Security

The Center for Cyber and Homeland Security (CCHS) at the George Washington University is a non-partisan “think and do” tank whose mission is to carry out policy-relevant research and analysis on homeland security, counterterrorism, and cybersecurity issues. By convening domestic and international policymakers and practitioners at all levels of government, the private and non-profit sectors, and academia, CCHS develops innovative strategies to address and confront current and future threats.

CCHS was established in early 2015 and integrates the activities and personnel of the Homeland Security Policy Institute (HSPI) and the GW Cybersecurity Initiative.
Into the Gray Zone...

This report—the result of a research initiative featuring the perspectives and expertise of the Center for Cyber and Homeland Security’s Active Defense Task Force, as led by the Task Force co-chairs—presents a practical framework for industry and government action that will enhance the private sector’s ability to defend its most valuable data and assets in the context of modern cybersecurity imperatives.
May 23, 2017

Facebook’s Community Standards: How and Where We Draw the Line

By Monika Bickert, Head of Global Policy Management

Last month, people shared several horrific videos on Facebook of Syrian children in the aftermath of a chemical weapons attack. The videos, which also appeared elsewhere on the internet, showed the children shaking, struggling to breathe and eventually dying.

The images were deeply shocking – so much so that we placed a warning screen in front of them. But the images also prompted international outrage and renewed attention on the plight of Syrians.

Reviewing online material on a global scale is challenging and essential. As the person in charge of doing this work for Facebook, I want to explain how and where we draw the line.

On an average day, more than a billion people use Facebook. They share posts in dozens of languages: everything from photos to live videos. A very small percentage of those will be reported to us for investigation. The range of issues is broad – from bullying and hate speech to terrorism – and complex. Designing policies that both keep people safe and enable them to share freely means understanding emerging social issues and
the way they manifest themselves online, and being able to respond quickly to millions of reports a week from people all over the world.

For our reviewers, there is another hurdle: understanding context. It’s hard to judge the intent behind one post, or the risk implied in another. Someone posts a graphic video of a terrorist attack. Will it inspire people to emulate the violence, or speak out against it? Someone posts a joke about suicide. Are they just being themselves, or is it a cry for help?

In the UK, being critical of the monarchy might be acceptable. In some parts of the world it will get you a jail sentence. Laws can provide guidance, but often what’s acceptable is more about norms and expectations. New ways to tell stories and share images can bring these tensions to the surface faster than ever.

We aim to keep our site safe. We don’t always share the details of our policies, because we don’t want to encourage people to find workarounds – but we do publish our Community Standards, which set out what is and isn’t allowed on Facebook, and why.

Our standards change over time. We are in constant dialogue with experts and local organizations, on everything from child safety to terrorism to human rights. Sometimes this means our policies can seem counterintuitive. As the Guardian reported, experts in self-harm advised us that it can be better to leave live videos of self-harm running so that people can be alerted to help, but to take them down afterwards to prevent copycats. When a girl in Georgia, USA, attempted suicide on Facebook Live two weeks ago, her friends were able to notify police, who managed to reach her in time.

We try hard to stay objective. The cases we review aren’t the easy ones: they are often in a grey area where people disagree. Art and pornography aren’t always easily distinguished, but we’ve found that digitally generated images of nudity are more likely to be pornographic than handmade ones, so our policy
There’s a big difference between general expressions of anger and specific calls for a named individual to be harmed, so we allow the former but don’t permit the latter.

These tensions – between raising awareness of violence and promoting it, between freedom of expression and freedom from fear, between bearing witness to something and gawking at it – are complicated, and there are rarely universal legal standards to provide clarity. Being as objective as possible is the only way we can be consistent across the world. But we still sometimes end up making the wrong call.

The hypothetical situations we use to train reviewers are intentionally extreme. They’re designed to help the people who do this work deal with the most difficult cases. When we first created our content standards nearly a decade ago, much was left to the discretion of individual employees. But because no two people will have identical views of what defines hate speech or bullying – or any number of other issues – we now include clear definitions.

We face criticism from people who want more censorship and people who want less. We see that as a useful signal that we are not leaning too far in any one direction.

I hope that readers will understand that we take our role extremely seriously. For many of us on the team within Facebook, safety is a passion that predates our work at the company: I spent more than a decade as a criminal prosecutor, investigating everything from child sexual exploitation to terrorism. Our team also includes a counter extremism expert from the UK, the former research director of West Point’s Combating Terrorism Center, a rape crisis center worker, and a teacher.

All of us know there is more we can do. Last month, we announced that we are hiring an extra 3,000 reviewers. This is
Technology has given more people more power to communicate more widely than ever before. We believe the benefits of sharing far outweigh the risks. But we also recognize that society is still figuring out what is acceptable and what is harmful, and that we, at Facebook, can play an important part of that conversation.
June 15, 2017

Hard Questions: How We Counter Terrorism

By Monika Bickert, Director of Global Policy Management, and Brian Fishman, Counterterrorism Policy Manager

In the wake of recent terror attacks, people have questioned the role of tech companies in fighting terrorism online. We want to answer those questions head on. We agree with those who say that social media should not be a place where terrorists have a voice. We want to be very clear how seriously we take this — keeping our community safe on Facebook is critical to our mission.

In this post, we’ll walk through some of our behind-the-scenes work, including how we use artificial intelligence to keep terrorist content off Facebook, something we have not talked about publicly before. We will also discuss the people who work on counterterrorism, some of whom have spent their entire careers combating terrorism, and the ways we collaborate with partners outside our company.

Our stance is simple: There’s no place on Facebook for terrorism. We remove terrorists and posts that support terrorism whenever we become aware of them. When we receive reports of potential terrorism posts, we review those reports urgently and with scrutiny. And in the rare cases when we uncover evidence of imminent harm, we promptly inform authorities. Although academic research finds that the
radicalization of members of groups like ISIS and Al Qaeda primarily occurs offline, we know that the internet does play a role — and we don’t want Facebook to be used for any terrorist activity whatsoever.

We believe technology, and Facebook, can be part of the solution.

We’ve been cautious, in part because we don’t want to suggest there is any easy technical fix. It is an enormous challenge to keep people safe on a platform used by nearly 2 billion every month, posting and commenting in more than 80 languages in every corner of the globe. And there is much more for us to do. But we do want to share what we are working on and hear your feedback so we can do better.

**Artificial Intelligence**

We want to find terrorist content immediately, before people in our community have seen it. Already, the majority of accounts we remove for terrorism we find ourselves. But we know we can do better at using technology — and specifically artificial intelligence — to stop the spread of terrorist content on Facebook. Although our use of AI against terrorism is fairly recent, it’s already changing the ways we keep potential terrorist propaganda and accounts off Facebook. We are currently focusing our most cutting edge techniques to combat terrorist content about ISIS, Al Qaeda and their affiliates, and we expect to expand to other terrorist organizations in due course. We are constantly updating our technical solutions, but here are some of our current efforts.

- **Image matching:** When someone tries to upload a terrorist photo or video, our systems look for whether the image matches a known terrorism photo or video. This means that if we previously removed a propaganda video from ISIS, we can work to prevent other accounts from uploading the same video to our site. In many cases, this means that terrorist content intended for upload to Facebook simply
• **Language understanding:** We have also recently started to experiment with using AI to understand text that might be advocating for terrorism. We’re currently experimenting with analyzing text that we’ve already removed for praising or supporting terrorist organizations such as ISIS and Al Qaeda so we can develop text-based signals that such content may be terrorist propaganda. That analysis goes into an algorithm that is in the early stages of learning how to detect similar posts. The machine learning algorithms work on a feedback loop and get better over time.

• **Removing terrorist clusters:** We know from studies of terrorists that they tend to radicalize and operate in clusters. This offline trend is reflected online as well. So when we identify Pages, groups, posts or profiles as supporting terrorism, we also use algorithms to “fan out” to try to identify related material that may also support terrorism. We use signals like whether an account is friends with a high number of accounts that have been disabled for terrorism, or whether an account shares the same attributes as a disabled account.

• **Recidivism:** We’ve also gotten much faster at detecting new fake accounts created by repeat offenders. Through this work, we’ve been able to dramatically reduce the time period that terrorist recidivist accounts are on Facebook. This work is never finished because it is adversarial, and the terrorists are continuously evolving their methods too. We’re constantly identifying new ways that terrorist actors try to circumvent our systems — and we update our tactics accordingly.

• **Cross-platform collaboration:** Because we don’t want terrorists to have a place anywhere in the family of Facebook apps, we have begun work on systems to enable us to take action against terrorist accounts across all our platforms, including WhatsApp and Instagram. Given the limited data some of our apps collect as part of their service, the ability to share data across the whole family is indispensable to our efforts to keep all our platforms safe.
Human Expertise

AI can’t catch everything. Figuring out what supports terrorism and what does not isn’t always straightforward, and algorithms are not yet as good as people when it comes to understanding this kind of context. A photo of an armed man waving an ISIS flag might be propaganda or recruiting material, but could be an image in a news story. Some of the most effective criticisms of brutal groups like ISIS utilize the group’s own propaganda against it. To understand more nuanced cases, we need human expertise.

- **Reports and reviews:** Our community — that’s the people on Facebook — helps us by reporting accounts or content that may violate our policies — including the small fraction that may be related to terrorism. Our Community Operations teams around the world — which we are growing by 3,000 people over the next year — work 24 hours a day and in dozens of languages to review these reports and determine the context. This can be incredibly difficult work, and we support these reviewers with onsite counseling and resiliency training.

- **Terrorism and safety specialists:** In the past year we’ve also significantly grown our team of counterterrorism specialists. At Facebook, more than 150 people are exclusively or primarily focused on countering terrorism as their core responsibility. This includes academic experts on counterterrorism, former prosecutors, former law enforcement agents and analysts, and engineers. Within this specialist team alone, we speak nearly 30 languages.

- **Real-world threats:** We increasingly use AI to identify and remove terrorist content, but computers are not very good at identifying what constitutes a credible threat that merits escalation to law enforcement. We also have a global team that responds within minutes to emergency requests from law enforcement.

Partnering with Others
Working to keep terrorism off Facebook isn’t enough because terrorists can jump from platform to platform. That’s why partnerships with others — including other companies, civil society, researchers and governments — are so crucial.

- **Industry cooperation:** In order to more quickly identify and slow the spread of terrorist content online, we joined with Microsoft, Twitter and YouTube six months ago to announce a shared industry database of “hashes” — unique digital fingerprints for photos and videos — for content produced by or in support of terrorist organizations. This collaboration has already proved fruitful, and we hope to add more partners in the future. We are grateful to our partner companies for helping keep Facebook a safe place.

- **Governments:** Governments and inter-governmental agencies also have a key role to play in convening and providing expertise that is impossible for companies to develop independently. We have learned much through briefings from agencies in different countries about ISIS and Al Qaeda propaganda mechanisms. We have also participated in and benefited from efforts to support industry collaboration by organizations such as the EU Internet Forum, the Global Coalition Against Daesh, and the UK Home Office.

- **Encryption.** We know that terrorists sometimes use encrypted messaging to communicate. Encryption technology has many legitimate uses — from protecting our online banking to keeping our photos safe. It’s also essential for journalists, NGO workers, human rights campaigners and others who need to know their messages will remain secure. Because of the way end-to-end encryption works, we can’t read the contents of individual encrypted messages — but we do provide the information we can in response to valid law enforcement requests, consistent with applicable law and our policies.

- **Counterspeech training:** We also believe challenging extremist narratives online is a valuable part of the response to real world extremism. Counterspeech comes in many forms, but at its core these are efforts to prevent people
from pursuing a hate-filled, violent life or convincing them to abandon such a life. But counterspeech is only effective if it comes from credible speakers. So we’ve partnered with NGOs and community groups to empower the voices that matter most.

- **Partner programs:** We support several major counterspeech programs. For example, last year we worked with the Institute for Strategic Dialogue to launch the Online Civil Courage Initiative, a project that has engaged with more than 100 anti-hate and anti-extremism organizations across Europe. We’ve also worked with Affinis Labs to host hackathons in places like Manila, Dhaka and Jakarta, where community leaders joined forces with tech entrepreneurs to develop innovative solutions to push back against extremism and hate online. And finally, the program we’ve supported with the widest global reach is a student competition organized through the P2P: Facebook Global Digital Challenge. In less than two years, P2P has reached more than 56 million people worldwide through more than 500 anti-hate and extremism campaigns created by more than 5,500 university students in 68 countries.

**Our Commitment**

We want Facebook to be a hostile place for terrorists. The challenge for online communities is the same as it is for real world communities – to get better at spotting the early signals before it’s too late. We are absolutely committed to keeping terrorism off our platform, and we’ll continue to share more about this work as it develops in the future.

*Read more about our new blog series Hard Questions. We want your input on what other topics we should address — and what we could be doing better. Please send suggestions to hardquestions@fb.com.*
Introducing Hard Questions

Giving People More Control Over Their Facebook Profile

June 26, 2017

Facebook, Microsoft, Twitter and YouTube Announce Formation of the Global Internet Forum to Counter Terrorism

Related News

1 Comment

Kavita Joshi
Safely and Enjoying Facebook

Like · Reply · Sep 22, 2017 9:30am

Facebook Comments Plugin

Category: Hard Questions

Introducing Hard Questions

Giving People More Control Over Their Facebook Profile

Picture
*INTRODUCTION

Scott McNealy, the Chairman and former CEO of Sun Microsystems, caused an uproar in 1999 when he dismissed online privacy concerns and proclaimed, “You have zero privacy anyway. Get over it.”¹ Was he right? Within the realm of cloud computing, he may have been uncomfortably close to the truth. The Stored Communications Act (SCA),² a component of the broader Electronic Communications Privacy Act (ECPA),³ is the primary federal source of online privacy protections, but it is more than twenty years old. Despite the rapid evolution of computer and networking technology since the SCA's adoption, its language has remained surprisingly static. The resulting task of adapting the

² SC 1202

³ SC 1738
Act’s language to modern technology has fallen largely upon the courts. In coming years, however, the courts will face their most difficult task yet in determining how cloud computing fits within the SCA’s complex framework.

This Note ultimately concludes that the advertising supported business model embraced by many cloud computing providers will not qualify for the SCA’s privacy protections. In exchange for “free” cloud computing services, customers are authorizing service providers to access their data to tailor contextual and targeted advertising. This quid pro quo violates the SCA’s requirements and many customers will find that their expectations of privacy were illusory. Consequently, a cloud provider’s terms of service agreement may be the only privacy protections applicable to its customers.

Subsequently, this Note explores whether the lack of privacy protections for cloud computing is consistent with Congress's intent in adopting the SCA and whether it will be a catalyst for expanding privacy measures in the future. In response, Part V explores the SCA's legislative history and argues that the modern form of cloud computing is incompatible with the concerns and Fourth Amendment principles that motivated Congress's adoption of the Act. Part VI further examines potential judicial, legislative, and societal forces that could prompt revisions to the SCA, but concludes that the lack of privacy protections in cloud computing is unlikely to be addressed anytime soon.

I. CLOUD COMPUTING: AN EMERGING DEFINITION

A. A BRIEF HISTORY OF COMPUTER NETWORKING

The law cannot keep up with the pace of change in computer networking. By the time legislatures or courts figure out how to deal with a new product or service, the technology has already progressed. It is, therefore, useful to learn the state of technology at the time Congress enacted a law or the Judiciary issued a legal opinion to clarify the logic and principles that girded its decision. This is particularly true of the Stored Communications Act, which Congress structured around the state of technology in 1986. To understand the Act, and recent innovations to which it might apply, a quick tour of some computer history is necessary.

Early computer technology was prohibitively expensive for all but the largest businesses and organizations. In 1965, IBM offered to rent its early mainframe computers for $50,000-$80,000 per month because few customers could afford their $2.2 million-$3.5 million price tag. By 1970, the rental cost of increasingly sophisticated IBM mainframes grew to $190,000-$270,000 per month and the purchase price exceeded $12 million. The few entities that could afford a mainframe, including the Department of Defense, the Internal Revenue Service (IRS), and the National Aeronautics and Space Administration (NASA), shared its processing power and data storage with the entire organization. The mainframe was a centralized resource that employees could access through lab-coat wearing specialists in their IT department or by using a “dumb” computer terminal that existed only as a gateway to the mainframe's functionality.

By the early 1980s, new advances diminished reliance on mainframes. Increasingly powerful personal computers allowed individual users to install applications and store data on their own equipment, rather than using a shared mainframe computer. The development of operating systems, such as Microsoft's MS-DOS and Apple's Macintosh interface, also made computers more friendly to the average user. By 1984, personal computer sales eclipsed those of large corporate mainframes in the $22 billion computer industry.

As computing decentralized, networking quickly developed. Users needed something more efficient than a large floppy disk to send a file created on their computer to a colleague. In corporate environments, users interconnected

*1198 As computing decentralized, networking quickly developed. Users needed something more efficient than a large floppy disk to send a file created on their computer to a colleague. In corporate environments, users interconnected
through a private, internal network to reach the company's e-mail server or communicate with co-workers. Many personal users began subscribing to self-contained networks, such as Prodigy, CompuServe, and America Online. Subscribers typically paid based on the amount of time they were connected to the network; unlike today's Internet users, few could afford to spend hours casually exploring the provider's network. After connecting to the network via a modem, users could download or send e-mail, post messages on a “bulletin board” service, or access information. It was on the cusp of this phase, with computer networking in its infancy, that Congress adopted the Stored Communications Act in 1986.

A new disruptive technology soon changed the course of networking. The World Wide Web arrived in 1990 and allowed the integration of individual networks via the Internet. The introduction of the web browser, such as Netscape Navigator in 1994, made it even easier for users to access and explore the content available through the Internet. Internet usage exploded and by 1997 more than fifty-six million Americans had Internet access at home, work, or school.

The Internet's capabilities continue to expand rapidly with the addition of new technologies and enormous infrastructure investment. Providers, such as Hulu (video content), the iTunes store (music and video content), and Skype (telephone and videoconferencing services), are now capitalizing on these enhancements to offer new Internet-based services. These services are possible, in part, due to the growing availability of high-speed Internet access; in April 2009, sixty-three percent of adults in the United States had a broadband Internet connection in their home. Mobile Internet access, through devices such as the iPhone, is also spreading rapidly and extending the Internet's reach beyond the home and workplace. These changes have made the Internet a ubiquitous part of our daily lives.

B. THE ERA OF CLOUD COMPUTING

The increasing functionality of the Internet is decreasing the role of the personal computer. This shift is being led by the growth of “cloud computing”—the ability to run applications and store data on a service provider's computers over the Internet, rather than on a person's desktop computer. Service providers operate a group of computer servers that are connected to each other and function as a single “cloud” of resources. The cloud is configured to divide the tasks of running applications and storing data into small chunks and to distribute them among the servers' aggregate resources. Providers recognize that this is difficult for the average user to understand and market the service as “cloud computing” to help strip away the complexity.

Many Internet users have experienced cloud computing, but fail to recognize or understand the technology making it possible. For example, most computer users are familiar with the operation of word processing programs, such as Microsoft Word. The program runs on the user's computer and the resulting documents are saved on the computer's hard drive. In contrast, cloud computing allows a user to complete the same task on the Internet. An Internet user can access a word processing application, such as Google Documents, that resides on a service provider's computers and save the completed document on the provider's server to access later. The user's computer is irrelevant in this process. This structure closely resembles the early mainframe computing model; instead of a “dumb terminal” designed solely to access a mainframe's resources, the personal computer is beginning to serve as a “dumb terminal” to access cloud computing's resources via the Internet.
The increasing importance of cloud computing is underscored by the intense competition it is creating within the technology industry. Many of the industry's largest players are moving aggressively to capitalize on the growing popularity of cloud computing and capture market share. In the midst of this competitive chaos, participants are organizing into opposing factions to promote different standards and operating principles to guide the development of cloud computing. The industry cannot even agree on the meaning of the term “cloud computing.” These battles have Internet forums and media outlets buzzing with anticipation about the potential for a period of open warfare within the industry.

Cloud computing promises to overcome the inefficiencies created when everyone has their own computer—a “dispersed computing” structure. For the last several decades, computer companies focused their efforts on building faster processors and higher capacity storage devices. Despite the extra capacity this created, three problems inherent in a dispersed computing structure have not been resolved. First, computer purchasers must buy more processing power and storage capacity than they currently need to anticipate future growth or rare moments of peak demand. Until that day comes, if it ever does, that expensive capacity will remain idle and unproductive. Second, the assembly and maintenance of computer equipment and applications requires users to develop technological expertise. This is a costly and time consuming endeavor that distracts organizations and individuals from other activities in which they offer specialized knowledge or abilities. Finally, dispersed computing lacks the redundancy necessary to protect valuable data and overcome equipment failures. Everyone has an unfortunate tale of a hard drive failure that resulted in hours, weeks, or years of lost effort and memories. While this is a painful event for a person, it can be disastrous for a business. When a calamity or technology failure strikes, essential data is lost and workforces are idled—unless redundant storage or processing power is available to remedy the problem.

Advances in computer and networking technology have also surmounted many of the limitations that encouraged the initial development of a dispersed computing model. Network capacity and transmission speeds presented the largest roadblocks to cloud computing in earlier years. Users need a fast Internet connection to upload or retrieve large quantities of data or interact with a server-based application in real-time. Until recently, though, the unavailability or expense of broadband Internet access limited many users to relatively slow dial-up connections. The widespread deployment of fiber optics, high-speed DSL, and cable broadband services during the last decade overcame this problem across much of the nation and most American households now have access to high-speed Internet. Additionally, the software and hardware required to share computing resources among multiple users advanced rapidly. Cloud providers must be able to divide users' tasks among CPUs, allocate storage capacity efficiently, and safeguard users' transmissions and stored data. These challenges are now being met with innovative solutions, including multicore processing technology, grid-computing infrastructure, and improved data center architecture.

While computer science created the ability to provide cloud computing, other factors were creating the demand. Escaping the endless cycle of buying and installing “upgrades” required by technology vendors is among cloud computing's most attractive features. By withdrawing support for previous hardware and software versions, technology companies essentially force users to buy their latest products. Yet, these upgrades can be difficult and costly to install and any new features they include offer little benefit to many users. Additionally, as people and organizations shift their data to a digital environment, the constraints of the personal computer are becoming more visible and less acceptable. A major limitation is people's need to interact with their applications or data while outside the home or office. Colleagues also struggle to collaborate on projects when content is trapped inside a personal computer. A common frustration is the
inability to jointly review or edit a document or presentation with other users. A personal computer user may need to
distribute the file via e-mail and manually synthesize the comments and edits received back from reviewers. 43

Cloud computing helps users circumvent these difficulties by making the personal computer largely irrelevant. 44 A cloud
user only needs to have a device connected to a cloud provider--a laptop, smartphone, or shared public computer will
suffice. 45 Both the application and data are stored in the cloud, allowing the cloud provider to install upgrades and
complete the maintenance for all of its users simultaneously. 46 The cloud user can focus on the desired task, rather
than the infrastructure or technology making it all possible.

Widespread consumer embrace of early cloud computing offerings suggests that a meaningful shift is underway, rather
than a passing fad. Webmail--e-mail services offered by a cloud provider through an Internet-based user interface-- was
among the first cloud computing services offered to the public. 47 This form of cloud computing--known within the
computer industry as “Software as a Service” 48 --moved e-mail from desktop applications, such as Microsoft Outlook, to
Internet-based e-mail applications running on cloud providers' servers. 49 Webmail offered users several improvements
over its desktop predecessors, such as remote access from any Internet-enabled device. The public quickly embraced
webmail services and millions have since established e-mail accounts with cloud providers such as Hotmail, Yahoo! Mail,
and Gmail. 50 Webmail's popularity led to the rapid development of other cloud-based applications, including calendars,
contact management, word processing, and digital photo applications. 51 Many desktop application publishers recognize
this trend and are changing their programs to operate in a cloud-based configuration. 52

Recent developments in cloud computing will further decentralize control over the applications and services hosted on a
cloud provider's infrastructure. Many providers are shifting away from designing their own applications (the “Software
as a Service” model) and instead opening up their systems to third-party developers who create applications that run on
the cloud provider's platform (the “Platform as a Service” model). 53 This cloud computing model allows programmers
to develop new applications or create “mashups” that combine the capabilities of multiple cloud applications. 54 Opening
the cloud *1204 platform to third-party programmers is likely to rapidly increase the pace of development and
functionality. 55 Additionally, some cloud providers are selling raw computer resources, including processing power and
data storage, as a type of utility service (the “Hardware as a Service” model). 56 These providers are offering their services
with usage-based rates that mirror the pricing structure used by electric utilities. 57 This business model is expanding
rapidly as users and providers realize its benefits. For consumers, these services provide access to reliable and easily
expandable computing resources for much less effort and cost than would be required to buy and maintain the hardware
themselves. 58 Meanwhile, providers recognize the opportunity to profit from their large reservoirs of unused processing
and storage capacity. 59

Cloud computing, through its applications, platforms, and services, is already affecting the ways that people and
businesses interact with and use computers and the Internet. The viability of the technology and its growing acceptance
by consumers and service providers offer powerful evidence that a lasting technological and societal shift is underway.
As a result, courts will need to determine how existing laws may or may not protect electronic communications and
content in this new computing model.

II. ORIGINS AND OPERATION OF THE STORED COMMUNICATIONS ACT
The Stored Communications Act is best understood by considering its operation and purpose in light of the technology that existed in 1986. The Act is not built around clear principles that are intended to easily accommodate future changes in technology; instead, Congress chose to draft a complex statute based on the operation of early computer networks. To apply the Act to modern computing, courts need to begin by extracting operating principles from a tangled legal framework. Fortunately, several sources can guide an inquiry into congressional intent. First, the legislative history of the Stored Communications Act, as represented in committee reports and transcripts of hearings from the House of Representatives and Senate, offers extensive background into the technology and problems that prompted the need for the legislation. Second, Congress notes its explicit reliance on a report from the Office of Technology Assessment (OTA) prepared in 1985 to review the potential threats to civil liberties resulting from new or emerging technologies. Finally, the language and structure of the Act offers some clues into Congress's approach to privacy in computer networks.

The first step in deciphering the Stored Communications Act is to recognize the two primary uses of computer networks that Congress sought to regulate: (1) electronic communication services (ECS) designed to handle “data transmissions and electronic mail” and (2) remote computing services (RCS) intended to provide outsourced computer processing and data storage. Congress decided to build the Act around these two categories and apply differing privacy protections to each. Any analysis under the Act must begin by classifying the data in question within one of these categories.

A. ELECTRONIC COMMUNICATION SERVICES

Congress explored the category of electronic communication services, designed to transmit information and data between users, primarily through the lens of early electronic mail systems. At the time, e-mail operated through a fragmented delivery system in which communications were slowly transmitted between the computer servers operated by e-mail providers. Each provider's servers would temporarily store an e-mail until transmitting it along to its next waypoint. After an e-mail reached its destination, the recipient would use a dial-up modem to connect to her e-mail provider and download the message to her computer; alternatively, some providers would conveniently “put the messages onto paper and then deposit it in the normal postal system.”

Elected officials struggled to understand this new technology and relied on analogies to the more familiar postal service. However, important differences limited the analogy's value. For example, the House report on the Act specifically noted that e-mail differs from traditional postal mail in that the service provider “may technically have access to the contents of the message and many retain copies of transmissions.”

The fragmented e-mail system used in the mid-1980s is embodied in the Stored Communications Act's provisions governing electronic communication services (ECS). A service provider needs to satisfy two requirements for communications stored on its system to receive the ECS privacy protections offered by the Act. First, the service provider must offer users “the ability to send or receive ... electronic communications.” Electronic communications is broadly defined to mean nearly any form or style of communication, including “signs, signals, writings, images, sounds, data or intelligence of any nature.” Second, the service provider must hold the electronic communication in “electronic storage.” This requirement is commonly misunderstood because the statutory definition of “electronic storage” is much narrower than its name suggests. The Act limits “electronic storage” to mean (1) “temporary, intermediate storage ... incidental to the electronic transmission” of the communication and (2) copies made by the service provider for “backup protection.” This rather odd definition is better understood in light of the e-mail delivery system in place at the
time, which required multiple service providers to store communications briefly before forwarding them on to their next destination or while awaiting download by the recipient. 73

B. REMOTE COMPUTING SERVICES

Congress created a second category covering “remote computing services” to address third-party service providers that offered “sophisticated and convenient computing services to subscribers and customers from remote facilities.” 74 Buying a lot of processing or storage capacity was prohibitively expensive for many organizations in 1986. Outsourcing these functions to a service provider, however, created economies of scale that offered a sustainable cost structure for the new technology. 75 The Senate report about the Stored Communications Act notes that “[i]n the age of rapid computerization, a basic choice has faced the users of computer technology. That is, whether to process data in-house on the user's own computer or on someone else's equipment.” 76 A company or organization that decided to outsource its computing needs would transmit its data for processing either to a third-party service provider's personnel or directly transfer it to the provider's remote computer. 77 At the time of the Act's adoption, outsourced computing was a service marketed to “businesses of all sizes--hospitals, banks and many others,” rather than individual consumers. 78

Congress included the category of remote computing services (RCS) in the Stored Communications Act to ensure the privacy of data outsourced to these third-party service providers. 79 A service provider must meet strict requirements to qualify as an RCS and enjoy the benefit of privacy protections for its customers' data. First, the provider must offer “computer storage or processing services” to the public through an electronic communications system. 80 Second, the data must be received electronically from the customer. 81 Third, the content must be “carried or maintained” by the service provider “solely for the purpose of providing storage or computer processing services” to the customer. 82 Finally, the provider cannot be “authorized to access the [customer's] content for purposes of providing any services other than storage or computer processing.” 83 The requirements for RCS precisely describe the nature of the commercial relationship that existed at the time of the Act's adoption between the outsourced computing providers and their business clientele. 84

C. PRIVACY PROTECTIONS

If a computing service qualifies as an electronic communication service (ECS), the Act provides two levels of privacy protection depending on whether disclosure of the communication is voluntary or compelled by the government. 85 Under the first tier, an ECS provider may voluntarily disclose a user's communication if one of eight conditions is satisfied, such as when the communication's sender or recipient consents or when necessary for “the protection of the rights or property of the provider.” 85 A second tier imposes much greater restrictions when the government seeks compelled disclosure from the ECS provider. 86 In these instances, a search warrant is required if the communication has been in “electronic storage” on the provider's service for 180 days or less. 87 After 180 days, the government may use an alternate legal process with a lower causal threshold. 88

Data stored by a remote computing service (RCS) is subject to the same two-tiered approach, but receives fewer privacy protections than communications held by an ECS. An RCS provider may voluntarily disclose a customer's data in compliance with one of the same eight statutory exceptions applicable to an ECS provider. 89 However, the second tier protections against compelled disclosure by the government are more limited. Data stored in an RCS for any duration...
may be accessed by the government through a § 2703(d) order requiring only “reasonable grounds to believe” the data is “relevant and material to an ongoing criminal investigation.” 90

In both an ECS and RCS, personal identifying information about the user, such as her name, physical or e-mail addresses, and IP address, is entitled to little protection. A service provider can voluntarily disclose the user's personal identifying information to any non-governmental entity 91 or provide it directly to the government upon receipt of an administrative subpoena. 92

Among the Act's most significant, although unstated, privacy protections is the ability to prevent a third party from using a subpoena in a civil case to get a user's stored communications or data directly from an ECS or RCS provider. Courts interpret the absence of a provision in the Act for compelled third-party disclosure to be an intentional omission reflecting Congress's desire to protect users' data, in the possession of a third-party provider, from the reach of private *1209 litigants. 93 Without this blanket immunity from subpoena in civil cases, a user's entire portfolio of stored communications and data might be fair game for an adversary. An important limitation to this privacy safeguard is the Act's allowance for a service provider to voluntarily share a user's personal identifying information with a non-governmental entity. 94 Consequently, an ECS or RCS provider is only limited by its contractual relationship with the user in deciding whether to respond for requests, via subpoena or otherwise, for a user's personal identifying information. 95

III. CLOUD COMPUTING AS AN ELECTRONIC COMMUNICATION SERVICE

Many cloud computing services fail to qualify for the heightened privacy protections provided to electronic communication services (ECS) in the Stored Communications Act. One of the Act's twin requirements is that an ECS give users “the ability to send or receive ... electronic communications.” 96 Yet, many of today's popular cloud computing services are designed for purposes other than communication, such as word processing or digital photo storage, and lack any “send or receive” capability. 97

Cloud services further violate the second condition for an ECS requiring that communications be held in “electronic storage.” 98 As discussed previously, electronic storage is a term of art within the SCA that is limited to (1) storage of a “temporary [and] intermediate” nature that is “incidental to the electronic transmission” of the communication or (2) storage of the communication by the ECS provider to provide backup protection. 99 But cloud services satisfy neither of these definitions. Contrary to the requirement that storage be temporary and incidental to the service, many cloud providers offer their customers generous *1210 storage capacity to enable long-term data retention. 100 As an example, the Google Documents service offers its customers the ability to store 5000 documents and presentations, in addition to 1000 spreadsheets--far more than any customer may need for temporary purposes. 101 Furthermore, the supplemental services that cloud providers offer clarify their intent to serve as a final repository for their customers' data, rather than a source of backup protection. For instance, many cloud providers offer their data storage services alongside applications designed to manipulate that data or mobile applications for accessing that data through remote computers. 102 Because users' content is not being stored by the ECS provider within the SCA's narrow definition of electronic storage, the ECS protections are inapplicable.

Webmail services are an exceptional category of cloud services that may qualify as an ECS. These cloud services offer customers the ability to “send or receive” e-mail and, therefore, satisfy the first prong of the ECS requirements. 103
The further requirement that communications be in “electronic storage” is more problematic, but expansive court interpretations provide some relief. Every circuit to consider the issue agrees that unopened e-mail remains in electronic storage for 180 days because it is being held temporarily until the recipient reads or retrieves it. The vast majority of unopened e-mail stored by a webmail service will, therefore, qualify as a electronic communication held by an ECS and receive the Act's privacy protections.

After an e-mail is opened, however, the analysis becomes more complicated. Many courts hold that an electronic communication is complete the moment it is opened or downloaded by its intended recipient. These courts reason that, upon completing the journey to the recipient, the e-mail converts immediately into plain data that the user can store or delete. Once viewed or downloaded though, the e-mail is no longer considered an “electronic communication” and the service provider is no longer an ECS with respect to that e-mail.

In these circuits, the loss of ECS protection is not the end of the story. The same provider can act in both an ECS and RCS capacity, and the services it provides must be considered individually to determine which standard is applicable in a given situation. Therefore, the possibility remains that a cloud provider might be acting as a remote computing service when storing the opened e-mail for its customer. Congress foresaw a similar situation within the legislative history of the Act:

Sometimes the addressee, having requested and received a message, chooses to leave it in storage on the service for re-access at a later time. The Committee intends that, in leaving the message in storage, the addressee should be considered the subscriber or user from whom the system received the communication for storage, and that such communication should continue to be covered by [the RCS provisions of] section 2702(a)(2).

A split among federal courts now complicates this otherwise straightforward analysis, but may provide greater protections for some webmail customers. In Theofel v. Farey-Jones, the Ninth Circuit held that an opened e-mail remains in “electronic storage” and, therefore, the communication continues to be protected by the Act's ECS provisions while it remains in storage with the provider. The Theofel decision embraces the novel theory that customers are storing opened e-mail on the provider's server as a form of backup protection--one of the two permissible definitions of “electronic storage.” The Ninth Circuit recently reaffirmed its holding in Theofel, but the decision continues to receive substantial judicial and academic criticism. Although the Ninth Circuit's position may be unpopular, the critical mass of technology companies located within the Circuit causes this reading of the Act's requirements for webmail to be applied in many cases.

IV. CLOUD COMPUTING AS A REMOTE COMPUTING SERVICE

A. APPLICATION OF THE STATUTORY LANGUAGE

At first glance the Stored Communications Act's requirements for a remote computing service (RCS) offer false hope that they will apply to cloud computing services. The RCS provisions in the Act would seem to be an intuitive fit for cloud computing because Congress originally added them to address outsourced computer processing and data storage. In many ways, cloud computing is a reversion to and expansion of this practice. The Act's language also offers some initial appeal for cloud computing. To qualify as an RCS, the cloud service must publicly offer “computer storage or
processing services” over a network. Most cloud providers offer both of these services via the Internet and would appear to satisfy this requirement. Some courts, relying on this short analysis, have applied the RCS provisions to cloud computing services, with alleged support from the Act's legislative history and the concurrence of legal scholars.

This analysis of cloud computing is flawed though because it fails to account for the Act's remaining requirements. Besides the types of services that may be provided, an RCS must satisfy five other prerequisites. As an initial matter, the data must (1) contain “content[],” (2) be “carried or maintained ... on behalf ... a subscriber or customer,” and (3) have been electronically transmitted to the provider. A cloud service will ordinarily satisfy these requirements. However, the final two requirements to be an RCS necessitate closer scrutiny. The Act demands that the customer's data be transmitted to the cloud provider “solely for the purpose of providing storage or computer processing services.” Finally, it insists that the cloud provider “not [be] authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.”

Cloud providers commonly embrace a business model that leaves the final two requirements unsatisfied and, as a result, they will not qualify as an RCS. Many cloud providers rely extensively on advertising revenue, rather than fees from customers, to fund their offerings. Although advertising does not violate the Act's requirements, a subset of cloud providers have sought a competitive advantage, against other advertising platforms, by providing contextual or targeted advertising opportunities. In these systems, advertisers no longer pay to reach every visitor to a particular website or advertising network. Instead, contextual advertising allows a marketing campaign to target a specific audience based on the content a website visitor is accessing. For example, a widget retailer can use the Google AdWords system to buy a keyword, such as “widget,” and ensure that its advertising appears whenever a website visitor browses content related to widgets on a website participating in the Google AdSense program. This marketing mechanism is particularly effective because it allows advertisers to appear at the moment a potential customer may be most receptive.

Contextual advertising requires access to content though, which violates the Stored Communications Act's requirements. Cloud users often authorize a provider to access their stored data--through implied or explicit consent to the provider's terms of service agreement and privacy policy--as a condition of using a cloud computing service. By sharing their data with the cloud provider, users make possible the advertising services that pay for the costs associated with providing the cloud service--a model familiar to radio listeners and television viewers who have long accepted commercials embedded in programming to offset some or all of its cost. In essence, a customer's privacy is the true cost of “free” cloud computing services.

But a customer's willingness to share her data for advertising purposes has privacy implications well beyond the relationship with the cloud provider. The Act's RCS privacy protections require that “storage or computer processing” be the sole reason that a customer transmits her data to the cloud provider. When data is also shared with the cloud provider to facilitate contextual advertising, this requirement is not satisfied. The Act further requires that the cloud provider only be authorized to access the customer's data to provide the processing or storage service. However, by agreeing to share her data with the cloud provider for contextual advertising purposes, this additional requirement is unfulfilled. The applicability of the RCS provisions in the Stored Communications Act will, therefore, always require examining the cloud provider's terms of service agreement and privacy policy. If a customer authorizes access to her data for the provision of contextual or targeted advertising services, the Act will not apply and the data will be at risk of disclosure to the government or another third party.
B. AN EXAMINATION OF EXISTING CLOUD PROVIDERS

Analyzing the existing terms of service agreements and privacy policies in use by large cloud providers offers insight into the types of data sharing provisions that courts are likely to encounter. Terms of service agreements and privacy policies are omnipresent and nearly every large company relies on them to regulate the use of its website and to disclose its data handling practices. Both documents are contracts that define the relationship between website operators, including cloud providers, and their visitors. Despite knowing that people rarely read them, courts often bind website visitors to these agreements. Yet, few cloud providers likely anticipate or understand the broader significance these agreements have for their customers' privacy under the Stored Communications Act.

Terms of service agreements and privacy policies in use by several major cloud providers offer varying degrees of authority to access a customer's data. The agreements can generally be classified into three categories: (1) explicit authority to access a customer's data for marketing purposes, (2) vague authority to potentially access a customer's data for purposes beyond the primary services, and (3) explicit prohibitions against accessing a customer's data for any purpose other than providing a specific service. Each type of agreement is likely to lead to a different conclusion under the Act's remote computing services standard and requires a unique analysis.

The least protective agreements empower cloud providers to access a customer's data for many purposes, including advertising. Google, one of the largest cloud providers, uses such agreements extensively. Google's advertising system relies on customers' data, among other variables, to provide targeted marketing opportunities for advertisers. To facilitate this service, Google uses a master terms of service (“ToS”) agreement and a master privacy policy that apply to all of its cloud services, supplemented by smaller sub-agreements with provisions unique to each service.

The master ToS agreement states that “Google reserves the right ... to pre-screen, review, flag, filter, modify, refuse or remove any or all Content from any [Google] Service.” With regard to the Gmail service, Google is overt with respect to its use of this authorization for marketing purposes; the Google Privacy Center informs customers that “[t]he Gmail filtering system also scans for keywords in users' e-mails which are then used to match and serve ads. When a user opens an e-mail message, computers scan the text and then instantaneously display relevant information that is matched to the text of the message.”

Furthermore, the master ToS agreement requires customers to agree that “[b]y submitting, posting or displaying the content you give Google a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any Content which you submit, post or display on or through, [Google's] Services.” Google, therefore, not only reserves the right to access a customer's data for any purpose, but also to disclose it publicly.

Sometimes Google's ToS agreements can even reach beyond a customer's own data and into the content of a third party. For example, website owners can use Google's popular AdSense marketing platform to earn money by displaying contextual advertising on their website. Of course, Google needs to know what type of content is appearing on the website to allow it to deliver properly targeted advertising. To secure this access, Google's ToS agreement for the AdSense service authorizes it to “access, index and cache” the customer's website. While a website owner might willingly expose her own content to Google, she must also be mindful of her customers' data that is stored or displayed on the website.
Thus, website owners participating in the AdSense program need to ensure they have authorization to share their own customers' data with Google for advertising purposes. 137

It is unfair to single out Google as having a particularly expansive agreement because many other cloud providers are similarly up-front about their intention to access customers' data for advertising purposes. Evernote, a cloud provider offering customers an online repository for documents, images, and other content, states that its services “may be supported by advertising revenue” and “display advertisements ... [that] may be targeted to Content subject matter.” 138 In order for Evernote to provide this targeted advertising, an express quid pro quo is written into its ToS agreement requiring customers to “agree that Evernote may present advertising in connection with the Service in consideration *1217 for the rights granted [customers] to access and use the Service.” 139  Epernicus, another cloud provider of social networking services, requires users to grant it an unrestricted license to access and use users' content “for any purpose, commercial, advertising, or otherwise.” 140

Other cloud providers use a terms of service agreement and privacy policy that occupy an ambiguous middle ground. The ToS agreements in use by these providers reserve the right to access a customer's data, but offer little guidance as to when or how that authority might be used. Several popular cloud providers, including Amazon Web Services and YouTube, use agreements with such indeterminate language. 141 Some of these providers, however, offer non-binding guidance about their intended use of that authority. For example, Yahoo! reserves the right to “pre-screen” content on its service, 142 but, at least for its webmail service, explains in its privacy policy that “Yahoo!'s practice is not to use the content of messages stored in your Yahoo! Mail account for marketing purposes.” 143

A final group of cloud providers rely on ToS agreements that offer customers an explicit promise not to access their data. Some providers, such as Remember the Milk, a cloud provider offering a task management application, disavow any authority to access a customer's data stored on its service. 144  Mozy, a cloud provider offering automated back-up storage for consumers, tries to assure customers about the privacy of their content by plainly asserting, “We will not view the files that you backup using the Service.” 145  Interestingly, rather than following Mozy's approach and offering a general promise not to access customers' data, many cloud providers elect to go even further and also specifically disclaim the ability to access content for advertising purposes. 146

**1218 C. EXISTING JUDICIAL PRECEDENTS**

Before analyzing how these differing terms of service agreements and privacy policies will be applied under the Stored Communications Act, it is helpful to survey the Act's existing jurisprudence. Courts have considered the precise contours of the Act's remote computing service (RCS) provisions in surprisingly few cases. For many years, outsourced computing services declined in popularity and the RCS provisions came to be viewed as antiquated and irrelevant. 147 However, two recent cases demonstrate that technology evolves in surprising ways and new computing services, including cloud computing, will reinvigorate the RCS privacy protections.

In Flagg v. City of Detroit, the defendants argued that the RCS provisions applied to stored text messages. 148 Because the Act does not allow an RCS provider to disclose a customer's data to an opposing party in civil litigation, the defendants sought to qualify the text messaging service as an RCS to prevent the service provider from divulging their messages. 149 While the court conceded that there is not a discovery mechanism for data stored in a qualifying RCS, it held that the text messaging service failed to satisfy the requirements to be a remote computing service. The court noted that
the Act requires that an RCS provider not be “authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.” 150 In a strict interpretation of this requirement, the court held that the text messaging service provider was authorized to access a customer's messages to provide the additional “service of retrieval” for stored text messages. 151 Consequently, the stored text messages were not protected by the RCS privacy protections and their production during civil litigation was appropriate. The court proceeded to determine that, even if the text messages were being stored on an RCS, two of the eight exceptions allowing their disclosure would apply. 152

The Flagg court's interpretation of the requirements for an RCS cautions that many cloud computing users will not enjoy the Stored Communications Act's privacy protections. Any cloud service necessarily requires the “service of retrieval” for using applications or data stored with the cloud provider. Based on *1219 the interpretation applied in Flagg, this “service” would universally disqualify cloud providers and their customers from seeking refuge from disclosure under the Act. However, there are several reasons to believe that this reading of the Act's requirements is unduly harsh. Most importantly, it would seemingly invalidate Congress's allowance for an RCS to provide computer storage, which requires the ability to later retrieve customers' stored data. The Flagg court's opinion includes multiple alternate holdings and suggests that it too was unsure about the soundness of this argument. Regardless of its precise holding, the court's approach to interpreting the RCS provisions in the Act may prove more informative. Flagg suggests, at a minimum, that future courts will strictly interpret and rigidly impose the Act's RCS provisions and are unlikely to offer leniency when a cloud provider is allowed to access customers' data for advertising or other purposes not explicitly authorized in the Act.

In Viacom International Inc. v. YouTube Inc., a district court interpreted the remote computing service provisions within the context of a cloud provider's video sharing service. 153 The court held that YouTube qualified as an RCS when storing private videos and other user content on its cloud service. 154 In a brief footnote, the opinion notes that YouTube was authorized by its terms of service agreement to “access and delete potentially infringing private videos.” 155 The court determined that this authorization was permissible under the Act because it occurred “in connection with [YouTube]'s provision of alleged storage services”--presumably a reference to the exception allowing cloud providers to access a customer's data when it is “necessarily incident to the rendition of the service.” 156 The court relied almost exclusively on an analysis of YouTube's terms of service agreement to reject an additional argument that customers' videos should be disclosed under the SCA's consent exception. 157 After dissecting the ToS agreement, the court determined it did not offer a user's implied consent to divulge private videos to unauthorized third parties.

Viacom provides valuable guidance on the interaction between the RCS provisions and a non-webmail cloud service. The court's extensive reliance on YouTube's terms of service agreement shows the increasingly important role these contracts are serving to define the legal rights of cloud providers and their customers--well beyond the scope of their contractual relationship with each other. Viacom also follows Flagg's approach of narrowly reading the scope of the “solely for storage or computer processing” requirement for an RCS. In both cases, the courts questioned whether any actions by the service provider, even slightly different from its primary storage function, could disqualify the customer's data from the Act's privacy protections. The courts in Flagg and Viacom hesitated to allow basic functions, such as retrieval or screening for unlawful *1220 content, to come within the RCS provisions, which suggests a court would almost certainly reject instances where a cloud provider is authorized to access a user's content for advertising or other tangential purposes.

D. INTERPRETING TERMS OF SERVICE AGREEMENTS
The judicial precedents interpreting the remote computing service (RCS) provisions, although limited, offer valuable guidance in determining how courts are likely to apply the Act's requirements to cloud providers.

The two categories of terms of service (ToS) agreements and privacy policies on the ends of the spectrum offer relatively straightforward analyses. The category of protective agreements that expressly limit or disclaim the cloud provider's authority to access a customer's data for any secondary purposes, including advertising, is the most likely to qualify under the Act. Because these cloud providers are confining their access to the underlying "storage or computer processing" services, the Act's plain language is satisfied. Therefore, these cloud services will likely survive scrutiny under the RCS provisions and their customers will benefit from the Act's privacy protections.

On the other end of the spectrum, cloud providers who expressly rely on content for contextual or targeted advertising will fail to satisfy either of the twin requirements for an RCS. Specifically, by authorizing access to their data for advertising purposes, customers are offering their content for a purpose other than "storage or computer processing" in two ways. First, a cloud provider's marketing program is a means to generate revenue and offer its services profitably. A customer's willingness to make her content available for use in this program is part of a quid pro quo in which the customer receives “free” cloud services in exchange. Sharing one's data with the cloud provider's advertising program to offset any direct costs is thus a secondary purpose and contravenes the Act's requirement that the customer's data be transmitted to the cloud provider “solely for the purpose of providing storage or computer processing.”

Second, the targeted advertising may itself represent a direct service to the customer, despite its parallel financial benefit to the cloud provider. The tremendous revenue generated through online marketing, especially pay-per-click advertising, shows that Internet users rely on advertising to identify and explore offerings that interest them. Consumers appear to value a service that matches advertisements to their specific interests, by considering their stored content and other personal data, and guiding them to relevant products and services among the Internet's seemingly infinite offerings. Ultimately, contextual advertising is problematic under the Act whether it is considered as a cost-offsetting service for the cloud service's customer or as a separate service for exploring a consumer's unique interests. In either scenario, the user's content is being used for a secondary purpose, beyond simply "storage or computer processing," and the Act's privacy protections would not apply.

A more difficult analysis awaits when the cloud provider reserves authority to access a customer's data in its ToS agreement, but offers limited guidance about its exercise of that power. When read in the context of the ToS agreement, many providers appear to be reserving authority to access customers' data to proactively remove harmful or offensive content. A cloud provider is understandably concerned about the potential legal liability or harm to its goodwill that may result when its cloud service is used to store objectionable materials. Such a defensive purpose arguably falls within the Act's exception allowing RCS providers to divulge content to protect its “rights or property.” However, the desire to preventively identify and remove these undesirable materials logically compels the provider's need for a universal license to access all of a customer's data. A more tailored authorization to access only objectionable content would essentially preclude advance screening because it creates circularity: whether specific content would be objectionable could not be known until after it was accessed. However, the difficulty with being authorized to access all of a customer's data is that its exercise depends on the business practices and trustworthiness of the cloud provider. The same provision that allows access to a customer's data to identify harmful material could also justify access for advertising purposes. To understand whether a cloud provider is authorized and intending to access a customer's data for purposes other than “storage or computer processing,” a court would need to delve into each cloud provider's operations and practices.

This uncertainty will likely result in courts refusing to apply the RCS's privacy protections to cloud providers with ambiguous ToS agreements. There are several reasons why this is so. First, courts have no incentive to undertake the
**E. IMPLICATIONS FOR CLOUD COMPUTING USERS**

As this analysis shows, the privacy protections that a cloud user will be entitled to under the Stored Communications Act will ultimately be determined by the cloud provider's terms of service (ToS) agreement and privacy policy. When the ToS agreement allows the cloud provider to rely on the customer's data to provide contextual advertising, the cloud service will not qualify as a remote computing service (RCS). Similarly, when the cloud provider reserves a general right to access a customer's data without specifying the limits of that authority, the cloud service is also unlikely to qualify as an RCS. Only when a cloud provider expressly limits its access to a customer's data for the purposes of providing computer storage or processing functions will the customer benefit from the Act's RCS provisions, including the protection from compelled disclosure by the government and civil litigants.

**V. CAN THIS BE WHAT CONGRESS INTENDED?**

Not every cloud computing service will qualify for the Stored Communications Act's (SCA) privacy protections. Rather than viewing this as a failure of the Act's language to adapt to modern technology, this result is consistent with Congress's desire to limit the scope of the Act's protections. The SCA includes, for example, several prerequisites before a user's content in a remote computing service (RCS) receives the Act's privacy protections. These requirements are a
deliberate attempt by Congress to limit the Act's reach, and when they are not satisfied, as is the case for many cloud providers, the Act's protections are lost.

Many cloud services are not within the Act's coverage for the same reasons that Congress intended some computing services to lie beyond the Act's reach in 1986. The legislative history and language of the Act clarify that Congress had two purposes in adopting the SCA: eliminating privacy concerns that might harm the development of new technology and applying the privacy principles that developed in Fourth Amendment jurisprudence to computer networks. To accomplish these goals, Congress made compromises and adaptations based on the unique characteristics of computer networks. But the Act's final formulation plainly reflects a congressional desire for a narrowly tailored solution that would not apply to every computing service.

A. COMPETITION AND FREE MARKET DETERMINATIONS

Congress recognized early on that privacy considerations might limit the utilization of efficient, outsourced computing services. The Subcommittee on Courts, Civil Liberties, and the Administration of Justice explored these concerns in detail during its consideration of the Stored Communications Act. At one point during the hearings, an exchange occurred between committee members and P. Michael Nugent, who testified for Electronic Data Systems Corporation (EDS) and an industry group of RCS providers. Nugent opened his testimony with an overview of the need for the Act to protect privacy for both the RCS providers and their users:

> We firmly believe, and it is a problem that is going to be growing as we go through the information age, that our customers should not lose their privacy rights and communication when relying on third party providers of data processing and data transmission services. The results of that, of course, are, we may lose business, so that's why we're here.

> [I]f we do not accord or deal with these very basic [privacy] concerns, we may not get the business. Often, the hardware, the software, the technology is as important to the customer as privacy protection; put it the other way, privacy protection is as important as the service that we perform. So, therefore, we believe that our customers shouldn't lose their rights when they go outside for data processing and data transmission services as they must in this day and age.

In a later follow-up question, Representative Boucher reinforced this message with a leading question, asking, “And so the absence of that protection creates a disincentive for individuals to use the new technology; would you agree with that?” After their legislative hearings, both the House and Senate Committees expressed their intent to address RCS clients' privacy concerns in the SCA.

Congress wanted to deal with these privacy issues for two reasons. First, privacy concerns threatened the burgeoning RCS industry. Nugent emphasized this point in his prepared written statement to the House Subcommittee, arguing that the absence of RCS privacy protections may encourage construction of private networks among large companies or force smaller companies to choose between privacy and the competitive advantages offered by the new technology. Second, Congress believed ECS and RCS providers were competing at a disadvantage with other forms of communication, including the postal system and telephone networks. Congress frequently noted that computer networks were analogous...
to telephones and first-class mail, both of which enjoyed significant statutory or constitutional privacy protections. Indeed, the anomalous absence of privacy protections when a computer is used “in lieu of, or side-by-side with” these protected services provided much of the momentum for the Act's introduction. At its core, the Act reflected Congress's concern that the varying privacy protections offered to different mediums for transmitting or processing information might influence market forces in determining the viability of the new technology.

Neither of Congress's concerns about ensuring a level playing field or fostering the growth of new technologies is implicated when applying the Act to cloud computing. Unlike the RCS providers that lobbied for the Act's adoption, cloud providers have access to a statutory scheme that allows them to address customers' privacy concerns. Of course, cloud providers may also choose to adopt a business model that opts out of the Act's protections in exchange for the opportunity to access a customer's data for advertising purposes. Whether users' preference for more privacy will place the opt-out cloud providers at a competitive disadvantage will ultimately be decided by market forces--just as Congress intended. Whatever the result, it will not be the result of inequities in the federal legal regime.

B. CODIFYING THE FOURTH AMENDMENT

After shifting its Fourth Amendment jurisprudence to a “reasonable expectation of privacy” framework in *Katz v. United States*, the Supreme Court decided a series of cases reiterating that the Fourth Amendment does not typically protect the privacy of information that is disclosed to a third party. These decisions caused concern that constitutional privacy protections may be lacking for computer networks and, particularly, remote computing services that were developing rapidly in the 1980s. In *United States v. Miller*, for instance, the Court refused to apply the Fourth Amendment's protections to copies of checks and deposit slips held by the defendant's banks. Similarly, in *Smith v. Maryland*, the Court held that a telephone number dialed from the defendant's home was not within the Fourth Amendment's scope. The Court reasoned in both cases that a person cannot have a reasonable expectation of privacy in information that is disclosed to a third party, such as a bank or telephone company. Computer networks necessarily involve a third-party service provider and the application of the third-party disclosure doctrine adopted in *Miller* and *Smith* suggested that the Fourth Amendment would not protect computer networks. Congress adopted the Stored Communications Act to respond to this perceived constitutional void.

Congress relied extensively on existing Fourth Amendment jurisprudence to draft the Act's electronic communications service (ECS) and remote computing service (RCS) privacy protections. For instance, Congress imposed a bright-line rule eliminating the warrant requirement for unopened communications stored by an ECS provider after 180 days--paralleling the Fourth Amendment concepts of abandonment and relinquishment of privacy interests. In § 2702(b)(8), Congress provided an exception allowing a provider to divulge a customer's data when a “good faith” belief exists that “death or serious physical injury to any person requires disclosure.” This exception closely tracks both the principle and language of the exigent circumstances exception to the Fourth Amendment's warrant requirement. The Court's case law allowing a person to waive her privacy interests by consent is incorporated explicitly in § 2702(b)(3) and § 2703(c)(1)(C). The incorporation of these legal principles shows the extent to which Congress relied upon and codified the existing jurisprudence of the Fourth Amendment.

The unique characteristics of computer networks required Congress to alter the application of some Fourth Amendment principles. Certain of these modifications provide stronger privacy protections than the Fourth Amendment offers in
comparable contexts. One notable area of strengthening occurred through the limitations placed upon the private search doctrine. The Court has long recognized the Fourth Amendment to be a constraint solely upon government actors; this leaves non-governmental actors free to invade the privacy of others on their own accord and share the evidentiary fruits of those invasions with the government. But in § 2702(b)(7), Congress dramatically narrowed the opportunity for voluntary disclosure by computer network providers. Rather than the limitless cooperation allowed by the private search doctrine in the physical world, a computer network provider can only share users' communications and data with the government when it relates to the commission of a crime and is discovered inadvertently.

However, the third-party disclosure doctrine (reaffirmed in Miller and Smith), which initially motivated the Act's adoption, presented Congress with its most difficult problem. Congress needed to determine when the third-party disclosure doctrine should yield, in whole or part, to allow computer network users to enjoy a protected sphere of privacy despite sharing their content with a third-party provider. The resulting legislative solution to this dilemma accounts for much of the Act's complexity.

Congress found a helpful roadmap in the doctrinal approaches to privacy previously applied to the postal service and telephone system. Both communication mediums presented the same underlying conflict between Fourth Amendment principles and evolving societal expectations of privacy; in each case, the Judiciary--and ultimately Congress--decided that privacy should be protected under limited circumstances. Two factors defined the scope of the privacy interest: necessity and expectations. Courts recognized the necessity of using the postal service and telephone system for communication and commerce in modern society and the lack of practical alternatives for people wanting greater privacy. Additionally, courts considered users' expectation that a mailed parcel or telephone conversation would not actually be exposed to a service provider during its transmission. Congress evaluated these same two criteria to guide its adaptation of the third-party disclosure doctrine for electronic communications and remote computing services.

Since Ex Parte Jackson in 1877, the Court recognized a Fourth Amendment right to keep private the content of letters and sealed packages transmitted through the U.S. Postal Service. The Court understood that use of the mail system was no longer a voluntary decision that signaled a user's willingness to share materials with a third-party service provider. Instead, the mail system had become a necessary aspect of modern life for interpersonal communication and commerce. The Court did not, however, provide complete privacy for letters and packages; a right to privacy remained intact only for the internal part of a letter or package that the sender sought to conceal. For example, newspapers and other open mailings exposed to the plain view of postal employees are not entitled to the Fourth Amendment's privacy protections. Similarly, courts held that users expect the postal service to see the writings on the external part of a sealed parcel and there is no reasonable expectation of privacy in the information.

Telephone communications presented a similar privacy dilemma because they are transmitted over the telephone company's infrastructure. When first confronted in 1928 with the issue of privacy in telephone conversations, the Court took a firm stance in Olmstead v. United States and held that the government's wiretap on the defendant's home telephone did not implicate a Fourth Amendment privacy interest. However, the ubiquity of telephone services by the 1960s caused the Court to reconsider its position and in Katz the Court found a valid Fourth Amendment privacy interest in a conversation over a public payphone. The technology had reached a societal tipping point and transitioned from a convenience to a modern-day necessity. Accordingly, the courts modified the Fourth Amendment's scope to accommodate this change. Following the doctrinal path of the earlier mail cases, courts relied...
on a caller's reasonable expectations to define the scope of privacy given to telephone communications. Consequently, courts found a Fourth Amendment privacy interest in the content of a telephone conversation, but declined to extend privacy protections to the telephone number dialed to initiate the conversation.

Congress applied a looser analysis of the necessity and expectation factors in drafting the Stored Communications Act than courts had demanded for mail or telephone communications. When Congress adopted the Act in 1986, electronic communication systems had not become a necessity to the same degree that drove the Judiciary to enlarge privacy protections for mail and telephone services. Similarly, remote computing services were growing in popularity at the time of the Act's adoption, but they were not necessary for businesses to compete effectively or survive. Congress's willingness to construct privacy protections for computer networks—with the expectation that the requisite necessity would develop later—was a departure from the judicial practice of extending safeguards only after a service matured. Rather than anticipating the success of computer networks, Congress's early embrace of the new technology may have become a self-fulfilling prophecy that catalyzed its widespread adoption. Ultimately, Congress's decision to preemptively extend privacy protections to computer networks and outsourced computing services represented a more ambitious approach to privacy than the Court's cautious “wait and see” attitude toward the postal service and telephone calls.

Congress adopted a more cautious approach in aligning the Act's privacy protections with the privacy expectations of computer network users. The Act reflects a tiered compromise, creating a spectrum of privacy protections that apply to different types of information. The strongest protections were reserved for electronic communication services (ECS), such as e-mail, in § 2702(a)(1) and § 2703(a). Because ECS operates similarly to mail and telephone communications—both of which receive the full benefit of the Fourth Amendment under existing constitutional law—Congress reasoned that users would rightfully expect similar treatment for their e-mail communications. To the contrary, personal identification data that a network user voluntarily shares with a service provider receive the weakest protections under § 2702(c) and § 2703(c).

The remote computing service (RCS) functionality of computer networks, however, caused Congress to develop a mid-level tier offering a modest degree of privacy protections. Congress recognized that some user content is transmitted over a computer network to a service provider with the intent to store or process that data, rather than communicate it. Although the service provider's servers hold the user's content, she may not expect that it would be exposed to prying eyes. This unusual arrangement presented Congress with a situation in which analogies to existing precedents in the physical world broke down. Comparisons to sealed letters provided an awkward comparison at best because of the intangible nature of digital information. Prior privacy approaches to facilities that rent storage units also offered limited assistance because customers in those facilities could secure their possessions and deny access to the storage provider. Because the user shared the content with the service provider, the high level of protection given to ECS was unjustified, but in Congress's view some degree of privacy was appropriate. The RCS category was therefore created to provide a limited set of privacy protections when a user has an actual, reasonable expectation that the service provider will not view her stored content.

Despite Congress's liberalization of privacy protections in the SCA, many cloud providers rely on a business model that will run astray of the limitations in the Act. Congress did not express an unlimited tolerance for interaction between RCS providers and their customers; rather, Congress sought to preserve at least a modicum of privacy when users expect to maintain it. For instance, Congress specifically recognized that users' privacy expectations remained intact when RCS providers stored or processed users' data without peering into its contents, But terms of service agreements empowering a cloud provider with far-reaching authority to access stored content, for marketing or other purposes,
eliminate the user's expectation of privacy that Congress considered critical. Thus, excluding many cloud computing services from the protections of the SCA is entirely consistent with Congress's intent to limit the Act's scope.

VI. WILL CLOUD COMPUTING BE A TIPPING POINT FOR ONLINE PRIVACY?

As most Americans move their personal content into the cloud, a corresponding increase in privacy protections seems appropriate. There are, however, significant obstacles to expanding privacy rights for cloud computing that widespread adoption alone cannot overcome. These judicial, legislative, and societal impediments make it unlikely that an enlargement of the Stored Communications Act or the protective scope of the Fourth Amendment will necessarily follow.

A. JUDICIAL OBSTACLES

The trajectory of Fourth Amendment jurisprudence suggests that courts are unlikely to enhance privacy protections for cloud computing users. Courts only rarely serve as the initial impetus for expanding privacy protections; when they do, it is typically through cautious extension of the Fourth Amendment, in response to societal or technological changes. Yet, since the 1960s, the Supreme Court has applied an even narrower view of the Fourth Amendment's protections and the applicability of its remedies. The Court has focused its recent Fourth Amendment efforts on reexamining the costs and benefits of excluding evidence gathered in violation of the Fourth Amendment and limiting the range of situations that invoke the Fourth Amendment's protections. Given the current state of its Fourth Amendment jurisprudence, it seems unlikely that the Court will drastically expand the scope of privacy protections for Internet users--after failing to accept an Internet-related privacy case for more than two decades. Not only would this significantly change the dimensions of the Fourth Amendment's scope, it would likely require reassessing core privacy principles, such as the third-party disclosure doctrine, that would have repercussions beyond the digital world.

Without meaningful guidance from the Supreme Court, lower courts are in disarray with respect to privacy interests in computer networks. Federal courts cannot reach consensus on the privacy protections applicable to e-mail; for instance, a circuit split currently exists over the categorization of e-mail within the Stored Communications Act. Courts have also struggled to determine if the Fourth Amendment protects e-mail. In Warshak v. United States, the Sixth Circuit held that the Fourth Amendment protected a person's e-mail from government searches and seizures, only to retract the opinion a short time later in an en banc decision that avoided the issue. In United States v. Maxwell, an earlier case heard by the Court of Appeals for the Armed Forces, the Fourth Amendment was also held to apply to e-mail, but other courts have discounted its precedential value. These cases reflect the degree of uncertainty among lower courts about how the SCA and Fourth Amendment apply to e-mail--making it unlikely that they can proceed anytime soon to the thornier issues surrounding communications and stored data in cloud services.

Judicial modification of online privacy protections is further complicated by the Act's existence. Despite the eloquence of the two-prong test developed in Katz v. United States, "the phrase 'reasonable expectation of privacy' is essentially a legal fiction that masks a normative inquiry into whether a particular law enforcement technique should be regulated by the Fourth Amendment." The SCA, however, reflects Congress's own normative judgment about the appropriate degree to which a person's privacy interests should be protected in an online environment. The lack of a contrary societal or judicial consensus with respect to online privacy issues further suggests that Congress's solution might be the best of the imperfect options available. At the very least, there is nothing to suggest that Congress's view departs from
societal norms so spectacularly that it contradicts constitutional privacy principles. Consequently, there is little basis upon which the Court might render the SCA unconstitutional--either directly or implicitly--and be tempted to substitute Congress's balancing act with its own normative inquiry under the guise of Fourth Amendment jurisprudence.

B. LEGISLATIVE OBSTACLES

Congress has expanded privacy protections several times when the use of a new technology was not addressed by the courts or was held to be unprotected. Indeed, some of Congress's broadest expansions of privacy protections have followed the Court's unwillingness to do so. After Olmstead v. United States, in which the Court held that the Fourth Amendment did not apply to telephone communications, Congress responded by proscribing wiretapping in the Communications Act of 1934. Similarly, Congress adopted the Pen Register Act to respond to Smith v. Maryland, which held that the Fourth Amendment did not extend to telephone numbers processed by a telephone company's automated routers. In other instances, such as the provisions covering remote computing services in the Stored Communications Act, Congress has injected new privacy protections before the courts have had an opportunity to consider them.

Although Congress has historically favored the enlargement of privacy protections, it is unlikely to lead the fight to expand online privacy. Congressional inertia can be overcome when the right combination of variables intersect, including political momentum and societal demand. Two main obstacles currently prevent these variables from aligning for online privacy issues. First, the SCA itself impedes the adoption of new privacy measures by shrinking the gap between the existing and ideal degree of privacy protections that Congress might want. Second, recent congressional actions are reducing the sphere of individual privacy, especially after the September 11, 2001 terrorist attacks, rather than seeking its expansion.

The SCA limits the political value of tackling online privacy issues and, therefore, obstructs efforts to adopt stronger protections. Congress has a limited capacity to pursue new legislation and it is hard to get its finite attention focused on a particular issue. Consequently, seeking incremental change in a previously legislated subject area is particularly difficult. The SCA already provides some quantum of privacy in online communications and content, but as society embraces new technologies, including cloud computing, the balance that the Act struck more than two decades ago may no longer be appropriate. But aligning the SCA's provisions with current mainstream views about online privacy would not require dramatic changes that would generate substantial public attention. Instead, such an effort would likely involve making incremental enhancements to the Act's structure, clarifying issues of judicial dispute, or modernizing statutory language. Because of the limited political return such modest changes would offer, politicians have few incentives to advocate for them.

The SCA also influences societal expectations about online privacy and thus minimizes the political pressure for change. Societal forces can cause both Congress and the courts to revisit privacy protections. Within the judicial realm, the Court held in Katz v. United States that privacy issues under the Fourth Amendment focus on whether society is prepared to recognize an expectation of privacy under certain circumstances as being reasonable. This approach makes it difficult for privacy advocates to advance their interests because of the circularity in using societal expectations to define new legal protections for individual privacy when those expectations are influenced by existing legal protections. In the same circular manner, the SCA's privacy standards subtly influence societal norms when they are reflected in media reports, judicial decisions, and terms of service agreements. In the legislative realm, the lack of a significant
disparity between societal privacy expectations and the SCA's existing protections minimizes the political pressure to bring about change. Political action is motivated when constituencies expand and engage their members to generate enough momentum to attract attention. 246 Yet, privacy issues attract a limited natural constituency and building a large coalition of interested online users to generate political change is difficult 247 --particularly when the SCA's existing statutory scheme continues to define and reinforce societal norms about online privacy.

Even if there is societal demand for greater online privacy protections, elected officials and judges need to recognize that a shift in expectations has happened. However, the demographics of Congress and the Judiciary make it unlikely that their members are well-positioned to determine society's expectations, especially about emerging technologies. Younger people are much more likely to embrace cloud computing services, 248 but the average age of senators 249 and House members 250 --as well as the Justices 251 on the Court--reflects a notable generational gap from this core user population. Advocates for enhanced online privacy measures will have to bridge this divide and ensure that elected officials and judges understand the technology and its implications for individual privacy before they can secure their assistance in changing the status quo.

C. SOCIETAL OBSTACLES

A final obstacle to strengthening online privacy protections is the changing societal attitude toward online privacy. 252 Younger generations have much less concern about online privacy than older generations. 253 This divergence is partially attributable to the different ways that each generation uses the Internet. Older users generally rely on the Internet for transactional encounters, such as gathering information from websites, exchanging direct communications via e-mail, managing personal finances, and purchasing goods. 254 In contrast, younger users are more likely to embrace the Internet's interconnectedness and convenience by participating in social networking, sharing digital content, and using cloud services. 255

The generational differences in Internet usage are shifting societal calculations about the value of online privacy. Privacy involves a tradeoff with other competing values, such as cost, convenience, efficiency, and networking. 256 The widespread use of cloud computing services by younger generations is driven extensively by these latter values. Popular social networking sites, such as Facebook and MySpace, necessarily involve the public (or semi-public) sharing of personal information and content with a network of other users. 257 In contrast, old users are more likely to embrace the Internet's interconnectedness and convenience by participating in social networking, sharing digital content, and using cloud services. 255

Expecting to receive something for “free” from cloud providers is also reducing users' privacy expectations. 260 One sign of this change is users' growing comfort, especially among younger users, with cloud providers analyzing the content of websites they visit in order to deliver targeted advertising. 261 From a market-based perspective, the frequency with which Internet users of all ages are willing to expose their online activities or exchange their personal data for free services and content suggests that they assign a low market value to their privacy. Additionally, if people truly want greater privacy protections, one would expect cloud providers to compete to offer consumers better protections; instead, new users continue streaming toward Google and other cloud providers to partake in their advertising-sponsored offerings. 262
The generational gap in privacy expectations and embrace of free services from cloud providers suggest little opportunity to generate societal momentum for greater online privacy protections. Younger generations are less concerned with personal privacy than older generations and are likely to carry those views forward as they gradually assume society's reins in the future. The expanding business model of exchanging privacy for free access to cloud providers' offerings will also continue to reduce the perceived market price of individual privacy. Thus, the likelihood for building a societal consensus about the need for heightened online privacy protections is gradually slipping away.

**1239 CONCLUSION**

The business model embraced by many cloud computing providers is incompatible with the requirements of the Stored Communications Act. A provider's authorization to access a customer's data, for the provision of contextual advertising or other purposes, will likely disqualify that customer from receiving the Act's privacy protections. As a result, courts will need to carefully scrutinize a cloud provider's terms of service agreement and privacy policy to determine the degree to which it is authorized to access customers' data. A brief analysis of the agreements currently used by Google and several other cloud providers confirms that many users will ultimately discover they are outside the boundaries of the SCA and their data is vulnerable to disclosure. 263 Although unsettling, this result is consistent with Congress's doctrinal approach in drafting the Act to limit its protections to certain contexts. Yet, despite the growing popularity of cloud computing services, there appears to be little opportunity for judicial or legislative relief in the near future. Professor Kerr notes that “there are many problems of Internet privacy that the SCA does not address.” 264 It appears that cloud computing is one of them.

Footnotes


See CERUZZI, supra note 6, at 269-76.


See CERUZZI, supra note 6, at 291-95.


See Jeffrey A. Tannenbaum, Speed, Cost and Cachet Aid Growth of Electronic Mail, WALL ST. J., July 27, 1988, at 29 (“In May 1987, for example, Compuserve dropped its hourly rate for certain fast-transmission users to $12.50, from $19.50 evenings and $22.50 during the day.”).

See JANET ABBATE, INVENTING THE INTERNET 203 (1999); Peter H. Lewis, A Boom for On-Line Services, N.Y. TIMES, July 12, 1994, at D1.

See generally Joseph L. Bower & Clayton M. Christensen, Disruptive Technologies: Catching the Wave, HARV. BUS. REV., Jan.-Feb. 1995, at 43 (exploring how disruptive technologies can unexpectedly achieve widespread adoption and alter existing markets).

See CARR, supra note 8, at 17; CERUZZI, supra note 6, at 295-304.

See ABBATE, supra note 14, at 217; CARR, supra note 8, at 17.


See Tom Wright, Poorer Nations Go Online on Cellphones, WALL ST. J., Dec. 5, 2008, at B4. Mobile Internet access also has the potential to extend service into areas where fixed-line infrastructure is lacking or prohibitively expensive. Id.

See MILLER, supra note 7, at 13-15.

See, e.g., Rearden LLC v. Rearden Commerce, 597 F. Supp. 2d 1006, 1021 (N.D. Cal. 2009) (finding that cloud computing is “a term used to describe a software-as-a-service (SAAS) platform for the online delivery of products and services”); FTC Complaint of Electronic Privacy Information Center at 4, In re Google, Inc. & Cloud Computing Servs. (Mar. 17, 2009) (“Cloud Computing Services are an emerging network architecture by which data and applications reside on third party servers, managed by private firms, that provide remote access through web-based devices.”), available at http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf; ROBERT GELLMAN, WORLD PRIVACY FORUM, PRIVACY IN THE CLOUDS: RISKS TO PRIVACY AND CONFIDENTIALITY FROM CLOUD COMPUTING 4 (2009) (“[C]loud computing involves the sharing or storage by users of their own information on remote servers owned or operated by others and accessed through the Internet or other connections.”) (emphasis omitted); Posting of Bob Boorstin to Google Public Policy Blog, What policymakers should know about “cloud computing,” http://googlepublicpolicy.blogspot.com/2009/03/what-policymakersshould-know-about.html (Mar. 20, 2009, 10:35 EST) (defining cloud computing as “the movement of computer applications and data storage from the desktop to remote servers”).
For some large organizations, the development of a private cloud may be a cost-effective means of serving the entity's computing needs. See MICHAEL ARMBRUST ET AL., UNIV. OF CAL. AT BERKELEY, ABOVE THE CLOUDS: A BERKELEY VIEW OF CLOUD COMPUTING 1 (2009) (differentiating between public and private cloud computing). However, for purposes of this Note, the analysis will focus on public clouds intended to serve third parties.

See CARR, supra note 8, at 17 (“Instead of relying on data and software that reside inside our computers, inscribed on our private hard drives, we increasingly tap into data and software that stream through the public Internet.”).


ARMBRUST ET AL., supra note 23, at 3 (noting the industry-wide disagreement about the exact meaning of “cloud computing”); Cloud Computing: Clash of the Clouds, ECONOMIST, Oct. 17, 2009, at 80, 80-82 (same). In October 2009, the National Institute of Standards and Technology (NIST) released another proposed definition of cloud computing--its fifteenth draft of the proposal--providing, in part, that: “Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” PETER MELL & TIM GRANCE, NAT'L INST. OF STANDARDS AND TECH., THE NIST DEFINITION OF CLOUD COMPUTING (15th version 2009).

See Cloud Computing: Clash of the Clouds, supra note 26, at 80-82 (noting that Apple, Google, and Microsoft are “preparing for battle” over cloud computing).

See CARR, supra note 8, at 55-56 (noting studies of corporate data centers showing that only 25%-50% of storage capacity and less than 25% of processing power are being used); Nicholas G. Carr, The End of Corporate Computing, MIT SLOAN MGMT. REV., Spring 2005, at 67, 70 (estimating CPU processing power utilization rates of 5% for desktop computers and 10%-35% for corporate servers).

See CARR, supra note 8, at 57-58 (discussing the large inefficiencies involved in having corporations develop and maintain their own technology infrastructure and personnel).

See PRABHAKAR CHAGANTI, CLOUD COMPUTING WITH AMAZON WEB SERVICES, PART 1: INTRODUCTION 3 (2008), http:// download.boulder.ibm.com/ibmdl/pub/software/dw/architecture/ar-cloudawsl/ar-cloudawsl-pdf.pdf (“According to Amazon's estimates, businesses spend about 70 percent of their time on building and maintaining their infrastructures while using only 30 percent of their precious time actually working on the ideas that power their businesses.”).

See, e.g., Virginia Heffernan, The Great Crash, N.Y. TIMES MAG., June 14, 2009, at 24 (recounting the author's painful loss of her diary, photos, music, e-mail, address book, and documents following the failure of her laptop's hard drive).

See MILLER, supra note 7, at 26.

See Harry McCracken, Online Storage: The Next Generation, PC WORLD, Oct. 2000, at 45 (reviewing several of the earliest online storage providers and noting their sluggish performance when transmitting files).


See, e.g., id. at 32-34.

By December 2007, more than 121 million homes and businesses subscribed to high-speed Internet connections and the number of subscribers grew at an annual rate of 46%. INDUS. ANALYSIS & TECH. DIV., FED. COMM'CNS COMM'N, HIGH-SPEED SERVICES FOR INTERNET ACCESS: STATUS AS OF DECEMBER 31, 2007, at 1 (2009), available at http://
hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-287962Al.pdf; see also HORIZGAN, supra note 20, at 9-11 (indicating that an April 2009 survey found that “63% of adult Americans have broadband internet connections at home”).

See CARR, supra note 8, at 64-68 (discussing Google's proprietary development of many of these technological advances); MILLER, supra note 7, at 12-13.


See David H. Freedman, Upgrade Madness, INC. MAG., Feb. 2006, at 65, 66 (“Upgrades are an enormous source of revenue for the software industry, and most vendors aren't above engaging in some form of stick-waving with customers who won't jump for the carrot. The big stick in this regard is the threat to retire older versions--declare them officially obsolete and withdraw support.”).

Id. at 65-66.

See MILLER, supra note 7, at 27.

Id. at 14-15.

Id. at 75, 148-50.

See Cloud Computing: Clash of the Clouds, supra note 26, at 80 (noting that cloud computing renders personal computing devices and their operating systems less important).

The minimal processing and storage needs of a device needed primarily to access cloud applications is driving the growth of a new generation of less powerful and cheaper computers, commonly referred to as “netbooks.” See Randall Stross, The PC Doesn't Have To Be an Anchor, N.Y. TIMES, Apr. 19, 2009, at BU-4; Clive Thompson, The Netbook Effect, WIRED, Mar. 2009, at 60, 62.

See Freedman, supra note 39, at 66.

See CERUZZI, supra note 6, at 318-19. Webmail has also given courts their first exposure to the cloud computing environment. See, e.g., United States v. Bach, 310 F.3d 1063 (8th Cir. 2002) (examining the Fourth Amendment issues relating to the seizure of e-mail from a Yahoo! webmail account).

See MILLER, supra note 7, at 40-41.

See id. at 52.

See JOHN B. HORRIOAN, PEW INTERNET & AM. LIFE PROJECT, USE OF CLOUD COMPUTING APPLICATIONS AND SERVICES I (2008) (finding that 56% of Internet users now use a webmail service).


55 Professor Zittrain attributes much of the success of personal computers and the Internet to their role as “generative technologies” that allowed experimentation and innovation by third parties. See Zittrain, supra note 12, at 1980-94, 2039-40. In a more recent example of this phenomenon, Apple opened the iPhone to third-party software developers, and users downloaded more than three billion applications from its App Store within eighteen months. Press Release, Apple Inc., Apple's App Store Downloads Top Three Billion (Jan. 5, 2010), available at http://www.apple.com/pr/library/2010/01/05 appstore.html. Apple's competitors are now scrambling to open up their own platforms. See Jenna Wortham, Apps Boom as Companies Seek a Place on Your Phone, N.Y. TIMES, June 8, 2009, at B4 (noting that “Apple showed that new apps sell phones” and others are seeking to replicate its App Store model).

56 See CARR, supra note 8, at 85-103 (analogizing cloud computing to the decentralization of electricity production and the growth of modern utilities at the turn of the century); MILLER, supra note 7, at 41-42.


58 See Michael Fitzgerald, Cloud Computing: So You Don't Have To Stand Still, N.Y. TIMES, May 25, 2008, at BU-4 (discussing the benefits of using Amazon Web Services for a small Internet-based business that unexpectedly generated more than 750,000 customers in three days).

59 See, e.g., Amazon: Lifting the Bonnet, ECONOMIST, Oct. 7, 2006, at 91 (“In order to cope with the Christmas rush, Amazon has far more computing capacity than it needs for most of the year. As much as 90% of it is idle at times. Renting out pieces of that network to other businesses, such as SmugMug, an online photo site that uses the S3 service, is a way to get extra return on Amazon's $2 billion investment in technology”).


64 See infra Parts III-IV for an application of the Act's ECS and RCS categories to cloud computing services.


66 See S. REP. NO. 99-541, at 8; Tannenbaum, supra note 13, at 29 (noting that an e-mail user in 1988 paid forty cents per message, which typically reached its recipient within twenty minutes). The OTA report noted there were at least five stages in the transmission and storage of an e-mail. OTA REPORT, supra note 61, at 48-50.

67 See S. REP. NO. 99-541, at 8; OTA Report, supra note 61, at 45.
68 H.R. REP. NO. 99-647, at 22 & n.34.
70 Id. § 2510(15).
71 Id. § 2510(13).
72 Id. § 2510(17).
73 See Kerr, supra note 2, 1213-14; see also supra notes 65-68 and accompanying text.
75 Electronic Communications Privacy Act: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties and the Admin, of Justice of the H. Comm. on the Judiciary, 99th Cong. 84--85, 89 (1986) thereafter ECPA Hearings) (statement of Michael P. Nugent, Chairman, Comm. on Computer Systems and Communications Privacy, ADAPSO); see also CARR, supra note 8, at 52 (noting that “a typical IBM mainframe was about $30,000 a month in the mid-1960s”); Patricia L. Bellia, The Memory Gap in Surveillance Law, 75 U. CHI. L. REV. 137, 142-44 (2008) (discussing the decline in storage pricing over the past five decades).
76 S. REP. NO. 99-541, at 10-11.
77 Id.
78 Id. at 10. Not until 1990--more than four years after the SCA's adoption--did the first provider begin offering Internet access to consumers. Deirdre K. Mulligan, Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act, 72 GEO. WASH. L. REV. 1557, 1572 (2004).
80 Id. §§ 2510(14), 2711(2).
81 Id. §§ 2702(a)(2)(A), 2703(b)(2)(A).
82 Id. §§ 2702(a)(2)(B), 2703(b)(2)(B).
83 Id.
84 See Kerr, supra note 2, at 1213-14; see also supra notes 74-78 and accompanying text.
86 The protections offer surprisingly little recourse for criminal defendants because of the lack of a suppression remedy for evidence gathered in violation of the Stored Communications Act's (SCA) requirements. See United States v. Meriwether, 917 F.2d 955, 960 (6th Cir. 1990) (holding that Congres's did not provide a suppression remedy for evidence gathered in violation of the SCA). Some observers have suggested that the lack of a meaningful incentive for criminal defendants to challenge detrimental court decisions explains the seemingly modest amount of case law surrounding the SCA's application. See Orin S. Kerr, Lifting the “Fog” of Internet Surveillance: How A Suppression Remedy Would Change Computer Crime Law, 54 HASTINGS L.J. 805, 841 (2003) (arguing for the creation of a suppression remedy to further doctrinal development of the SCA).
88 Id. § 2703(a).
89 Id. § 2703(b).
89 18 U.S.C. § 2702(b).

90 18 U.S.C. § 2703(d). The Act also requires that the government provide the customer with notice of the compelled disclosure, but notification may be delayed with a court's permission. Id. § 2705 (2000 & Supp. I 2009).

91 18 U.S.C. § 2702(c)(6).

92 Id. § 2703(c)(2)(A).

93 See, e.g., Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256, 264 (S.D.N.Y. 2008); In re Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606, 611-12 (E.D. Va. 2008); O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 89 (Ct. App. 2006); see also H.R. REP. NO. 99-647, at 89 (1986) (discussing the burdens placed on RCS providers to comply with disclosure requests from civil litigants). However, nothing in the SCA precludes courts from ordering litigants to divulge their own content, held by a cloud provider, under the consent exception. See 18 U.S.C. § 2702(b)(3) (noting that a provider may disclose content information with the “consent of ... the subscriber ... of [a] remote computing service”); Flagg v. City of Detroit, 252 F.R.D. 346, 366 (E.D. Mich. 2008).


97 An important distinction should be noted between sharing and communicating data. Some cloud computing services allow data to be shared with other users, but no actual electronic communication of the data occurs. For instance, a word processing application may allow the customer to provide other users with access to the document. However, the data itself never leaves the service provider's cloud and, thus, the required “send or receive” functionality is lacking.


99 Id. § 2510(17); see supra section II.A.

100 See, e.g., Gmail Help: Archiving Mail, http://mail.google.com/support/bin/answer.py?hl=en&answer=6576 (last visited Feb. 12, 2010) (noting that Gmail's archive function “moves messages out of your inbox ... letting you tidy up your inbox without deleting anything”).


102 For instance, the Google Docs service offers multiple applications for creating and editing documents, presentations, and spreadsheets while allowing access to that stored data from any Internet-connected computer or mobile device. See Google Docs Tour, http://www.google.com/google-ds/tourl.html (last visited Jan. 3, 2010).

103 But see infra notes 107-11 and accompanying text (discussing the alternate approach used in the Ninth Circuit and some district courts in the Sixth Circuit).


105 Kerr, supra note 2, at 1215.
See Quon v. Arch Wireless Operating Co., 529 F.3d 892, 902 (9th Cir. 2008), rehe'g en banc denied, 554 F.3d 1066, 1075-76 (9th Cir. 2004) (refusing to distinguish between intermediate and post-transmission e-mail storage in defining ECS).

Quon involved the privacy of text messages sent by a City of Ontario police officer using an employer-issued text-messaging pager. Id. at 895. The City contacted Arch Wireless, its service provider for the pagers, and asked for copies of the text messages sent by Sergeant Quon after he exceeded his monthly allocation several times. Id. at 897-98. The transcripts revealed inappropriate personal messages, allegedly in violation of the City's policy, and resulted in an Internal Affairs investigation. Id. at 898. The Ninth Circuit held that Arch Wireless was an ECS and, by releasing his messages to the City, it violated Sergeant Quon's rights under the SCA. Id. at 903. The court further held that the search of the archived text messages violated Quon's Fourth Amendment rights. Id. at 910. The Supreme Court recently granted certiorari in Quon, but it does not appear that the SCA-related issues will be considered. City of Ontario v. Quon, 78 U.S.L.W. 3359 (U.S. Dec. 14, 2009) (No. 08-1332). Instead, the Court will only consider the issues surrounding the Fourth Amendment privacy rights of government employees in the workplace. See Petition for a Writ of Certiorari at i, City of Ontario v. Quon, No. 08-1332, 2009 WL 1155423 (Apr. 27, 2009).


See, e.g., Kerr, supra note 2, at 121 ( remarking that “the Ninth Circuit's analysis in Theofel is quite implausible and hard to square with the statutory text”); Marc J. Zwillinger & Christian S. Genetski, Criminal Discovery of Internet Communications Under the Stored Communications Act: It’s Not A Level Playing Field, 97 J. CRIM. L. & CRIMINOLOGY 569, 580 (2007) (noting that “the Theofel court's analysis is somewhat tortured”).}

See Zwillinger & Genetski, supra note 110, at 581; see also SEARCHING AND SEIZING COMPUTERS, supra note 104, at 123 (“Unfortunately ... there is now a split between two interpretations of ‘electronic storage’--a traditional narrow interpretation and an expansive interpretation supplied by the Ninth Circuit .... As a practical matter, federal law enforcement within the Ninth Circuit is bound by the Ninth Circuit's decision in Theofel, but law enforcement elsewhere may continue to apply the traditional interpretation of ‘electronic storage.’”).

See supra section II.B.

See Bellia, supra note 75, at 145.


See H.R. REP. NO. 99-647, at 65 (1986) (noting that opened electronic mail stored on the provider's server may fall within the RCS provisions).

See, e.g., Kerr, supra note 2, at 1216 (citing COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEPT OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS § III.B (2002)).
119 Id. § 2702(a)(2)(B).
120 Id. (emphasis added).
121 See Chris Anderson, Free! Why $0.00 is the Future of Business, WIRED, Mar. 2008, at 140; see also The End of the Free Lunch--Again, ECONOMIST, Mar. 21, 2009, at 16 (noting the widespread use of the advertising-based business model among web service providers and its limitations).
122 See Rescueom Corp. v. Google Inc., 562 F.3d 123, 125-26 (2d Cir. 2009) (discussing the operation of the Google AdWords contextual advertising system).
124 See, e.g., Jonathan Lemonnier, Contextual TargetingBoosts Loyal Following, ADVERTISING AGE, Apr. 14, 2008, at 7 (discussing a contextual advertising case study showing a 19% increase in brand recall versus non-targeted advertising); Yahoo! Customized Advertising FAQ, http://info.yahoo.com/relevantads/faq/ (last visited Feb. 12, 2010) (“Customization features are designed to bring you the news, weather, or other content you want, and to help you find what you are looking for more efficiently. We apply this principle to advertising, believing that relevant ads will be more useful.”).
125 See infra section IV.B. These website contractual agreements also use other titles, including “terms of use” and “statement of rights and responsibilities.” This Note uses “terms of service” in reference to all such agreements.
126 See, e.g., Evernote Terms of Service § 10 (July 9, 2009), http://www.evernote.com/about/tos/(noting the existence of a quid pro quo by requiring users to “agree that Evernote may present advertising in connection with the Service in consideration for the rights granted you to access and use the Service”); Google Terms of Service § 17.1 (Apr. 16, 2007), http://www.google.com/accounts/TOS (“Some of the Services are supported by advertising revenue and may display advertisements and promotions. These advertisements may be targeted to the content of information stored on the Services, queries made through the Services or other information.”).
128 See Suhong Li & Chen Zhang, An Analysis of Online Privacy Policies of Fortune 100 Companies, in ONLINE CONSUMER PROTECTION: THEORIES OF HUMAN RELATIVISM 269, 277 (Kuanchin Chen & Adam Fadlalla eds., 2009) (finding that 94% of Fortune 100 companies have posted an online privacy policy).
129 See, e.g., United States v. Drew, 259 F.R.D. 449, 462 & n.22 (CD. Cal. 2009) (surveying cases in which courts enforced website agreements); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 248 (S.D.N.Y. 2000) (holding that a website user assented to the terms of service by using the provider's service). But see Jason Isaac Miller, Note, “Don't Be Evil”: Gmail's Relevant Text Advertisements Violate Google's Own Motto and Your E-Mail Privacy Rights, 33 HOFSTRA L. REV. 1607, 1632-35 (2005) (arguing that website visitors should not be bound to the Terms of Use agreement for Google's Gmail service because it “provides a flawed registration process that robs prospective users of the opportunity to give informed consent and manifest their agreement”).
131 Google Terms of Service, supra note 126, § 8.3.
Google Privacy Center: Advertising and Privacy, supra note 130.

Google Terms of Service, supra note 126, § 11.1.

Id. § 11.2 (“You agree that this license includes a right for Google to make such Content available to other companies, organizations or individuals with whom Google has relationships for the provision of syndicated services, and to use such Content in connection with the provision of those services.”).


Google AdSense Online Standard Terms and Conditions § 16 (Feb. 25, 2008), http://www.google.com/adsense/terms (“You grant Google the right to access, index and cache the Property(ies), or any portion thereof, including by automated means including Web spiders or crawlers.”); see also Bradley v. Google, Inc., No. C 06-05289(WHA), 2006 WL 3798134, at *1 (N.D. Cal. Dec. 22, 2006) (finding that Google AdSense “ads were tailored to the host website's content”).


Evernote Terms of Service, supra note 126, § 10.

Id.


See Amazon Web Services Terms of Use (Sept. 22, 2008), http://aws.amazon.com/terms/(“AWS has the right but not the obligation to monitor and edit or remove any activity or content.”); YouTube Terms of Service § 6.C, http://www.youtube.com/t/terms (last visited Dec. 21, 2009) (“[B]y submitting User Submissions to YouTube, you hereby grant YouTube a worldwide, non-exclusive, royalty-free, sublicenseable and transferable license to use, reproduce, distribute, prepare derivative works of, display, and perform the User Submissions in connection with the YouTube Website ....”).

Yahoo! Terms of Service § 6 (Nov. 24, 2008), http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html (“You acknowledge that ... Yahoo! and its designees shall have the right (but not the obligation) in their sole discretion to pre-screen, refuse, or remove any Content that is available via the Yahoo! Services.”).


Remember the Milk Terms of Use § 5, http://www.rememberthemilk.com/help/terms.rtm (last visited Dec. 21, 2009) (“We will not use any of your content for any purpose except to provide you with the Service.”).


See, e.g., Zoho Terms of Service (Sept. 7, 2009), http://www.zoho.com/terms.html (“We respect your right to ownership of content created or stored by you. You own the content created or stored by you. Unless specifically permitted by you, your use of the Services does not grant Zoho the license to use, reproduce, adapt, modify, publish or distribute the content created by you or stored in your Account for Zoho's commercial, marketing or any similar purpose.”).

See Patricia L. Bellia, Surveillance Law Through Cyberlaw's Lens, 72 GEO. WASH. L. REV. 1375, 1436 (2004)(“[T]he concept of a remote computing service is outdated.”).
Specifically, the court held that retrieving the text messages and sharing them with the customer might be viewed as “necessarily incident to the rendition of the [storage] service” and, thus, disclosure would be permissible under the exception available in § 2702(b)(5). *Id.* at 359 (quoting 18 U.S.C. § 2702(b)(5)). Additionally, the court held that the particular facts of the case would support disclosure, under § 2702(b)(3), based on the consent of the customer or sender. *Id.* at 359-66.

By one estimate, $21-$25 billion in advertising is already sold annually to support “free” online services to consumers. See ANDERSON, supra note 127, at 165.


*See, e.g.*, Press Release, TRUSTe, Behavioral Targeting: Not That Bad?! TRUSTe Survey Shows Decline in Concern for Behavioral Targeting (Mar. 4, 2009), available at http://www.truste.com/about_TRUSTe/press-room/news_truste_behavioral_targeting_survey.html (“[Seventy-two] percent of those surveyed said they found online advertising intrusive and annoying when the products and services being advertised were not relevant to their wants and needs.”); Hapax-NLP Targeting Technology, http://www.hapax.com/amplify.cfm (last visited Feb. 12, 2010) (“‘If it's hyper-targeted, it doesn't feel like advertising anymore-- it feels like a service.’” (quoting Chris Anderson, Editor-in-Chief of Wired Magazine)); see also supra note 124.


*See* Yahoo! Inc. v. La Ligue Contre Le Racisme Et L’Antisemitisme, 433 F.3d 1199 (9th Cir. 2006).

18 U.S.C. § 2702(b)(5) (2006). Arguably, the mere authorization to access content to screen for objectionable material is not within the requirement that an RCS provider only provide “storage and computer processing” functions. However, this argument requires a narrow reading of these two authorized purposes, and at least one court has rejected such an interpretation. See Lukowski v. County of Seneca, No. 08-CV-6098, 2009 WL 467075, at *11-12 (W.D.N.Y. Feb. 24, 2009).

Courts are generally unwilling to engage in speculation about future applications of existing practices or policies by a party to the litigation. See, e.g., City of L.A. v. Lyons, 461 U.S. 95, 109-10 (1983) (refusing to speculate about a police department's future application of a chokehold policy).

However, irrespective of these agreements, webmail may receive the heightened ECS privacy protections in the Ninth Circuit and some districts within the Sixth Circuit because of those jurisdictions' controversial views about the classification of opened webmail. See supra notes 107-11 and accompanying text.

See supra section II.C.


See, e.g., Warshak v. United States, 490 F.3d 455 (6th Cir. 2007), vacated, 532 F.3d 521 (6th Cir. 2008) (en banc) (vacating an earlier opinion holding that a Fourth Amendment privacy right exists in stored e-mail); United States v. Rodriguez, 532 F. Supp. 2d 332, 339-40 (D.P.R. 2007) (holding that there is no expectation of privacy in Internet transmissions or e-mail that has arrived at its recipient); United States v. Charbonneau, 979 F. Supp. 1177, 1184-85 (S.D. Ohio 1997) (holding that there is no expectation of privacy after an e-mail is received by its intended recipient, distributed widely, or sent to an undercover agent). The Government has argued that even if a Fourth Amendment privacy right does exist, the terms of service agreements used by many service providers would still authorize the disclosure of a customer's e-mail to law enforcement. See Final Reply Brief for Defendant-Appellant United States of America at 13-14, 18-19, Warshak, 490 F.3d 455, vacated, 532 F.3d 521 (No. 06-4092), 2007 WL 2085416.

See infra section VI.A.

See supra section IV.B.


See supra notes 93-95 and accompanying text.

See ECPA Hearings, supra note 75.

EDS, until being acquired in May 2008 by Hewlett-Packard, remained among the largest cloud computing providers, primarily serving large business and institutional users, with over one million cloud applications hosted on its infrastructure. See EDS Application Servs., Transform and Modernize Your Applications 7 (Dec. 2008), http://h10134.www1.hp.com/services/apps/downloads/apps_services_overview.pdf.

ECPA Hearings, supra note 75, at 76.

Id. at 90.

See H.R. REP. NO. 99-647, at 19 (1986) (commenting that the questionable privacy protections available to users of computer networks “may unnecessarily discourage potential customers [from] using such systems”); id. at 65-66 (“This provision reflects the rapidly growing importance of information storage and processing to the Nation's commerce. Today, the subject matter of commerce increasingly is information in electronic form and the processing of information itself has become a major industry. The secure storage of electronic information has thus become as important to the commercial system as the protection of paper records.”); S. REP. NO. 99-541, at 5 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3559 (noting that the uncertain privacy protections “may unnecessarily discourage potential customers from using innovative communications systems” or “discourage American businesses from developing new ... forms of telecommunications and computer technology”).
See ECPA Hearings, supra note 75, at 81 (“[O]nly those companies who were large enough and financially able to afford to maintain and operate their own private networks would be able to protect their privacy interests, and there would be a definite disincentive to the use of commercial systems, which is definitely not in the national interest.”).

See S. REP. NO. 99-541, at 5.

See id.

See O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 87 (Ct. App. 2006) (“[A] fundamental purpose of the SCA is to lessen the disparities between the protections given to established modes of private communication and those accorded new communications media.”).

See infra note 262.


Miller, 425 U.S. at 440-43.

Smith, 442 U.S. at 742-46.

Id. at 743 (“Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.”); Miller, 425 U.S. at 443 (“This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.”).

See S. REP. NO. 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555 (“Nevertheless, because it is subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection.”) (citing United States v. Miller, 425 U.S. 435 (1976))).


See, e.g., Abel v. United States, 362 U.S. 217, 241 (1960) (“There can be nothing unlawful in the Government's appropriation of... abandoned property.”); cf. United States v. Thomas, 451 F.3d 543, 545-46 (8th Cir. 2006) (holding that the defendant abandoned his mail after failing to retrieve it from a rented postal box for one year and, therefore, destroyed any Fourth Amendment property interest in the mail).

195 See, e.g., Mincey v. Arizona, 437 U.S. 385, 392 (1978) (“The need to protect or preserve life or avoid serious injury is justification for what would be otherwise illegal absent an exigency or emergency.”) (quoting Wayne v. United States, 318 F.2d 205, 212 (D.C. Cir. 1963)).

196 Compare 18 U.S.C. § 2702(b)(3), and 18 U.S.C. § 2703(c)(1)(C), with Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973) (“It is equally well settled that one of the specifically established exceptions to the requirements of both a warrant and probable cause is that a search is conducted pursuant to consent.”).

197 See, e.g., United States v. Jacobsen, 466 U.S. 109, 113 (1984) (holding that the Fourth Amendment “proscrib[es] only governmental action,” and does not apply to searches conducted by private individuals); Burdeau v. McDowell, 256 U.S. 465, 475 (1921) (“[The Fourth Amendment’s] origin and history clearly show that it was intended as a restraint upon the activities of sovereign authority, and was not intended to be a limitation upon other than governmental agencies ....”).


199 See supra notes 186-92 and accompanying text.

200 See H.R. REP. NO. 99-647, at 22 (1986) (noting the House committee's belief that e-mail “combines features of the telephone and regular first class mail” and discussing three differences between the these communication mediums that influenced the SCA’s development).

201 See Susan Freiwald, First Principles of Communications Privacy, 2007 STAN. TECH. L. REV. 3, ¶ 29 (arguing that the Katz decision depended “on the overriding importance of the telephone” and that “any other result would be destructive of society's ability to communicate”); see also infra notes 205, 212.


203 See S. REP. NO. 99-541, at 2-3, 5 (1986), reprinted in 1986 U.S.C.C.A.N. 3555 (discussing the importance of new communications and computer networking technology to individuals and commerce); id. at 5 (noting the statutory privacy protections for first-class mail and telephone calls, but absence of a statute protecting privacy in computer networks, despite each of these communication mediums being used interchangeably by consumers and businesses).

204 See, e.g., Ex Parte Jackson, 96 U.S. 727, 732-33 (1877) (holding that Fourth Amendment protections apply to the internal contents of letters and sealed packages in the possession of the U.S. Postal Service). Although many of the postal service privacy cases were decided before Katz and the third-party disclosure cases that followed, their reasoning continues to be upheld after these shifts in Fourth Amendment jurisprudence. See, e.g., United States v. Van Leeuwen, 397 U.S. 249, 251-53 (1970) (noting the continued Fourth Amendment interest in the privacy of the contents of first-class mail after Katz); United States v. Choate, 576 F.2d 165, 174-80 (9th Cir. 1978) (applying the Court's post-Katz framework and affirming prior case law holding that there is no Fourth Amendment privacy interest in the information appearing on the external parts of an envelope or package); see also Kerr, supra note 192, at 824 & n.126 (arguing that Katz actually caused little change in the Court's previous approach to the Fourth Amendment).

205 See, e.g., United States ex rel. Milwaukee Social Democratic Pub. Co. v. Burleson, 255 U.S. 407, 437-38 (1921) (Holmes, J., dissenting) (noting that use of the second-class mail was essential for a newspaper publisher to remain in business); Ex Parte Jackson, 96 U.S. at 733 (noting that access to the mail or other modes of transportation was necessary to circulate a publication).

206 Ex Parte Jackson, 96 U.S. at 733 (“Letters and sealed packages ... are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles.”).
Id. at 732-33 ("[A] distinction is to be made between different kinds of mail matter, [between what is intended to be kept free from inspection, such as letters, and sealed packages subject to letter postage; and what is open to inspection, such as newspapers, magazines, pamphlets, and other printed matter, purposely left in a condition to be examined.").

See, e.g., United States v. Huie, 593 F.2d 14, 15 (5th Cir. 1979); Choate, 576 F.2d at 174-80 (holding that there was no Fourth Amendment privacy interest in the information on the outside of a mailed package “because the information would foreseeably be available to postal employees and others looking at the outside of the mail”).


389 U.S. at 352-53.

See id. at 352 (“To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.”).

See id. at 352-53.


As Professor Kerr argues, there are many benefits to a statutory approach to privacy protections, including the development of policies on an ex ante basis and the ability to receive input and feedback from experts. Kerr, supra note 192, at 867-70, 875-82.


Encryption may ultimately remedy this problem in computer networks and, more specifically, in cloud computing. See Kerr, supra note 192, at 866 & n.389; Stephen J. Dubner, Bruce Schneier Blazes Through Your Questions, N.Y. TIMES, Dec. 4, 2007, http://freakonomics.blogs.nytimes.com/2007/12/04/bruce-schneier-blazes-through-your-questions/. However, the current lack of readily available encryption options for consumers and the inability of many cloud providers to support encryption limit their utility for constraining a cloud provider's access to a user's content.

With regard to the relationship between an RCS provider and a user's content, the SCA requires that the content be in the provider's possession “solely for the purpose of providing storage or computer processing” and that access to the content “not [be] authorized ... for purposes of providing any [other] services.” 18 U.S.C. § 2702(a)(2)(B) (2006).

See Kerr, supra note 192, at 807 (“[C]ourts rarely accept claims to Fourth Amendment protection in new technologies that do not involve interference with property rights, and have rejected broad claims to privacy in developing technologies with surprising consistency.”).


Court resurrected search-and-seizure rights in the form of the Fourth Amendment during the early part of the twentieth century, the Justices have subsequently dismantled the substance of those rights, especially during the last four decades."


\textit{See Herring v. United States, 129 S. Ct. 695 (2009)} (affirming the lawfulness of a search completed pursuant to an erroneous arrest warrant).

\textit{See, e.g., Kerr, supra} note 192, at 831 (arguing that “courts generally do not engage in creative normative inquiries into privacy and technological change when applying the Fourth Amendment to new technologies”); Richards, \textit{supra} note 187, at 1118 (“Moreover, the Court has been loath as a general matter to read the protections of the Fourth Amendment broadly in the context of new technologies.”). \textit{But see Mulligan, supra} note 78, at 1595-96 (“With respect to files on third-party servers, the case law supporting reasonable expectations of privacy in rented physical spaces and in computers and files stored on them, turned over for repair, suggest that electronically stored personal files on an RCS would fall within the zone of privacy protected by the Fourth Amendment.”).

\textit{See supra} notes 107-11 and accompanying text.


389 U.S. 347, 361 (Harlan, J., concurring).


Kerr, \textit{supra} note 192, at 857 (“[S]ince the 1960s Congress rather than the courts has shown the most serious interest in protecting privacy from new technologies.”). Professor Kerr argues that “legislatures often are better situated than courts to protect privacy in new technologies” because of their ability to respond to technological changes more rapidly, gather additional information, and consider the context of the technology’s application and future development. \textit{Id.} at 806-08, 888.

277 U.S. 438, 466 (1928).


\textit{See H.R. REP. NO. 99-647, at 23 (1986)} (“[R]emote computing services are still relatively new, and there is no case law directly on point.”); see also Anuj C. Desai, \textit{Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy}, 60 STAN. L. REV. 553, 577 (2007) (arguing that \textit{Ex Parte Jackson} merely constitutionalized the privacy protections that the Continental Congress adopted for the U.S. mail system in 1792).


242 See, e.g., Mulligan, supra note 78, at 1596-98.

243 Katz v. United States, 389 U.S. 347, 361 (Harlan, J., concurring) (“[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”).

244 See Smith v. Maryland, 442 U.S. 735, 740 n.5 (1979) (recognizing that government action influences expectations of privacy). The circularity is indirect though, and courts suggest that statutes do not reflect a per se threshold of societal expectations. See United States v. Hambrick, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999), aff'd, 225 F.3d 656 (4th Cir. 2000) (unpublished table opinion) (“Although Congress is willing to recognize that individuals have some degree of privacy in the stored data and transactional records that their ISPs retain, the ECPA is hardly a legislative determination that this expectation of privacy is one that rises to the level of ‘reasonably objective’ for Fourth Amendment purposes.”).

245 United States v. Drew, 259 F.R.D. 449 (CD. Cal. 2009), offers a timely example of this phenomenon. Few people are likely familiar with the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 (Supp. 2009), used to convict Drew, yet the resulting guilty verdict and media reports powerfully communicated to society the seriousness of violating a website's terms of service agreement under federal law. See, e.g., Jennifer Steinhauer, Woman Found Guilty in Web Fraud Tied to Suicide, N.Y. TIMES, Nov. 27, 2008, at A25. After the jury's verdict, the district court concluded that a “CFAA misdemeanor violation ... [for] the conscious violation of a website's terms of service runs afoul of the void-for-vagueness doctrine” and reversed her conviction. Id. at 464. But the court suggested that the CFAA's civil penalties or felony provisions might still be permissible for such violations. Id. at 464-67.

246 See, e.g., Anthony Downs, Up and Down with Ecology--The “Issue-Attention Cycle,” PUB. INT., Summer 1972, at 38, 38-41 (proposing a five-stage process through which public attention is focused on an issue and political action results).

247 See Lew McCreary, What Was Privacy?, HARV. BUS. REV., Oct. 2008, at 123, 126 (“[S]omeone will always have to speak for privacy, because it doesn't naturally rise to the top of most consideration sets, whether in government or in the private sector.”).

248 Compared to Internet users over sixty-five years old, Internet users under thirty years old are twice as likely to use cloud computing applications, nearly three times more likely to use webmail and online file storage, and seven times more likely to store personal videos online. HORRIGAN, supra note 50, at 5. These differences are further magnified when Internet utilization rates among the differing age groups are factored into account. Id.

249 In the 111th Congress, the average age of a senator was 63.1 years--an increase of more than three years since the 109th Congress. MILDRED AMER & JENNIFER E. MANNING, CONGRESSIONAL RESEARCH SERV., MEMBERSHIP OF THE 111TH CONGRESS: A PROFILE 1 (2008).

250 In the 111th Congress, the average age of a representative was 57 years--an increase of almost two years since the 109th Congress. Id.

251 At the beginning of the Court's 2009 Term, the average age of the nine Justices was 67.9 years. See THE JUSTICES OF THE SUPREME COURT (2009), http://www.supremecourts.gov/about/biographiescurrent.pdf.

252 See A Special Report on Social Networking: Privacy 2.0, ECONOMIST, Jan. 30, 2010, at 12, 12-13 [hereinafter Privacy 2.0] (summarizing recent comments by Mark Zuckerberg, the Chief Executive Officer of Facebook, arguing “that social norms ha[ve] shifted and that people ha[ve] become willing to share information about themselves more widely”).

253 See JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES 82 (2008) (“Digital Natives, who live so much of their lives in networked publics, are unlikely to come to see privacy in the same terms that previous generations have, by and large.”); Press Release, Zogby Int'l, What is Privacy? Poll Exposes Generational Divide on Expectations of Privacy, According to Zogby/Congressional Internet Caucus Advisory


255 See id. at 3; JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 231 (2008) (“People [born after 1985] routinely set up pages on social networking sites--in the United States, more than 85 percent of university students are said to have an entry on Facebook--and they impart reams of photographs, views, and status reports about their lives, updated to the minute.”).

256 See FRED H. CATE, PRIVACY IN THE INFORMATION AGE 102 (1997) (arguing that privacy conflicts with important values, including “society's interest in free expression, preventing and punishing crime, protection of private property, and the efficient operation of government”).

257 See Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 862-63 (Ct. App. 2009) (noting that an individual had no reasonable expectation of privacy when she posted material on MySpace, even if she “expected a limited audience,” because the material is “opened ... to the public at large” and the “potential audience was vast”).

258 See Matt Asay, Google Privacy Controls: Most People Won't Care, CNET, Nov. 5, 2009, http://news.cnet.com/8301-13505_3-10390456-16.html (“[F]or all our hand-wringer over privacy--and for good reason--the reality is that most of us, most of the time, really don't care. Or, rather, if accessing useful services or getting work done more efficiently requires some privacy concessions, we gladly concede.”).

259 See PALFREY & GASSER, supra note 253, at 63-64 (arguing that parents and teachers should educate younger generations about the potential long-term consequences of posting their intimate personal details on the Internet).

260 See Anderson, supra note 121, at 194 (describing the increasing availability of free digital services and the business model for such services).

261 See Privacy 2.0, supra note 252, at 13 (“Most people who use Facebook and other social networks seem prepared to accept the idea of targeted advertising as the price of getting free access to the service.”); Harris Interactive, Majority Uncomfortable with Websites Customizing Content Based Visitors Personal Profiles, http://www.harrisinteractive.com/harris_poll/index.asp?pid=894 (last visited Feb. 12, 2010) (finding that 49% of eighteen-to thirty-one-year olds are comfortable with cloud providers using their online activity to display contextual advertising or content, while just 31% of Internet users over the age of sixty-two approved).

262 See Reihan Salam, Good Guys Don't Make Billions, SLATE, Feb. 26, 2008, http://www.slate.com/id/2185113/ (“The vision of immaculate capitalism, in which no one gets screwed and everyone gets awesome, free stuff, is as old as capitalism itself. The trouble is that filthy lucre needs to change hands at some point, or else capitalism goes kaput.”). But see Steven Hetcher, Changing the Social Meaning of Privacy in Cyberspace, 15 HARV. J.L. & TECH. 149, 174 (2001) (“[D]ue to the efforts of norm proselytizers and norm entrepreneurs, the demand for privacy among consumers has surged.”).

263 See supra section IV.B.

264 Kerr, supra note 2, at 1214.

98 GEOLJ 1195
As e-mail and other forms of electronic communications began becoming widely used, Congress recognized the need to protect these new forms of communication from impermissible intrusion. Unsure whether the flexible approach to determining the extent of Fourth Amendment protections as announced in Katz v. United States would extend to electronic communications, Congress enacted the Electronic Communications Privacy Act (ECPA) to ensure a baseline level of protection. This Note argues that the Fourth Amendment does extend to electronic communications and, therefore, the provisions of the ECPA that allow the government to access certain electronic communications without a search warrant are unconstitutional.

Table of Contents

Introduction 350
I. Communications and the Fourth Amendment 351
A. The Third-Party Doctrine 355
1. Delivery and Routing Information Directly Conveyed to Third Parties 356
2. Records and Information Stored in Databases Managed by Third Parties 357
B. Fourth Amendment Standards Evolve with Technology 361
1. Telephone Conversations 362
a. Olmstead v. United States 362
b. Katz v. United States 363
2. Postal Mail 365
3. Telegraph Messages 368
C. Legislative Actions To Protect Electronic Communications 372
1. Motivation for the Electronic Communications Privacy Act 372
2. The Electronic Communications Privacy Act Framework 375
3. Internet Use After the Electronic Communications Privacy Act 378
4. Protections Under State Law 380
II. Different Levels of Protection Afforded by the Stored Communications Act and the Fourth Amendment 382
A. The Stored Communications Act in Action 382
B. Applying the Fourth Amendment to Electronic Communications 383
1. E-mail: Warshak v. United States 384
3. Protection for Other Electronic Information 389
a. Information Held by, but Not Directed to, Third Parties 389
Imagine that local law enforcement officers suspect one of the town's residents is trafficking drugs. The officers have a hunch that this person may be involved but have never observed anything that would give them probable cause to obtain a warrant to search him or any of his property. But, with some legwork, the officers discover that the suspect uses a free, public e-mail service. They then serve a subpoena on that service directing the provider to turn over all of the suspect's messages that are over 180 days old and prohibiting the provider from notifying the suspect. In response to this request, the officers receive thousands of old messages spanning everything from legitimate business correspondence to personal messages, online shopping receipts, and beyond. Still armed with nothing more than a hunch, the officers begin to comb through this individual's voluminous e-mail records describing all manner of personal information on a quest for probative evidence.

Congress recognized the potential problems that could flow from unlimited review of e-mails and other electronic communications in this and similar situations and grew concerned that existing Fourth Amendment jurisprudence might not encompass these new forms of communication. This is partly because electronic communications frequently pass through third-party intermediaries during transmission, and even though the messages are not directed to the providers, these third parties often store copies of the communications on their servers. In response to these concerns, Congress enacted the Electronic Communications Privacy Act (ECPA) to guarantee a baseline level of protection for electronic communications including e-mail.

Despite the ECPA's goal of broadly protecting electronic communications, the Act is premised on computer technology from the 1980s, and the developments over the past twenty years render some provisions of the ECPA inconsistent with the requirements of the Fourth Amendment.

Part I of this Note describes the current Fourth Amendment framework and how it has been applied to other forms of communication as well as to information that passes through third-party intermediaries. Part I also discusses the history behind the ECPA. Part II examines the conflict between two recent cases, which hold that electronic communications are protected by the Fourth Amendment, and the provisions of the ECPA, which allow access to these communications on a lesser showing than is required under the Constitution. Finally, Part III concludes that § 2703(b) of the Stored Communication Act (SCA), which allows law enforcement access to electronic messages greater than 180 days old without a warrant, is unconstitutional as applied.

I. Communications and the Fourth Amendment

The Fourth Amendment protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” The U.S. Supreme Court has consistently stressed that the Fourth Amendment right to be free from unreasonable search and seizure is an individual right that “protects people, not places.” When drafting the Fourth Amendment, the framers could not have anticipated technological advances such as e-mail and other forms of electronic communications that would later arise and be used by the public. Similarly, they could not have envisioned the new modes of surveillance that would become available for government use in investigating crime. However, the framers did intend to protect individuals from unreasonable government interference, and,
consequently, courts continually have had to interpret the broad language of *352 this amendment in light of new technological and social developments in order to define the scope of the protections it offers. 9

The Supreme Court has recognized that, apart from the specific items enumerated, “[t]he overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State.” 10 “It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property.” 11

Government agents typically must obtain a warrant specifying the area to be searched and the items to be seized before they may conduct a search to comply with the requirements of the Fourth Amendment. 12 The Framers abhorred general warrants and writs of assistance, 13 and, to ameliorate these concerns, required that government agents obtain warrants supported by probable cause before conducting searches. 14 The Constitution incorporates this concern by requiring that “no Warrants shall issue” unless they “particularly describ[e] the place to be searched, and the persons or things to be seized.” 15 The specificity requirement prevents agents from engaging in “fishing expeditions” that were possible under general warrants. 16

*353 In spite of the broad protection the Fourth Amendment offers from warrantless searches, not all government actions that uncover probative evidence are “searches” within the meaning of the Fourth Amendment, 17 and the Fourth Amendment does not protect individuals from searches in all areas. 18 Justice John Marshall Harlan II, concurring in the judgment in Katz v. United States, 19 suggested that individuals are protected by the Fourth Amendment in only those areas where they have both a subjective expectation of privacy and that expectation is objectively reasonable. 20 Katz arose when government agents used an electronic surveillance device attached to the exterior of a phone booth to eavesdrop on the caller's conversation. 21 Although not explicitly enumerated in the text of the Fourth Amendment, the majority concluded that an individual using a public phone booth is “entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world,” and found that the contents of phone conversations are protected under the Fourth Amendment. 22

The Supreme Court has since embraced Justice Harlan's two-prong approach for determining the scope of Fourth Amendment protections. 23 A subjective expectation of privacy alone is insufficient to create a privacy right, because, as the Court noted, regardless of how private he believes his actions are, a burglar in an abandoned summer cabin should not be protected by the Fourth Amendment. 24 In that situation, any subjective expectation of privacy the burglar might have is not one society recognizes as reasonable. 25 Although the Court stressed that when considering whether an expectation of privacy is reasonable, “arcane distinctions developed in property and tort law . . . ought not to control,” the expectation must be one that has a source outside the Fourth Amendment. 26 This is a flexible test designed to account for the many varied situations under which Fourth Amendment searches may take place. 27 However, inherent in the flexibility is a level of uncertainty as to the extent of protection in areas the Supreme Court has not previously considered, particularly in new media such as electronic communications. 28

Katz did, however, affirm that individuals do not have reasonable expectations of privacy and, therefore, are not protected by the Fourth Amendment, where they voluntarily expose items to public view. 29 From this premise, the Court has developed a third-party exception that finds that individuals do not have reasonable expectations of privacy
in items turned over to third parties, and that the Fourth Amendment therefore does not govern search and seizure of items in a third party's possession. 30

E-mail and other forms of electronic communications are transmitted over servers which are frequently run by third parties. For example, if we were to imagine that Jeremy used the free e-mail account provided by his Internet service provider (ISP) to compose an e-mail to his friend Richard at Richard's work e-mail account, the message would go from Jeremy's computer, through his ISP's servers and over the Internet, to the mail server run either by Richard's company or another third-party ISP. The message will then be directed to Richard's mailbox, where it will sit until he attempts to retrieve it. When Richard downloads the message, if he wants to forward it to his coworker James, the message will go up from Richard's computer to the server run by his firm, and into James's mailbox. 31 Although Richard is the only intended initial recipient of Jeremy's e-mail message, the message passes through Jeremy's ISP's server, where administrators have the technical capability to inspect the contents of the message. However, when Richard forwards that same message to James at an address inside his firm, the message stays on the firm's e-mail server and does not pass through the hands of any third parties. 32

Many e-mail messages, such as the hypothetical one discussed above from Jeremy to Richard, are sent through free, public services or pass through servers run by third-party ISPs at many points during transmission. This third-party interaction with the communication complicates Fourth Amendment analysis. 33

A. The Third-Party Doctrine

The Fourth Amendment may protect an individual from unreasonable searches of items she seeks to maintain as private, but the Supreme Court has in several cases adopted a “Third-Party Doctrine,” which finds that an individual no longer has such an expectation of privacy where the items in question are voluntarily turned over to third parties. 34 For example, the Court found that the infamous president of the Teamster's Union, James “Jimmy” Hoffa, could not assert a Fourth Amendment challenge to suppress statements he voluntarily made to a third party who later turned and communicated the substance of those conversations to government agents. 35 Hoffa made the incriminating statements in his hotel room to an associate Edward Partin, who Hoffa expected would keep the information private. 36 However, in doing so the Court noted that Hoffa was “not relying on the security of the hotel room; he was relying upon his misplaced confidence that Partin would not reveal his wrongdoing.” 37 In this situation, Hoffa voluntarily turned the information over to the third party and, therefore, could not control that individual's use of the information or later complain if he chose to inform others, notably the government, about it. 38

Based on decisions like United States v. Hoffa, 39 the government is free to subpoena messages from their intended recipients without implicating the Fourth Amendment. However, individuals do not forfeit all Fourth Amendment protections merely by conveying some information to third parties. 40 Particularly in light of new technology and new forms of communication and surveillance, as present in Katz, the Supreme Court has had to balance these competing interests to determine the extent of an individual's protections.

Applying the principles of Hoffa, and focusing on information directed to third parties, the Court carved out an exception to the otherwise strong protections afforded to telephone conversations 41 and postal mail 42 for delivery and routing information that is directly conveyed to third parties for their use in connecting and delivering the communications. 43
The Court similarly held that other information voluntarily conveyed to third parties and stored in their databases is not protected by the Fourth Amendment.

1. Delivery and Routing Information Directly Conveyed to Third Parties

After Katz, although phone companies have the technical sophistication to easily listen to or record phone conversations, the content of these conversations is protected under the Fourth Amendment. However, in Smith v. Maryland, the Supreme Court approved the government's use of pen registers to track the telephone numbers individuals dialed. In contrast to the strong protections for the substance of phone conversations, the Court concluded that individuals do not have reasonable expectations of privacy in the numbers dialed since they voluntarily convey this information to the phone company. The Court inferred from the fact that customers received itemized bills listing the long-distance calls they made, “[t]elephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes.” With this awareness, the Court held that, in general, individuals do not have even a subjective expectation of privacy in the phone numbers they dial.

However, the Court went on to apply the second prong of the Katz test, and held that, even if the particular defendant in Smith did have a subjective expectation of privacy in the telephone numbers he dialed, it was not an expectation society recognized as reasonable in light of the telephone companies' regular practice of recording this information. Therefore, the government's use of this information still would not violate the Fourth Amendment.

Similarly, although postal workers could easily open and inspect the contents of the letters and packages they are delivering, these communications are strongly protected by the Fourth Amendment. At the same time, the U.S. Postal Service is expected to deliver the items deposited with it to their intended recipients. In doing so the Postal Service is expected to, and indeed must, read the address and other information displayed on the exterior of the package. Because this information is not only voluntarily turned over, but also directed to the third-party Postal Service, it is not protected by the Fourth Amendment.

These decisions recognize that the mere fact that some part of a communication, such as the telephone number or delivery address, is directed to a third party, does not give that third party access to the entire communication. Additionally, although the third party may have the potential to access information in its possession, this does not suffice to bring the information within the purview of the third-party doctrine or limit Fourth Amendment protections.

A limited application of the third-party doctrine to information actually conveyed to the third party is also applicable to electronic messages. Electronic communications will also generally pass through servers controlled by third parties before ultimately arriving in the intended recipient's mailbox. Like the Postal Service, e-mail providers' computer systems are expected to “read” some of the address information so that they may properly route and deliver the messages. However, e-mail providers are not expected to review the content of the messages, and Part III of this Note concludes that, because they are only expected to read the noncontent, address information, the sender does not forfeit her Fourth Amendment rights in the content of the message.

2. Records and Information Stored in Databases Managed by Third Parties
In addition to information directly conveyed to third parties for their use, many entities also maintain databases that contain information gathered from their users and customers. Consistent with its decisions regarding information turned over to third parties, the Supreme Court has held that where records are entrusted to third parties, the third party's concurrent access may eliminate an individual's privacy interest and, consequently, the protections she is afforded under the Fourth Amendment. For example, in *United States v. Miller* (1947), the Court concluded that individuals do not have reasonable expectations of privacy in financial records held by third parties.

In Miller, Mitchell Miller was convicted of carrying on the business of a distiller without giving bond in an attempt to avoid the whiskey tax. The government subpoenaed checks and financial records from the two banks used by Miller and relied on those documents as evidence at trial. The Court held that, like Jimmy Hoffa speaking to his associate, Miller had “assumed the risk” that any documents he turned over to the bank could later find their way into the hands of the government. Therefore, Miller had no reasonable expectation of privacy in their contents and could not claim the protections of the Fourth Amendment.

Much like in Smith, where the Court held that there was no reasonable expectation of privacy in the numbers dialed because they had been “turned over” to the phone company, here too, by turning his checks over to the bank, the Court concluded that Miller lost any expectation of privacy he might otherwise have had by maintaining the checks in his private possession.

The agents in Miller actually reviewed microfilm copies of Miller's records, which further supported the Court's conclusion that the Fourth Amendment did not protect Miller in this situation because the items searched were not Miller's “private papers,” but the bank's business records. However, the Court then went on to note that even if the agents had viewed the originals created by Miller and held by the bank, Miller still would not have a reasonable expectation of privacy in them. This is because “[t]he checks are not confidential communications but negotiable instruments to be used in commercial transactions.” Even the deposit slips and monthly accountings were not protected because they only contained information that, according to the Court, had been “voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.”

Similarly, three years earlier, in *Couch v. United States*, the Court held that an individual could not assert either Fourth or Fifth Amendment challenges to prevent the government from subpoenaing tax records in the possession of the individual's accountant. Writing for the majority, Justice Lewis Powell found that the defendant could not have a reasonable expectation of privacy in the records she handed over to her accountant because they were in the possession of a third party, and she knew that much of the information would have to be turned over to the government while preparing her taxes. However, in dissent, Justice William Douglas noticed that “[u]nder these circumstances, it hardly can be said that by giving the records to the accountant, the petitioner committed them to the public domain.” Unlike Justice Douglas's dissent, Justice Powell's opinion conceives of privacy under the Fourth Amendment as binary—as soon as a third party is given access to information the individual's privacy interest vanishes. However, Justice Douglas recognized the societal understanding that, although a third party had access to the information, the third party was expected to keep it private and not to disseminate it freely.
Like the financial institutions in Smith and the accountants in Couch, ISPs frequently maintain databases containing personal and transactional information about their users, and often store and archive copies of the electronic communications they process. Many individuals also use Internet-based e-mail (Webmail) systems where all of their messages are stored in electronic mailboxes on their e-mail providers' remote servers. Some lower courts have taken an expansive view of the third-party exception, and have found that individuals do not have reasonable expectations of privacy in credit card statements, utility records, motel registration records, or employment records. Some information in these databases, such as subscriber information, is directly conveyed to the ISP for its use, and is not protected by the Fourth Amendment after Miller. However, even though other information, such as archival or backup copies of messages, are not stored by the ISP for its use, an expansive interpretation of the third-party doctrine could potentially eliminate a user's Fourth Amendment protections for this information.

Smith and Miller have been criticized over time, particularly as more personal information is incorporated into privately managed databases. Private entities had already accumulated large amounts of information before Smith and Miller were decided. However, with a greater number of transactions being completed electronically, far more records are being created and stored, and the universe of information contained in databases controlled by third parties is greatly expanding. Since this information is currently accorded no Fourth Amendment protection, and may be accessed with a subpoena, the government frequently relies on it during criminal investigations and prosecutions. Even when information culled from databases is used to combat serious threats such as terrorism, the public has not always been in favor of extensive government use of this data.

In light of the rapidly expanding universe of information turned over to third parties, an expansive interpretation of Miller permits easy access to a tremendous amount of information. In its later decisions involving these issues, the Supreme Court began to recognize some of the potential problems stemming from the increased pooling of information in databases. For example, in United States Department of Justice v. Reporters Committee for Freedom of the Press, a CBS news correspondent made a request under the Freedom of Information Act to obtain information about the members of the Medico family contained in their “rap sheets.” The Court noted that, in spite of the fact that much of the information summarized in the rap sheets may have been public at one time, there was still a privacy interest in preventing disclosure of the compilation. More relevant to the Fourth Amendment inquiry, the majority also recognized that “[i]n an organized society, there are few facts that are not at one time or another divulged to another.” The Court also concluded that privacy and the “Third Party Doctrine” are, for Fourth Amendment purposes, not binary, and “the fact that an event is not wholly ‘private’ does not mean that an individual has no interest in limiting disclosure or dissemination of the information.” This approach is more analogous to the theory proposed several years earlier by Justice Douglas in Couch. In the arena of electronic communications, because ISPs are generally expected to keep communications private, it limits arguments that electronic communications are not protected under the Fourth Amendment merely because a third party retains backup or archival copies on its server. This analysis also comports with the distinction drawn in Smith and Katz between information actually turned over to the phone company for its use, and information merely in its possession.

**B. Fourth Amendment Standards Evolve with Technology**

As technology evolves, giving individuals new forms of communicating and government agents increasingly sophisticated tools for surveillance, courts have had to continually interpret the Fourth Amendment and define the extent of its
reach in light of these new advances. When writing for the majority in Kyllo v. United States, even Justice Antonin Scalia, a staunch believer in originalism, remarked on the dangers that would flow if the Fourth Amendment was not construed in a flexible manner. In particular, the Supreme Court considered the applicability of the Fourth Amendment to telephone conversations and postal mail, and in both cases concluded that the contents of the communication were protected by the Fourth Amendment. Additionally, although never decided in a reported judicial decision, commentators at the time argued that telegraph messages should also be protected under the Fourth Amendment.

1. Telephone Conversations

The Supreme Court has not always been as responsive to evolving technology as it was in Kyllo. In 1928, the Court first considered whether telephone conversations were protected by the Fourth Amendment, and concluded they were not. It was not until almost forty years later when the Supreme Court reconsidered this important question and, in light of the growing importance of the telephone, concluded the Fourth Amendment did extend to these communications.

a. Olmstead v. United States

In Olmstead v. United States, federal agents discovered Roy Olmstead was involved in an illegal conspiracy to distribute intoxicating liquors after listening in to conversations between Olmstead and his coconspirators. The agents had tapped Olmstead and his coconspirators' telephones without entering onto private property. Focusing on the elements of trespass, the Court concluded that “the Amendment cannot be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office any more than are the highways along which they are stretched.”

However, in dissent, Justice Louis Brandeis expressed his belief that in expounding the Constitution, the Court should not be so constrained by the limited scope of what the forefathers anticipated. Even in 1928, Justice Brandeis recognized that the progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.

Justice Brandeis's premonition did not then carry the day, and the Court's five-to-four decision in Olmstead left law enforcement free to eavesdrop on telephone conversations. However, as the government increasingly relied on information gleaned from wiretaps, the public began to question the majority's wisdom in condoning this activity.

b. Katz v. United States

Although telephones were widely used when Olmstead was decided, the telephone became increasingly important to daily life over time, and, almost forty years later, a situation similar to that in Olmstead arose in Katz v. United States. This time, however, the Court came to a different conclusion. In Katz, government agents attached an electronic
surveillance device to the exterior of a public phone booth and used it to eavesdrop on Charles Katz's conversation. In contrast to Olmstead, the Katz Court rejected the government's argument that because there was no physical entry into the phone booth, and therefore no trespass, the surveillance did not implicate the Fourth Amendment. Even though privacy in phone booths was not explicitly enumerated in the text of the Fourth Amendment, the majority concluded that an individual using a public phone booth is "entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world." Recognizing the importance of, and widespread reliance on, this new technology, the Court noted that "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."

By abandoning its previous approach to the Fourth Amendment, which focused on physical trespass, the Court recognized the importance the telephone had come to have in society. In doing so, Katz corrected the Court's previous error in Olmstead, which placed substantial emphasis on historical usages and failed to consider the practical import of the government's actions. Critics have noted that, in contrast to Katz, Olmstead "symbolizes the Court's lack of responsiveness to new technology, unwarranted formalism in its constitutional interpretation, and failure to see the larger purposes of the Fourth Amendment." Additionally, Katz is notable for Justice Harlan's concurrence suggesting that individuals are protected by the Fourth Amendment in areas where they have a subjective expectation of privacy as long as that expectation of privacy is objectively reasonable.

Although Katz was decided three years before Smith, the two decisions demonstrate the limits of the third-party doctrine. While an entire phone call--numbers dialed and content of the conversation--is "turned over" to a third-party telephone company, these decisions acknowledge that the third-party exception does not give government agents unbridled access to the entire call. The telephone number dialed is directly conveyed to the phone company so that it may connect (and bill for) the call, but the content of the call is not similarly directed. Even though both the number dialed and content of the phone conversation pass through the third party, the content of the phone call is not "turned over" in the same way that the telephone number dialed is. Katz recognizes that Fourth Amendment protections for the content of the conversation are not diminished simply because the content passes through the third-party-intermediary phone company.

E-mail plays a central role in daily life and is used in place of postal mail or the telephone for many communications. Just as the increased use and importance of the telephone played into the Court's constitutional analysis in Katz, the importance of modern day electronic communications also should inform the constitutional analysis. Additionally, the distinction between the strong protections offered for the content of phone conversations and the far weaker protections offered for numbers dialed demonstrates the boundaries of the third-party doctrine. This distinction also demonstrates that law enforcement cannot parlay a third party's limited access to one part of an item into access to all of it.

2. Postal Mail

The Supreme Court reached a very similar result to the decision it would later reach in Katz when, in Ex parte Jackson, it held that the Fourth Amendment protects the contents of letters and packages deposited in the U.S. mail system. The text of the Fourth Amendment specifically includes "papers," and the Court concluded that "[t]he
PROTECTIONS FOR ELECTRONIC COMMUNICATIONS:..., 78 Fordham L. Rev. 349

constitutional guaranty of the right of the people to be secure in their papers against *366 unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be.”

Notably, postal mail, like e-mail, is turned over to third parties who are physically capable of opening and inspecting the contents of the letters they have been given to deliver. During the colonial period individuals traditionally used wax to seal their letters, but this wax was ineffective and often failed to keep the letters securely closed. *367 Despite attempts to ensure that the mails would remain private, the public widely believed they were not secure, which prompted a number of prominent individuals to write in code in an attempt to keep their communications private. Thomas Jefferson, for example, remarked in a letter that “the infidelities of the post office and the circumstances of the times are against my writing fully and freely.” In response to these concerns, Congress passed several laws prohibiting the improper opening of mail, but, despite the reality that mail was not being kept private, the Supreme Court ultimately held that Fourth Amendment protections extended to include postal mail.

Particularly in light of these factual underpinnings, Professor Daniel J. Solove suggests that the Court's decision was more than just a recognition of an existing privacy interest, but was an example of the Court constructing a privacy interest that was necessary to preserve the integral role the mails had come to play in society. Justice Joseph Story believed, just as Thomas Jefferson had, that individuals would not be completely candid in their correspondence without having an expectation of privacy. In such a situation, Justice Story anticipated that the public would simply stop using the mails “to the detriment of the ‘well-being of society,’” resulting in slowed economic growth and unnecessary burdens being placed on commercial transactions forced to use less effective means of communication.

*367 In Ex parte Jackson, although the Court held that the sealed contents of the communications were protected, it concluded that the address and other information on the exterior of the package were not. Similarly, postcards, pamphlets, and other materials “purposely left in a condition to be examined” when deposited with the Postal Service are afforded no Fourth Amendment protections. This reasoning recognizes that although the item is placed in the custody of the Postal Service, the author of a letter still retains an expectation of privacy in the contents because the Postal Service is not expected to read that information. At the same time, the Postal Service is not expected to turn a blind eye to readily visible information. Quite the contrary, it is expected to deliver the letter to its intended recipient, and in doing so must read the address and other information contained on the package. While not the focus of the Court's decision, this distinction serves to protect the “content” information of a communication, and only allows the government warrantless access to the “noncontent” information. It also recognizes that depositing an item with a third party does not necessarily give that individual carte blanche to do what she wishes. In this case, although third parties theoretically could read everything, they are expected to read only the information directed to them-- the information on the exterior.

Although the Court in Smith did not discuss Ex parte Jackson, it reached a similar result, and together, the two cases highlight the limits of the third-party doctrine. In the case of a telephone, the number dialed is necessarily and intentionally conveyed to the phone company so that the company may complete the call. Similarly, individuals expect the Postal Service to read the addresses written on the exteriors of the letters they are sending so that the letters will be delivered properly. However, as the Court recognized in Ex parte Jackson, individuals do not expect the third-party carrier--or any other party--to read the contents of the items they are mailing. These decisions highlight that a third party merely having access to an item does not suffice to bring the information within the purview of the third-
party doctrine, and also recognize the importance of extending Fourth Amendment protections to dominant forms of communication.

*368 3. Telegraph Messages

Telegram transmissions share some of the characteristics of present day electronic communications, but the process of sending a telegram is far less automated and requires greater human interaction. 154 Like postal mail and e-mail, most telegrams traveled over networks run by third parties. 155 However, unlike sealed letters, telegraph messages are far more exposed to review by intermediaries while in transit. 156 Notwithstanding this reality, commentators writing while telegraphs were widely used viewed these messages as the then-modern-day equivalent of postal mail and believed that they should be protected to the same extent as the mails. 157

After Samuel Morse demonstrated his telegraph in 1838, telegraph networks were quickly deployed across the United States and other countries, enabling people to send instantaneous messages. 158 Despite the higher cost of sending messages by telegraph, the telegraph's speed advantage displaced some business from the Post Office. 159 Users would write out their messages and hand them over to telegraph operators to encode and transmit across the telegraph lines. 160 At the other end, another operator would capture, decode, and transcribe the transmission, and then deliver the message to its intended recipient. 161 In addition to the potential for eavesdropping during transmission, telegraphy in this setting requires that the operators on both ends actually read the messages. 162 At the time, telegraph operators sought to maintain an impersonal attitude to the messages they delivered, but, particularly in small towns, they were “privy to most everything that went on in the town.” 163

During the American Civil War, the telegraph was widely used, and government officials grew concerned about security leaks. 164 To uncover treason and guard military secrets, the government seized and reviewed all *369 telegrams. 165 After the war, Congress undertook additional investigations and sought to uncover evidence from the files of telegraph operators, particularly Western Union, the primary telegraph operator at the time. 166 Members of the public were outraged when they discovered that Congress was reviewing telegraph messages. 167 Eventually, members of the legislature discovered that even their own messages were being reviewed. 168 Even though Congress promised it would keep the information it learned confidential, these assurances were not enough to appease the public's concerns. 169 In response, Western Union adopted Rule 128, which prohibited the disclosure of messages to anyone other than the intended recipient. 170

Acting under orders from the company's president, William J. Orton, Western Union managers began to refuse government requests to turn over private telegrams, while Orton and other groups urged Congress to enact legislation to protect these messages. 171 Representative James A. Garfield, who went on to serve as the twentieth President of the United States, noted that the telegraph is, “next to the post office, the custodian of more secrets in relation to public and private affairs than any other institution on earth,” and urged Congress not to require Western Union to turn over the requested telegrams. 172 On the other side, Senator Roscoe Conkling noted that the process of sending a telegraph is akin to asking a third party to deliver an oral message, and therefore one cannot expect that the message will be kept private, and cannot complain if the government requires its disclosure. 173 Other members of Congress were similarly concerned
that limiting access to this evidence might unnecessarily burden criminal and other investigations. In a controversial action, Congress passed a resolution requiring the telegraph managers to deliver the requested messages.

In response to this action, and to protect against disclosure going forward, Western Union made arrangements to destroy messages after delivery. Although this would serve to protect their communications from government review, businesses were opposed to this measure as it would then be impossible to prove that Western Union had been responsible for mistakes in transmission. With some Western Union managers facing imprisonment for failing to comply with congressional demands, Western Union ultimately did not destroy the messages, and complied with the requests.

Eventually, prominent legal commentators like Judge Thomas M. Cooley, began to suggest that the rationale underlying finding strong Fourth Amendment protections for postal mail was equally applicable to communications by telegraph. Judge Cooley also expressed his view that the law cannot limit the protection afforded to telegraph users on the theory that they could send their messages by other means. Telegraph use, and the need for quick communication, had become so important that Judge Cooley remarked, “Neither is the use of the telegraph a matter of mere choice. Business transactions cannot be successfully carried on without resort to its facilities, and the exigencies of family communication are daily demanding the most speedy transmission of messages that shall be found possible.” Notably, because of how they are transmitted, telegraph messages were, as Senator Conkling noted, far more akin to asking a third party to deliver a message than depositing a sealed letter with the post office.

Western Union proposed a bill to protect telegraphic messages to the same extent as postal mail, and, although the bill was favorably reported out of committee, it was never passed. Congress kept its authority to demand messages from the telegraph companies but limited its subpoenas to particular and germane messages. Later state and federal cases considering the validity of government subpoenas only considered the statutory protections for telegraph messages and did not consider whether they were protected under the Fourth Amendment. These decisions concluded that, although telegraph messages were not entitled to the same level of protection as mail, the subpoenas requesting telegraph messages must at least specify the telegram by date and subject.

Several states later adopted laws forbidding the tapping and interception of telegraph messages, and by 1909 thirty states had adopted laws forbidding employees of private telegraph companies from disclosing messages to anyone other than the intended recipient. However, these laws either explicitly exempted judicial subpoenas, or were interpreted to include such exceptions by the courts. With the invention and widespread adoption of the telephone, telegraph use soon dropped. With decreased use, concern over government and third-party seizure of telegrams also diminished, leaving the issue unresolved.

This issue arose before the Supreme Court adopted the two-part Katz test, and the Court never decided whether telegraph messages were protected by the Fourth Amendment. But, even where telegraph operators reviewed the entire contents of the telegrams they transmitted, members of the public still expected these messages to be kept private and were outraged at government review of these communications. Commentators at the time, like Judge Cooley, argued that telegraphs were the modern day analogue of postal mail, and as such, should be given the same protections of the Fourth Amendment.

*370

*371
Modern-day electronic communications share some similarities with the way in which telegraph messages were transmitted, though e-mail messages are not nearly as exposed to the carriers as telegraph messages were. The strong opposition to leaving telegraph messages unprotected further supports finding that e-mail and other electronic communications are protected under the Fourth Amendment. Additionally, the experience with telegraph messages also highlights the importance of extending strong constitutional protections to new and important modes of communication.

*372  C. Legislative Actions To Protect Electronic Communications

In the 1980s, as electronic communications became increasingly widely used, legislators grew concerned that the existing Fourth Amendment and statutory framework left these new media vulnerable to government and private interception, and sought to enact legislation to protect them. Although the 1968 Wiretap Act was only eighteen years old when the ECPA was enacted, commentators noted that the old Wiretap Act was already obsolete, and this new action was necessary to protect the important, emerging field of electronic communications.

1. Motivation for the Electronic Communications Privacy Act

At the request of the House Committee on the Judiciary, Subcommittee on Courts, Civil Liberties, and the Administration of Justice, and the Senate Committee on Governmental Affairs, the Office of Technology Assessment (OTA) created a report summarizing the current protections available to electronic communications. The OTA Report found that current protections for electronic mail were “weak, ambiguous, or nonexistent,” and concluded that “[t]he existing statutory framework and judicial interpretations thereof do not adequately cover new and emerging electronic surveillance technologies.” In part because of the Supreme Court's treatment of information conveyed to third parties, when Congress enacted the ECPA it was unclear whether users maintained reasonable expectations of privacy in remotely stored files such that they would be protected under the Fourth Amendment. Consequently, Congress wanted to ensure that these communications could not be freely seized.

The OTA Report began by noting that “[a]lthough the principle of the fourth amendment is timeless, its application has not kept abreast of current technologies.” The report discussed government surveillance of several different methods of electronic communications, and recognizes the increasing importance of e-mail. The report also noted that in attempting to define the level of protection that should be afforded to new technologies, it is helpful to compare to them to their pre-electronic analogues. In the case of e-mail, the report concluded that the analogue is first class mail, which is afforded strong Fourth Amendment protections.

In spite of the inherent unpredictability of the Katz test, and the possible applicability of the third-party doctrine, the report concluded that a sender's messages will likely be protected by the Fourth Amendment while stored on her computer or in her remote electronic mailbox. Similarly, the recipient would also enjoy protection under the Fourth Amendment while the message is stored either in an electronic mailbox on his personal computer or in an electronic mailbox on his e-mail provider's server. Although the report concluded that the existing constitutional and statutory framework did not protect messages while in transit, it recognized that the information conveyed in these messages may be personal and that, in general, individuals expect that the contents will remain private among the group with whom they are communicating. The OTA Report also considered that, as a practical matter, e-mail providers have
access to the communications and frequently retain copies of messages in their databases for backup protection and billing purposes. After Miller, the OTA Report noted that these additional copies may limit an individual's Fourth Amendment protections.

The OTA Report proposed three possible paths for Congress to pursue: (1) legislate to ensure e-mail has the same degree of protection as first class mail; (2) give protection to the message while in the sender's and recipient's electronic mailboxes, but not specifically legislate to define the protection afforded during transmission, and instead rely on the existing aural limitation in Title III; or (3) wait to see how the e-mail market and case law develop to see if any action is necessary. Under any approach, the OTA Report recognized that intercepting a large quantity of email may constitute a fishing expedition and that, regardless of where it is intercepted, because the communications are electronic and there are in effect an infinite number of “copies,” it may be difficult or impossible for the user to tell if a message has been seized. The report also concluded that “given the high threat to civil liberties posed by interception of electronic mail . . . the governmental interest in interception would have to be quite compelling” to justify interception.

At a subcommittee hearing, Representative from Wisconsin and Chairman of the House Judiciary Subcommittee Robert Kastenmeier noted that “new modes of communication have outstripped the legal protection provided under statutory definitions bound by old technologies. The unfortunate result is that the same technologies that hold such promise for the future also enhance the risk that our communications will be intercepted by either private parties or the Government.” Representative Kastenmeier went on to say that “Congress needs to act to ensure that the new technological equivalents of telephone calls, telegrams, and mail are afforded the same protection provided to conventional communications.” Senator Patrick Leahy also participated in developing the ECPA, and during the hearing recognized that, although we may have shifted to a new form of communication, the public's privacy interest in its communications has not changed. Senator Leahy remarked that the “rules don't change at all. The technology changes. All the legislation does is to make sure that the rules stay consistent with the technology.”

Introducing the ECPA to the House of Representatives, Representative Kastenmeier explained that the “Act updates existing Federal wiretapping law to take into account new forms of electronic communications such as electronic mail, cellular telephones, and data transmission by providing such communications with protection against improper interception.” The Act was designed to provide broad protection in this quickly evolving and largely unknown field, and Representative Kastenmeier justified the broad scope by explaining that “[a]ny attempt to write a law which tries to protect only those technologies which exist in the marketplace today . . . is destined to be outmoded within a few years.” Although focused on electronic communications, the act recognized that the goal was to protect the “sanctity and privacy of the communication” itself. Despite its attempt to protect communications broadly, commentators have noted that the ECPA's provisions are narrow, and that it is not a “catch-all” designed to provide general protections to all computers and computer networks.

The ECPA enjoyed strong support from both the House and the Senate, and from industry and the public when it was enacted. The OTA report and statements from the bill's sponsors all suggest that Congress sought to provide broad protection to electronic communications so that they were at least as strongly protected as traditional forms of communication such as first class mail and telephone calls.

2. The Electronic Communications Privacy Act Framework
The ECPA was enacted in 1986, amending Title III of the Omnibus Crime Control and Safe Streets Act of 1968, and has not been significantly modified since. The Act contains three main sections: Title I protects wire, oral, and electronic communications while in transit (Wiretap Act); Title II contains the Stored Communications Act (SCA), which protects communications held in electronic storage; and Title III restricts the use of pen registers (Pen Register Act). The section relevant to the protection of e-mails, text messages, and other forms of electronic communications is Title II—the SCA. Even though the statute would seem to be quite important and it is frequently used, commentators have noted that the “statute is dense and confusing, and few cases exist explaining how the statute works.”

The SCA imposes a fine or imprisonment for any intentional access to a facility where electronic communication service is provided, but does not apply to conduct authorized by the person or entity providing the service. The SCA differentiates between providers of “Electronic Communication Service” (ECS), “which provides to users thereof the ability to send or receive wire or electronic communications,” and “Remote Computing Service” (RCS), which is characterized by “the provision to the public of computer storage or processing services by means of an electronic communications system.” When the SCA was passed, computers were far more expensive and far less powerful than they are today. In addition to using third-party service providers to send and receive messages, some also outsourced what may now be considered to be basic computer tasks, including processing and file storage. However, as the services provided continue to expand and evolve, the delineation between ECS and RCS providers has blurred.

The SCA generally prevents both ECS and RCS providers from disclosing data in electronic storage, but has an important exception for electronic messages stored by an RCS. The statute clarifies that the government may only obtain the contents of an electronic communication that has been in storage with an ECS for less than 180 days pursuant to a warrant. However, the government does not need a warrant supported by probable cause to obtain communications maintained in an ECS that are more than 180 days old or to obtain communications stored in an RCS. The government may use either an administrative subpoena, if authorized by statute, or a court order to obtain this information. A court order only requires “specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication ... are relevant and material to an ongoing criminal investigation,” which is less than is required to establish probable cause and obtain a warrant. There is no requirement that the government specify the type of messages it is seeking or the date of the messages. Although the government is required to give notice to the subscriber, it may delay notice for ninety days where there is reason to believe that notification may have an “adverse result.” And, if the government does elect to procure a warrant, then it is not required to give notice to the subscriber at all. Section 2703 of the SCA also requires ECS and RCS providers to disclose the name, address, method of payment, and other information about subscribers when subpoenaed.

When enacting the ECPA, Congress found that “[m]ost--if not all-- electronic communications systems ... only keep copies of messages for a few months.” The Committee concluded that beyond this point, the storage is more akin to that of business records maintained by a third party, which are accorded less protection. This is in part because when the Act was drafted, users generally needed to take affirmative steps to move e-mail messages they wanted to preserve into storage in order for e-mail providers to save them beyond 180 days.
to providing “first-class mail-like protections” to e-mail, and the distinction between e-mail less than 180 days old and greater than 180 days old. 249 This also helps explain why communications greater than 180 days old are only afforded the same protection as records stored in a remote server. 250

*378 3. Internet Use After the Electronic Communications Privacy Act

Internet and e-mail use have dramatically increased since the SCA came into force. 251 More and more households have broadband Internet access in their homes, 252 and a 2008 report found that nearly 70 percent of Americans used Internet Webmail services, stored data and photos online, or used online software programs. 253 The study found that in the eighteen- to twenty-nine-year-old age group, 77 percent of users surveyed used a Webmail service. 254 49 percent of users surveyed stated they would be “very concerned” if their providers allowed law enforcement to access their files when requested to do so. 15 percent would be “somewhat” concerned, and 11 percent would be “not too” concerned. 255 However, 22 percent stated they would be “not at all” concerned if the government were allowed access. 256

In addition to its increased use, e-mail is routinely held on providers' servers for increasing periods of time, and, in some cases, even indefinitely. For example, several companies, including Google, offer free Webmail service. When Google launched its Webmail service, GMail, in 2004, it provided users with one gigabyte of storage for free. 257 Now, just five years later, GMail users have over seven and a half gigabytes of storage available, and that amount is continually increasing. 258 With so much space at their disposal, users are encouraged not to delete their messages, but to archive them so that they are always available and always *379 searchable. 259 Irrespective of the level of protection that should be afforded to these messages, this use does not comport with Congress's general perception of e-mail use when it drafted the SCA, particularly the expectation that mail would rarely be retained for more than 180 days. 260 Although these servers store e-mail, they store it for the user, and there is no indication that the providers read the private correspondence. 261

In addition to storing e-mail on remote servers, individuals are also increasingly turning to third parties for remote file storage and backup. 262 Users generally expect the information stored remotely to be kept private, and the providers also promise not to view the data stored on their servers. 263

Despite the changes in e-mail and computer use, the SCA has been largely unmodified. In 2000, Representative Charles Canady introduced a bill amending certain provisions of the 1986 ECPA, 264 and, although the bill was favorably reported out of committee, 265 it was ultimately not enacted. The proposed amendments included a number of changes, and, relevant to electronic communications, would have required the government to demonstrate probable cause before accessing location information for cellular phones and to procure a warrant before accessing e-mail messages greater than one year old-- doubling the time required under the 1986 act. 266 The report does not explain the significance of the change to one year, 267 but one year is still a far shorter period of time than the period for which messages are typically retained. 268 More recently, the Constitution Project, a coalition of twenty-five organizations and seventy-five individuals interested in constitutional law, recommended that the President and Congress take action to ensure Fourth Amendment protections for all location information, all e-mail messages (regardless of how old they are), and, additionally, for some user-generated content stored on remote servers. 269
4. Protections Under State Law

In addition to the protections provided by federal law and under the U.S. Constitution, several state legislatures have taken steps to protect electronic communications. State constitutions also have a role to play. For example, the New Jersey Supreme Court has held that the New Jersey Constitution provides broader protection in some cases than the Fourth Amendment of the U.S. Constitution.

In State v. Reid, the New Jersey Supreme Court found that under the state constitution individuals have reasonable expectations of privacy in their Internet Protocol (IP) addresses, and law enforcement may not compel disclosure of the subscriber information linked to an IP address from an ISP without a grand jury subpoena. In Reid, Shirley Reid's employer discovered that someone had changed the company's shipping information on a supplier's website in order to create a disruption and suspected Reid might have been responsible. The supplier provided the police with the IP address used to make the modification, which the police used to trace back to the ISP that controlled that IP address. The police subpoenaed all information pertaining to the IP address recorded at the time the modification was made and discovered that Reid had been assigned that IP address at the time the shipping information was changed.

The court noted that the language of the Fourth Amendment is nearly identical to its counterpart language in the New Jersey Constitution. The court also acknowledged that, after the Supreme Court's decisions in Miller and Smith, an individual cannot challenge the disclosure of this information under the Fourth Amendment. However, the court held that the New Jersey Constitution offers broader protections than the U.S. Constitution. In particular, the court relied on the fact that the state constitution had been interpreted to protect disclosure of telephone numbers dialed or bank records even though such disclosure is permissible under the U.S. Constitution.

The court found that subscriber information is analogous to bank records and phone numbers dialed because, in all of these situations, individuals are forced to turn the information in question over to the providers as part of using the service. The court noted that “when users surf the Web from the privacy of their homes, they have reason to expect that their actions are confidential.” Even though a decoded IP address does not allow access to the contents of an individual's transactions on the Internet, it still may reveal intimate details about personal affairs, such as where the person shops or in which political organizations he or she is involved. In light of these concerns, the court held that individuals were entitled to the same level of protection for their subscriber information as for phone and banking records.

Several other states also recognize the privacy interest in subscriber information, and Minnesota and Nevada both have enacted statutes prohibiting disclosure of personal subscriber information without consent. No state appears to have legislated to define whether an ISP may monitor an individual's Internet use, but Connecticut and Delaware both prohibit employers from monitoring their employees' Internet and e-mail use without first giving them notice.

While Reid did not consider the level of protection afforded to the contents of e-mail communications, subscriber information is generally afforded less protection than information that reveals the content of an individual's correspondence. The flexibility in construing language nearly identical to that contained in the U.S. Constitution, combined with the recognition of the sensitivity of information that can be culled from these databases, suggests that the contents of electronic communications would almost certainly be protected under the New Jersey Constitution. This approach also casts doubt on the wisdom of the Court's earlier decisions in Smith and Miller and, in particular,
raises questions about whether their reach should be extended to cover electronic communications stored in remote databases.  

*382 II. Different Levels of Protection Afforded by the Stored Communications Act and the Fourth Amendment

Although Congress sought to broadly protect electronic communications with the SCA, it did not give Fourth Amendment-like protections to all electronic communications. Two recent cases that considered the level of constitutional protection afforded to electronic communications have concluded that the messages are protected by the Fourth Amendment irrespective of how long they have been stored. Because § 2703(b) of the SCA permits the government to access electronic communications greater than 180 days old with a showing of less than probable cause, these cases suggest that the statute provides an unconstitutionally low level of protection.

A. The Stored Communications Act in Action

Under the SCA, government agents may only obtain electronic communications less than 180 days old pursuant to a warrant issued by a court with jurisdiction over the offense under investigation. However, § 2703(b) permits law enforcement to obtain documents in storage for more than 180 days with just a subpoena or court order. Under this section, the government does not need to establish probable cause, but must only "offer [] specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." Additionally, the government may delay notifying the individual whose communications are being monitored by up to ninety days.

In Warshak v. United States, law enforcement used the SCA to obtain court orders directing the defendant's ISPs to turn over all of the defendant's messages greater than 180 days old stored on their servers. The order prohibited the providers from informing Warshak about the search and allowed the government to delay notifying Warshak for ninety days. However, where users have reasonable expectations of privacy in messages stored on their ISP's server, these communications are protected under the Fourth Amendment and law enforcement must generally obtain a warrant before they may review them. If these messages are protected under the Fourth Amendment, the provision in § 2703(b) of the SCA that allows access to communications greater than 180 days old, without first demonstrating probable cause and securing a warrant, conflicts with the Constitution's requirements.

B. Applying the Fourth Amendment to Electronic Communications

When applying legal rules to the Internet, Professor Orin Kerr points out that courts and lawyers have two choices: they can either take the perspective of a user and try to draw analogies between “realspace” and cyberspace, or take an external perspective and apply the law to the transactions underlying the network's operation. In the Internet context, the different perspectives may lead to particularly divergent results, because a user may be fully immersed in the network, but have no idea of its inner workings. For example, from a user's perspective, e-mail is the equivalent of postal mail, and should thus be entitled to the same high standard of Fourth Amendment protection. However, from an external perspective, that same message is stored on both the recipient's computer and the sender's computer and may have been transmitted between two different ISPs, either of which may have also retained a copy. From this perspective, Fourth Amendment protections are less clear.
Some early decisions to address the protection afforded to electronic communications placed considerable emphasis on the technical details of how electronic messages are transported and delivered. For example, in United States v. Councilman, the U.S. Court of Appeals for the First Circuit engaged in an in-depth review of how e-mail is transmitted between computers. Although such a highly technical analysis is not required under the Katz test focusing on reasonableness, even courts considering the technical details of how an electronic message is transmitted have found that a third party's limited interaction with a message during delivery does not limit the Fourth Amendment protections.

In Warshak v. United States, a unanimous panel of the U.S. Court of Appeals for the Sixth Circuit held that e-mail messages were protected under the Fourth Amendment in spite of the third-party ISP's limited access. More recently, the U.S. Court of Appeals for the Ninth Circuit concluded in Quon v. Arch Wireless Operating Co. that individuals have reasonable expectations of privacy in their text messages and that those messages are, therefore, also protected by the Fourth Amendment. Additionally, in other analogous areas, courts have found that a third party's limited access to some part of an electronic communication does not eliminate all Fourth Amendment protections, further supporting the decisions in Warshak and Quon. However, these decisions conflict with § 2703(b) of the SCA, which is premised on the concept that electronic communications stored by third parties are not protected under the Fourth Amendment.

1. E-mail: Warshak v. United States

While investigating Steven Warshak and Berkeley Premium Nutraceuticals, Inc.--the company Warshak controlled--for mail and wire fraud, money laundering, and other federal offenses, the government obtained an order from a magistrate judge under § 2703 of the SCA that required Warshak's ISPs to turn over all “electronic communications (not in electronic storage unless greater than 181 days old) that were placed or stored in directories or files owned or controlled by Warshak.” The court issued the orders under seal and prohibited the ISPs from informing Warshak. Over a year after the orders issued, the government finally informed Warshak about the orders.

In addition to challenging the use of the messages as evidence, because the government failed even to comply with the delayed notice provisions contained in the SCA, Warshak also raised a Fourth Amendment challenge to the search of these messages. Writing for a unanimous panel of the Sixth Circuit, Judge Boyce F. Martin, Jr. found that the reasonable expectation of privacy question must “focus on two narrower questions than the general fact that the communication was shared with another.” First, courts need to “identify the party with whom the communication is shared.” Second, courts must consider the precise information conveyed to the party from whom disclosure is sought.

The court recognized that the depositor in Miller and the caller in Smith had assumed the risk that the bank and phone company might disclose the information they had voluntarily conveyed to them. However, the panel concluded that the “assumption of risk” is limited to the information actually conveyed to the provider, which, in the context of a phone conversation, does not include the content of the call. This distinction led the court to hold that the third-party exception only permits the government to compel disclosure of the specific information to which the third party had access. “It cannot, on the other hand, bootstrap an intermediary's limited access to one part of the
communication (e.g. the phone number) to allow it access to another part (the content of the conversation)." 318 Even though the “ISP could access the content of e-mails and phone calls, the privacy expectation in the content of either is not diminished, because there is a societal expectation that the ISP or the phone company will not do so as a matter of course.” 319 Consistent with the third-party doctrine, the court noted there would be no Fourth Amendment violation if the government subpoenaed the recipient of the e-mails. 320 However, here, the government subpoenaed the ISP, which was “not expected to access the content of the documents, much like the phone company in Katz.” 321

Even though the court found that Warshak did have a reasonable expectation of privacy in his e-mails, it did not declare the statute unconstitutional. The court instead issued an injunction prohibiting the government from compelling disclosure of e-mails unless it first obtained a warrant, provided notice to the account holder, and allowed him the same judicial review he would have if subpoenaed. 322 Alternatively, the order allowed the government to simply subpoena the e-mails if it could show “specific, articulable facts, demonstrating that an ISP or other entity has complete access to the e-mails in question and that it actually relies on and utilizes this access in the normal course of business, sufficient to establish that the user has waived his expectation of privacy with respect to that entity.” 323

On rehearing en banc, a majority of the Sixth Circuit found the issue was not fit for judicial review as it was unclear whether the government intended to perform further ex parte review of Warshak's e-mail. 324 The majority also noted that the lack of Fourth Amendment challenges to the SCA since its inception in 1986 further validated the court's decision not to address the Constitutional issue. 325 Except for this reference, the majority did not discuss the panel's earlier conclusions regarding the constitutionality of § 2703 of the SCA. 326 In dissent, Judge Martin remarked that “[i]nstead of reaching the question that is on everyone's mind-- whether or not the delayed notification provision of the Stored Communications Act is constitutional--the majority sidesteps the question.” 327 Expressing his discontent with the majority's decision, Judge Martin went on to speculate, “[I]f I were to tell James Otis and John Adams that a citizen's private correspondence is now potentially subject to ex parte and unannounced searches by the government without a warrant supported by probable cause, what would they say? Probably nothing, they would be left speechless.” 328

Although the panel's initial decision is no longer in force, its reasoning regarding the underlying constitutional issue is still persuasive. Taking an internal perspective and accepting the validity of the Supreme Court's third-party doctrine, the panel recognized that, although Warshak's messages were stored in a commercial ISP's database, the ISP was not a party to the communications and its limited interaction with the communications did not vitiate Warshak's legitimate expectation of privacy in them. 329 Recognizing that Warshak had a reasonable expectation of privacy in the messages would extend Fourth Amendment protections to them and render § 2703 of the SCA unconstitutional.


More recently, in Quon v. Arch Wireless Operating Co., the Ninth Circuit found that city employees have reasonable expectations of privacy in text messages sent from pagers provided by their employers. 330 The city of Ontario, California contracted with Arch Wireless for wireless text messaging services, and distributed pagers to various city employees, including Ontario Police Department Sergeants Jeff Quon and Steve Trujillo. 331 The city lacked an official policy for the pagers but had a general technology policy limiting the use of computer equipment to city-related business. 332 The policy admonished that users “should have no expectation of privacy or confidentiality when using these resources.” 333
Each pager had a monthly character allotment under the contract, and the city's unofficial policy was to refrain from auditing usage so long as the users paid any overages. However, as part of an internal affairs investigation, city officials obtained transcripts of some officers' usage and discovered personal and sexually explicit messages. The officers and the parties with whom they were communicating brought an action challenging the police department's review of their messages under the Fourth Amendment and the SCA.

The district court concluded that “electronic storage” as defined in the SCA included storage after transmission and that to read it more narrowly and find it only covers pretransmission storage would undermine the purpose of the SCA. The court then denied Arch Wireless's motion to dismiss the claim, rejecting the argument that, because the sergeants were not subscribers, they were not users of the system and not entitled to the protections of the SCA.

The district court later granted the defendants' summary judgment motion, finding that Arch Wireless was an RCS under § 2702(a) of the SCA and committed no harm when it released the text message transcripts to its subscriber, the city. However, the district court found that, in light of the informal policy that the officers' pager use would not be monitored if they paid the overage charges, the officers had reasonable expectations of privacy in the messages they sent.

On appeal, the Ninth Circuit affirmed in part, reversed in part, and remanded for further proceedings. The court disagreed with the district court's conclusion that Arch Wireless was acting as an RCS. Although an RCS may release private information with the consent of a subscriber, addressee, or intended recipient, an ECS may only release the information with the consent of the addressee or intended recipient. The court looked at the plain language of the SCA and its “common-sense definitions” and found that Arch Wireless provided the city with electronic communication services and not just remote storage, even though it retained backup copies of the messages city employees transmitted. Concluding that Arch Wireless was acting as an ECS, the court found that it violated the SCA by releasing the messages without consent from either the sender or the intended recipient.

Most relevant for present purposes, the Ninth Circuit affirmed the district court's determination that the users had reasonable expectations of privacy in their text messages and that they were therefore protected by the Fourth Amendment. Even though the official department policy indicated that the officers should not expect any privacy while using the department-supplied technology, the court concluded that because Sergeant Quon had in the past exceeded the character limit and his messages had not been reviewed, the department followed an “informal policy” of not reviewing messages. Because the department did not review the messages, the policy did not foreclose the officer's expectations of privacy.

Similar to the Sixth Circuit's reasoning in the panel decision in Warshak, the court also recognized the distinction between Katz, which offered strong protection for the content of a phone conversation, and Miller, which found there was no protection for telephone numbers dialed, and held that the content of the text messages was protected. The court opined that the fact “[t]hat Arch Wireless may have been able to access the contents of the messages for its own purposes is irrelevant” when determining the scope of the user's privacy. Because the parties “did not expect that Arch Wireless would monitor their text messages, much less turn over the messages to third parties without . . . consent,” Arch Wireless's limited access did not diminish the user's reasonable expectations of privacy. The Court did, however, note that whether an expectation of privacy is reasonable was a “context-sensitive” inquiry and, had Sergeant Quon permitted the department to review his messages, none of the parties to the conversations would have had a reasonable expectation of
privacy. In this case, in spite of the warnings not to expect privacy while using department-supplied technology, because the police department followed a policy of not auditing his messages as long as he paid the overage, the Ninth Circuit agreed that Sergeant Quon had a reasonable expectation of privacy in the text messages.

Quon, like Warshak, recognized the limits of the third-party doctrine and that a user's expectation of privacy was not eliminated merely because a communication was stored on a third party's server. Arch Wireless was expected to provide text messaging services, including storing and transmitting messages, but the parties did not expect that Arch Wireless would review or disclose their private messages. Unlike Hoffa speaking to his associate, Arch Wireless was not a party to the conversations, but merely a storage facility, and the users did not assume the risk that they would disclose their messages.

3. Protection for Other Electronic Information

a. Information Held by, but Not Directed to, Third Parties

As the Supreme Court recognized in Katz, the mere fact that a conversation is shared with another does not eliminate all Fourth Amendment protections. In the electronic communications context, both Quon and the panel opinion in Warshak recognized that individuals have reasonable expectations of privacy in electronic communications, even where the communications pass through third-party intermediaries who could theoretically review the contents of the communications. In this situation, practice and societal expectations indicate that the service providers, like the phone company in Katz, will not review the communications.

However, consistent with Katz's mandate that information voluntarily exposed to the public is not subject to Fourth Amendment protection, several courts have found that an individual does not have a reasonable expectation of privacy in her personal, subscriber information conveyed to an ISP. Law enforcement officers are often aware of the IP address associated with a user engaging in illegal activity online, but must obtain that user's subscriber information from the ISP in order to ascertain the identity of the actual person linked to that IP address. Several courts have held that users do not have legitimate expectations of privacy in this information because they voluntarily conveyed it to their third-party ISP, and it is therefore not protected by the Fourth Amendment. These courts find that this information is akin to the bank records in Miller, which were voluntarily turned over to the third party for its use and hence were not protected by the Fourth Amendment.

Highlighting the difference between information simply made available to a third party and information directed to a third party, some courts have found that pen registers cannot be used to capture post-cut-through dialed digits (PCTDD). Frequently, individuals enter credit card, social security, personal identification, or other numbers into a phone system in response to prompts from an automated system at the other end of the line after a call is connected. These PCTDDs can, in principle, be recorded by pen registers. In considering a request from law enforcement for approval to use such a device, a court noted that although the phone company certainly could view this information if it chose, unlike dialed telephone numbers, which are used to connect a call and may show up on an invoice, this information is not regularly recorded or processed by the phone company. Relying on the Sixth Circuit's panel decision in Warshak, the court also noted that finding no expectation of privacy wherever an intermediary merely has
the potential to access information would eviscerate important Fourth Amendment protections recognized previously by the Supreme Court.  

*391 In addition to finding protection for information held by third parties but not directed to them, some courts have held that individuals maintain reasonable expectations of privacy in historical cell site information recorded by their wireless providers.  

Wireless providers record their users' locations when their phones are active, and, by obtaining an individual's historical cell site information, law enforcement officials can track where an individual has been. Some courts have concluded that, even though cellular providers regularly store this information, users still have reasonable expectations of privacy in it. Even though this information is stored in the provider's database where the provider could access it, one court has recognized that because the provider would not regularly as a matter of course review this information, let alone identify a customer's location to a third party, users still have reasonable expectations of privacy in this information. These holdings go beyond the decisions in Warshak and Quon because the cellular provider is not an intermediary with respect to the historical cell site information, but actually the intended recipient of it. These decisions suggest that information in the possession of others is still private if it is not generally disclosed and appear to conflict with the Supreme Court's earlier decision in Miller. However, both the proposed 2000 amendments to the ECPA and the Constitution Project's proposals advocate adopting Fourth Amendment-like protections for historical location information--just as the courts in these cases have found.

Although it was never the subject of a reported decision, even in the case of telegraph communications--where an operator read and transmitted a message to another operator who received and transcribed it--the public still expected those communications to remain private. Because of the way the system worked, unlike telephone companies or ISPs, who merely have the capability to review communications, here the operators were actually privy to the content of the transmissions. In spite of these technical realities, many individuals still viewed these communications as private and were outraged at the possibility of government or other private individuals reviewing their messages.

b. Information Reviewed by Third Parties

Conversely, an individual may not prevail on a Fourth Amendment challenge where there is evidence demonstrating the provider or some other party did regularly review the information in question. When considering whether an individual has a privacy interest in electronic information on a computer used at work, courts have been heavily influenced by the employer's written policies regulating computer use. For example, in United States v. Mosby, the court found that, even though not enforced, a policy that informed employees that their computer use was not private and was subject to monitoring made any expectations of privacy the employees had unreasonable. In Warshak, the panel recognized that if the government could demonstrate that it was the ISP's practice to review the users' messages, then the third-party doctrine would apply, and the government could access the messages with a subpoena.

In situations where communications are regularly reviewed, and users are aware that their communications are not private, they may not have legitimate expectations of privacy. However, even where an official policy instructs users not to expect privacy, courts still must engage in a fact-based inquiry to determine whether an employee could have a reasonable expectation of privacy in spite of such warnings. In the case of electronic communications, even where a provider's use policy purports to limit an individual's privacy, courts still must consider what actually takes place in order to determine whether an individual's expectation of privacy is legitimate. Where there is no use policy or other evidence demonstrating the third party reviewed the user's communications, as was the case in Quon and Warshak, these...
III. Section 2703 of the Stored Communications Act Is Unconstitutional as Applied

As e-mail and other forms of electronic communications became more widely used, Congress recognized their tremendous importance and grew concerned that the existing statutory and constitutional framework was not robust enough to adequately protect them for two main reasons. 388 First, Congress was concerned about the unpredictability of which expectations of privacy courts would recognize as reasonable and, therefore, sufficient to satisfy the Katz test for determining the scope of Fourth Amendment protections. 389 Second, Congress was unsure how the third-party doctrine that evolved in Fourth Amendment analysis through the Supreme Court's decisions in cases like Hoffa, Smith, and Miller would be applied. 390 However, when considered in light of this precedent, electronic communications are still protected by the Fourth Amendment, as the Warshak and Quon courts recognized. 391

The nature of the technology requires that electronic communications will frequently bounce between several different servers controlled by third parties during transmission, and these third-party servers may create backup or archival copies of messages. 392 However, these intermediaries are not parties to the conversations in the same way that the bank in Miller was, and Quon and Warshak recognize that merely retaining a copy of the message does not bring the communication within the purview of this exception. 393

In this situation, the provider is a fundamental part of the communication process because it delivers the messages, but it is not an intended recipient. 394 The provider's relationship with the message is not akin to the situation in Hoffa, where Hoffa shared information with an associate believing he would keep it confidential. 395 Here, although the provider carries the message, the message is not directed to it.

This distinction between information carried by third parties and information directed to third parties for their use is consistent with the Supreme Court's decision in Smith, holding that individuals do not have reasonable expectations of privacy in the telephone numbers they dial, 394 thereby permitting the government to request copies of a user's call history from the phone company. 396 Dialing information is conveyed directly to the phone company so that it may complete the phone call, and for the purpose of this information, the phone company is the intended recipient and is--like Hoffa's associate--free to disseminate this information to whomever it chooses. 397 However, even though the content of the conversation that takes place after the phone company uses the number dialed to route and connect the call also passes through the phone company's network, it is strongly protected under the Fourth Amendment. 398 This is because the content is not like the phone number dialed and is not conveyed to the phone company for it to use. Additionally, there is a strong societal expectation that the conversation will be kept private. 399

The Supreme Court also recognized this distinction earlier when it considered protections available for postal mail in Ex parte Jackson. 400 Like a telephone call, when an individual deposits a letter in the mail, the Postal Service has full control over the communication. Although postal agents could easily open up letters and read their contents, as was in fact widely done during the colonial period, 401 the Postal Service is not expected to do so, and the contents of letters are strongly protected by the Fourth Amendment. 402 The Postal Service is, however, expected to deliver letters and, in doing so, is expected to read the address and other information written on the exterior. 403 Similar to a phone number,
because the address is directly communicated to the Postal Service for use in delivering the letters, it is not protected by the Fourth Amendment. However, the content of the letter, like the content of the phone call, is not similarly directed and is strongly protected by the Fourth Amendment.

This distinction is equally applicable to e-mail and other electronic communications. Some information, namely the recipient's address, is conveyed to the ISP for its use in routing the message. The ISP is privy to this information and, for Fourth Amendment purposes, is analogous to Hoffa's associate--free to disseminate the information as it wishes. However, like the substance of a telephone conversation or the text of a letter, the contents of e-mail messages are not directed to, nor expected to be read, by ISPs. The ISP in this case is not truly a party to the communication, and the third-party doctrine does not apply as the Sixth Circuit panel concluded in Warshak and the Ninth Circuit suggested in Quon.

Additionally, by analogy to postal mail and telephone conversations, the contents of e-mail messages should also be strongly protected by the Fourth Amendment. As the Court recognized early on in Ex parte Jackson, “The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be.” Electronic communications are similarly “closed” and not expected to be reviewed by the intermediaries merely charged with delivering the messages.

This analysis does not change merely because an ISP may retain backup or archival copies of messages in its database. This storage is fundamentally different from the storage of bank records in Miller because, in that instance, the information had been communicated to the bank for its use. In this situation, the ISP merely has access to the information, but was never an intended recipient of the message. In Miller, the documents were shared with the bank on the assumption that it would not turn the information over to anyone else, and certainly not law enforcement. However, like Jimmy Hoffa, that “misplaced reliance” eliminated the depositor's expectation of privacy in the documents. There is no misplaced reliance in the case of the electronic communications at issue because, unlike the financial instruments in Miller, they are never directed to the provider. As such, users still maintain reasonable expectations of privacy in their communications even if archival copies are created and stored in the third party's electronic database.

Further bolstering the conclusion that the nature of the third-party service provider's use of, and interaction with, the communications does not work to bring it within the purview of the third-party doctrine is the immense importance of privacy in electronic communications. In Katz, the Supreme Court recognized the tremendous importance of the telephone and corrected its earlier error in Olmstead by giving strong protection to telephone calls. Similarly, in Ex parte Jackson the Court acknowledged the central role of the mail system and, in the face of widespread snooping, gave strong protection to the mails. Although never discussed in a reported judicial opinion, the public even expected privacy in telegraph messages, where the technology required operators to actually read the contents of transmissions. And, in attempting to enact protective legislation, congressional representatives noted the tremendous importance of the telegraph system and the problems that would flow if individuals could not be guaranteed some privacy in using it.

Congress recognized that many of these same problems would exist if electronic communications were not adequately protected and attempted to enact strong protective legislation. However, in the short period since the SCA was enacted, computer use has significantly changed.
decision in Warshak recognize that electronic communications are protected by the Fourth Amendment and that the provision in § 2703 of the SCA that permits the government to access messages greater than 180 days old without first securing a warrant supported by probable cause is unconstitutional. 422 An individual's reasonable expectation of privacy and Fourth Amendment protections do not evaporate over time. Congress recognized that messages less than 180 days old would likely be protected under the Fourth Amendment, 423 and, now that individuals frequently store messages on servers for longer periods of time, the statute should be modified to recognize this.

Furthermore, this provision is also problematic because it allows government actors broad access to all of an individual's electronic communications without any meaningful restriction. 424 This unbridled access would in some cases permit law enforcement to engage in “fishing expeditions,” one of the chief evils against which the framers of the Fourth Amendment sought to guard. 425

At the same time, consistent with Smith and Miller, users do not have legitimate expectations of privacy in information turned over to third parties. 426 Therefore, the provision in § 2703(c)(2) of the SCA that allows government access to subscriber information is consistent with the Supreme Court's Fourth Amendment jurisprudence because this information is *voluntarily turned over to the provider in order to establish an account.* 427 However, particularly where the provider expressly states that it will not review a user's messages, 428 and where Congress itself recognized that mail less than 180 days old is likely protected under the Fourth Amendment, 429 subscriber information is significantly different from communications the provider stored in a database but was never a party to.

As the panel decision in Warshak concluded, because § 2703 of the SCA allows the government to access material protected by the Fourth Amendment without a warrant supported by probable cause, it is unconstitutional. 430 Although this Note argues that, irrespective of legislative action, electronic communications are protected by the Fourth Amendment, until the Supreme Court considers this issue the level of protection remains largely unknown, and lower courts could potentially reach divergent results. In the face of this uncertainty, Congress should revise the SCA to eliminate the distinction between mail greater and less than 180 days old and extend the same, high level of protection to all electronic communications, regardless of how long they have been in storage.

**Conclusion**

Information gleaned from e-mail messages will likely become an increasingly important tool for law enforcement agencies to use in combating crime, and they should be encouraged to rely on it going forward. However, law enforcement may not take advantage of the anomaly that has resulted where, although Congress attempted to legislate to protect electronic communications, evolving uses actually resulted in communications having less protection than is provided by the Constitution. Electronic communications do frequently pass through third parties, but the third parties are not parties to the transmissions. Their minimal interaction does not eliminate the sender or receiver's expectation of privacy in, or Fourth Amendment protections for, the messages. The same requirement that law enforcement obtain a warrant before searching e-mail messages less than 180 days old should also apply to mail greater than 180 days old. Users' expectations of privacy do not disappear over time, and the same rationale that led Congress to conclude that messages less than 180 days old are protected by the Fourth Amendment should be adopted to keep pace with technology and the current practice of storing messages for more than 180 days. Because all electronic messages, regardless of age, are protected by the Fourth Amendment, § 2703(b) of the SCA, which allows law enforcement to access communications greater than 180 days old without a warrant, is unconstitutional.
Footnotes

a1 J.D. Candidate, 2010, Fordham University School of Law; B.E., 2006, Cooper Union. I would like to thank my advisor, Professor Katherine Strandburg, for her insightful comments and feedback and my family and friends for their support and encouragement.


2 See infra Part I.C.

3 See infra Part II.B.

4 U.S. Const. amend. IV.


9 See, e.g., Kyllo v. United States, 533 U.S. 27, 40 (2001) (concluding that the use of a thermal imager to detect heat radiating from a home is a search within the meaning of the Fourth Amendment); California v. Ciraolo, 476 U.S. 207, 215 (1986) (holding that aerial surveillance of a home is not a search in an age “where private and commercial flight in the public airways is routine”); Katz, 389 U.S. at 352-53 (recognizing that telephone conversations are protected under the Fourth Amendment); see also infra Part I.B.

10 Schmerber v. California, 384 U.S. 757, 767 (1966) (finding no Fourth Amendment violation where a police officer directed a physician to draw a blood sample from a person suspected of drunk driving).

11 Boyd v. United States, 116 U.S. 616, 630 (1886) (holding that forcing a criminal defendant to produce incriminating documents is a search within the meaning of the Fourth Amendment).

12 U.S. Const. amend. IV; see, e.g., Maryland v. Dyson, 527 U.S. 465, 466 (1999) (noting that “[t]he Fourth Amendment generally requires police to secure a warrant before conducting a search”). The primary exception to the warrant requirement is for situations involving exigent circumstances where the law enforcement officer does not have time to procure a warrant because of dangerous conditions, possible disappearance of evidence, or other similar concerns. See, e.g., Schmerber, 384 U.S. at 770. For a discussion of practical examples stemming from this exception, see Craig M. Bradley, Two Models of the Fourth Amendment, 83 Mich. L. Rev. 1468, 1473-74 (1985).

13 Writs of assistance were generally used in support of customs and excise investigations and enabled the bearer to search any and all houses he or she suspected might contain probative evidence. See generally William J. Cuddihy, “A Man's House Is His Castle”: New Light on an Old Case, Revs. in Am. Hist., Mar. 1979, at 64, 64-69.

14 See Levy, supra note 8, at 158; Cuddihy, supra note 13, at 64-69.

15 U.S. Const. amend. IV.

16 See Louis Fisher, Congress and the Fourth Amendment, 21 Ga. L. Rev. 107, 115 (1986) (“The spirit and letter of the fourth amendment counselled against the belief that Congress intended to authorize a ‘fishing expedition’ into private papers on the possibility that they might disclose a crime.”). The warrant requirement is not a mere technicality, but strikes the appropriate
balance between the rights of individuals to be free from unreasonable searches and the government's need to uncover probative evidence. See, e.g., Brinegar v. United States, 338 U.S. 160, 176 (1949). Additionally, the Fourth Amendment's exclusionary rule offers strong protections to those whose rights have been violated by barring the government from using any illegally obtained evidence. Mapp v. Ohio, 367 U.S. 643, 657-58 (1961).

See, e.g., Illinois v. Caballes, 543 U.S. 405, 408-09 (2005) (holding that a drug-detecting dog's sniff is not a search).

See, e.g., Rakas v. Illinois, 439 U.S. 128, 148 (1978) (holding that passengers in a car are not entitled to Fourth Amendment protection for search of the car).


See id. at 361 (Harlan, J., concurring).

Id. at 348 (majority opinion).

Id. at 352.

See, e.g., Rakas, 439 U.S. at 151 (Powell, J., concurring).

Id. at 143 & n.12 (majority opinion).

Id.

Id. at 143.


See infra Part I.A.


There is, of course, the possibility that Richard and James's office will not run its own mail server, but will rely on the services provided by a third party ISP.

See infra Part I.A-B.


Id. at 302.

Id.

Id. at 302-03. The Court also relied on its earlier decision in Lopez v. United States, 373 U.S. 427 (1963), which noted that the risk of being "betrayed by an informer or deceived as to the identity of one with whom one deals is probably inherent
in the conditions of human society. It is the kind of risk we necessarily assume whenever we speak.” Id. at 465 (Brennan, J., dissenting).

38 U.S. 293.

See infra notes 136-37 and accompanying text.

See infra Part I.B.1.b.

See infra Part I.B.2.

See infra Part I.A.1.

See infra Part I.A.2.


42 U.S. 735 (1979).

“A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed.” United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1 (1977).

Smith, 442 U.S. at 741-42.

Id. at 742.

Id. at 743.

Id. at 742.

Id. at 744-45.

Id.

See infra Part I.B.2.


See Ex parte Jackson, 96 U.S. 727, 733 (1877); see also United States v. Huie, 593 F.2d 14, 14-15 (5th Cir. 1979) (finding no Fourth Amendment violation in performing a “mail cover” by recording all information on exterior of mail before delivering).

Cf. infra Part I.A.2.

See infra Part II.A-B.

See supra notes 31-33 and accompanying text.

See supra notes 31-33 and accompanying text.

See infra Part III.


Id. at 442.

Id. at 436.

Id. at 437-38.

Id. at 443.

Id. (“The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.”).

Smith v. Maryland, 442 U.S. 735, 744 (1979); supra notes 47-54 and accompanying text.

Miller, 425 U.S. at 442-43.

Id. at 440.

Id. at 442.

Id.

Id.


Id. at 335-36.

Id. at 335.

See id. at 340 (Douglas, J., dissenting).

See id. at 329 (majority opinion).

Id.

See infra notes 257-59 and accompanying text.

See infra notes 251-59 and accompanying text.

United States v. Phibbs, 999 F.2d 1053, 1077-78 (6th Cir. 1993).


United States v. Willis, 759 F.2d 1486, 1498 (11th Cir. 1985).


See, e.g., United States v. Perrine, 518 F.3d 1196, 1204-05 (10th Cir. 2008) (acknowledging that “[e]very federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment’s privacy expectation”).
See Christopher Slobogin, Privacy at Risk 153 (2007). In the context of electronic communications, although third-party intermediaries will sometimes have access to the information, they are generally expected not to freely divulge it. For example, GMail, a popular free e-mail provider, specifically states on their website that they do not read users' e-mail. See Does Google Read My Mail?, http://mail.google.com/support/bin/answer.py?answer=6599&topic=12787 (last visited Aug. 20, 2009).

See Daniel J. Solove, Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 S. Cal. L. Rev. 1083, 1137 (2002) (“Smith and Miller have been extensively criticized throughout the past several decades.... [They] are the new Olmstead and Goldman.”); see also Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 85 (1974) (Douglas, J., dissenting) (“In a sense a person is defined by the checks he writes. By examining them the agents get to know his doctors, lawyers, creditors, political allies, social connections, religious affiliation, educational interests, the papers and magazines he reads, and so on ad infinitum.”). But see generally Kerr, supra note 34 (defending the third-party doctrine).

See Kenneth L. Karst, “The Files”: Legal Controls over the Accuracy and Accessibility of Stored Personal Data, 31 Law & Contemp. Probs. 342, 342-43 (1966). For example, in 1960, First National Bank of Boston began using an underground bunker made of steel-reinforced concrete strong enough to survive a three megaton blast to maintain records. John H. Fenton, Bank Constructs a Bomb Shelter, N.Y. Times, Dec. 2, 1960, at 41. The facility was not designed to store money or valuables--only microfilm and duplicates of original transactions. Id.


For example, in the wake of the September 11 terrorist attacks, the Department of Defense began the Total Information Awareness Project (T.I.A.) to help anticipate and stop terrorist attacks based on information culled from databases. See Jeffrey Rosen, The Year in Ideas: Total Information Awareness, N.Y. Times, Dec. 15, 2002, at E65; American Civil Liberties Union, Q&A on the Pentagon's “Total Information Awareness” Program (Apr. 20, 2003), http://www.aclu.org/privacy/spying/15578res20030420.html. However, just a few years later, in response to concerns that aggregating all this information posed a threat to personal privacy, Congress halted the project. Adam Clymer, Congress Agrees To Bar Pentagon from Terror Watch of Americans, N.Y. Times, Feb. 12, 2003, at A1.


Id. at 757.

Id. at 762-63, 767 (noting there is a “privacy interest inherent in the nondisclosure of certain information even where the information may have been at one time public”).

Id. at 763.

Id. at 770 (quoting William H. Rehnquist, Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement?, Nelson Timothy Stephens Lecture at the University of Kansas Law School, (Sept. 26-27, 1974).

101 See supra notes 49-58 and accompanying text.


103 For example, see Scott Turow, Scalia the Civil Libertarian?, N.Y. Times Mag., Nov. 26, 2006, at 22. Turow notes that “[t]o Scalia, the Bill of Rights means exactly what it did in 1791, no more, no less. The needs of an evolving society, he says, should be addressed by legislation rather than the courts.” Id.

104 Kyllo, 533 U.S. at 35-36 (rejecting a mechanical interpretation of the Fourth Amendment).

105 See infra Part I.B.1-2.

106 See infra Part I.B.3.

107 See supra note 104 and accompanying text.


109 See infra Part I.B.1.b.

110 277 U.S. 438 (1928).

111 Id. at 456; see also Mabel Walker Willebrandt, The Inside of Prohibition, N.Y. Times, Aug. 19, 1929, at 14.

112 Olmstead, 277 U.S. at 464.

113 Id. at 465.

114 Id. at 472 (Brandeis, J., dissenting).

115 Id. at 474.

116 See, e.g., United States v. Nardone, 106 F.2d 41, 43-44 (2d Cir. 1939) (relying on Olmstead and approving law enforcement use of wiretaps); Valli v. United States, 94 F.2d 687, 691 (1st Cir. 1938) (same).


120 Id. at 348.

121 See id. For a more detailed description of the factual underpinnings, see Katz v. United States, 369 F.2d 130, 131-32 (9th Cir. 1966).

122 Katz, 389 U.S. at 353. The Court went on to note that “the underpinnings of Olmstead and Goldman have been so eroded by our subsequent decisions that the ‘trespass’ doctrine there enunciated can no longer be regarded as controlling.” Id.
123 Id. at 352.
124 Id.
125 Id.
126 See Solove, supra note 90, at 1086 (describing Olmstead as “a relic of the past, a long discredited decision”); see also Fred P. Graham, High Court Eases Curbs on Bugging; Adds Safeguard, N.Y. Times, Dec. 19, 1967, at 1.
127 Solove, supra note 90, at 1086.
128 See Katz, 389 U.S. at 361 (Harlan, J., concurring); see also supra notes 18-20 and accompanying text.
129 See supra notes 49-58 and accompanying text. Similarly, even though § 605 of the Wiretap Act was not successful in limiting government eavesdropping, it recognized the importance of restricting private wiretapping. See supra note 117.
131 Compare Katz, 389 U.S. at 352 (holding that the contents of telephone conversations are protected under the Fourth Amendment), with Smith v. Maryland, 442 U.S. 735, 743-44 (1979) (concluding that the telephone numbers an individual dials are not protected under the Fourth Amendment because they are conveyed to the third-party telephone company).
132 Cf. supra notes 49-54 and accompanying text. This result does not change even though the phone company has the technological sophistication to, and could quite easily, eavesdrop on the phone conversation. See supra note 45 and accompanying text. In the mid-1990s, however, several circuit courts held that individuals did not have reasonable expectations of privacy in the contents of conversations made using cordless telephones. See, e.g., United States v. Smith, 978 F.2d 171, 180 (5th Cir. 1992); Tyler v. Berodt, 877 F.2d 705, 706-07 (8th Cir. 1989). Early cordless telephones used radio frequencies to communicate and conversations could easily be intercepted by third parties within range. See Brad Graham & Kathy McGowan, 101 Spy Gadgets for the Evil Genius 165-66 (2006); see also Smith, 978 F.2d at 178. These courts considered the details of how the technology worked and found that, because the cordless telephone systems could be easily intercepted, it was not reasonable for the user to expect privacy. See Smith, 978 F.2d at 180. Surprisingly, although the court noted that the materials to tap a regular phone could be readily purchased for under twenty-five dollars, they did not find that this reduced an individual’s expectation of privacy in wired communications. Id. at 179 n.10.
133 See infra notes 251-54 and accompanying text.
134 See supra notes 129-32 and accompanying text.
135 96 U.S. 727 (1877).
136 Id. at 733.
137 Id.
For example, Benjamin Franklin was in charge of the colonial mails and required all of his employees to swear an oath not to open the mail. Smith, supra note 138, at 49; David J. Seipp, The Right to Privacy in American History 13 (Harvard Univ., Working Paper No. W-77-5, 1977).

Smith, supra note 138, at 50-51; see also Seipp, supra note 139, at 12-24.


Smith, supra note 138, at 50-51.

Ex parte Jackson, 96 U.S. 727, 733 (1877).

See Solove, supra note 138, at 1143.

Smith, supra note 138, at 51-52 (citing Joseph Story, Commentaries on Equity Jurisprudence 221 (2d ed. 1830)).

Id. at 51-52.

Ex parte Jackson, 96 U.S. at 732-33; see also United States v. Huie, 593 F.2d 14, 14-15 (5th Cir. 1979) (holding that performing a “mail cover” and recording all information on exterior of mail before delivering does not violate the Fourth Amendment).

Ex parte Jackson, 96 U.S. at 733.

Cf. supra note 29 and accompanying text (describing Katz's holding that what a person voluntarily exposes to the public view is not protected by the Fourth Amendment).

See Ex parte Jackson, 96 U.S. at 733.

See supra notes 50-54 and accompanying text.

See supra note 147 and accompanying text.

See supra note 137 and accompanying text; cf. supra notes 138-46 and accompanying text.

See infra notes 161-63 and accompanying text.


See infra notes 161-63 and accompanying text.

See infra notes 167-88 and accompanying text.


See id.; see also Over Land and Ocean, N.Y. Times, May 17, 1896, at 8 (describing the development of the worldwide telegraph network and the speed at which messages can be transmitted using the telegraph).

See generally Coe, supra note 155.

See id.; see also, e.g., Peterson v. W. Union Tel. Co., 74 N.W. 1022, 1022 (Minn. 1898) (describing the process of sending a telegraph); Pegram v. W. Union Tel. Co., 2 S.E. 256, 257-58 (N.C. 1887).
See Coe, supra note 155, at 70-71 (describing a particularly capable operator who was able to remember several minutes of transmitted messages while sharpening a pencil before transcribing); see also Peterson, 74 N.W. at 1022. Additionally, telegraphy students would frequently practice by listening to the wires at the local telegraph office. Coe, supra note 155, at 107.

See Coe, supra note 155, at 116.

See Seipp, supra note 139, at 46.

See id.

See id. at 47.

See, e.g., Secrets of the Telegraph, N.Y. Times, June 24, 1876, at 4.


See, e.g., Secrets of the Telegraph, supra, note 167.

Western Union Telegraph Company, Rules, Regulations, and Instructions 55 (Cleveland 1866).

See Seipp, supra note 139, at 48-50.


Id.; The Investigating Committees, N.Y. Times, Dec. 13, 1876, at 4; see also Seipp, supra note 139, at 51-52.

Seipp, supra note 139, at 53. Currently, Internet companies are also considering reducing the amount of time they store personally identifiable information. For example, Yahoo! used to keep search logs for thirteen months but now only retains some personally identifiable information for ninety days. See Press Release, Yahoo! Inc., Yahoo! Sets New Industry Privacy Standard with Data Retention Policy (Dec. 17, 2008), http://yhoo.client.shareholder.com/press/releasedetail.cfm?ReleaseID=354703; see also Miguel Helft, Yahoo Puts New Limits on Keeping User Data, N.Y. Times, Dec. 18, 2008, at B3.

Seipp, supra note 139, at 53.

Id. at 54.

Thomas M. Cooley, Inviolability of Telegraphic Correspondence, 27 Am. L. Reg. 65, 71 (1879); see also Seipp, supra note 139, at 55.

Cooley, supra note 179, at 71.

Id.

Id. at 73. Judge Cooley remarked, “[i]f the [telegraph] operator can be compelled to produce them, then on the same reasons a postmaster may be brought into court and compelled to produce the undelivered postal cards for examination.” Id. at 77.

Cf. supra notes 161-62 and accompanying text.

185. Seipp, supra note 139, at 58.

186. Id. at 58-59; see In re Storror, 63 F. 564, 567-68 (N.D. Cal. 1894); United States v. Hunter, 15 F. 712, 714-15 (N.D. Miss. 1882); W. Union Tel. Co. v. Bierhaus, 36 N.E. 161, 162-63 (Ind. App. 1894); Ex parte Jaynes, 12 P. 117, 117 (Cal. 1886); Ex parte Brown, 72 Mo. 83, 95 (1880); Nat'l Bank v. Nat'l Bank, 7 W. Va. 544, 546-47 (1874); State v. Litchfield, 58 Me. 267, 269-70 (1870).

187. Seipp, supra note 139, at 93-94; see also Alan F. Westin, Privacy and Freedom 337 (1967).

188. E.g., Woods & Bradley, 7 N.W. at 484-85; Ex parte Brown, 7 Mo. App. 484, 491-92 (1879); Seipp, supra note 139, at 94.

189. Currently, no reported decisions appear to consider the use of telegraph messages in criminal prosecutions. Given the state of the art, it is unlikely this issue will ever be resolved. Cf. Anuj C. Desai, Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy, 60 Stan. L. Rev. 553, 583-84 (2007).

190. See supra notes 20, 23-28 and accompanying text.

191. See supra notes 167-70 and accompanying text.

192. See supra note 179 and accompanying text.

193. See supra note 31.

194. The Office of Technology Assessment was a nonpartisan agency established in 1972 to assist Congress with complex and highly technical issues that affect society. The office closed in September 1995 when Congress withdrew funding. See The OTA Legacy, http://www.princeton.edu/~ota/ (last visited Aug. 20, 2009).


198. Id. at 29.

199. Id. at 10.


201. See infra notes 216-19 and accompanying text.

202. OTA Report, supra note 197, at 3. The report noted that, although the Katz standard for determining the extent of Fourth Amendment protections is broad and flexible, reasonable expectation of privacy is “nebulous” and predicting its meaning in new contexts is difficult. Id. at 17-18.

203. See id. at 45-46.
PROTECTIONS FOR ELECTRONIC COMMUNICATIONS:..., 78 Fordham L. Rev. 349

204 See id. at 51; cf. notes 179-82 and accompanying text.

205 See OTA Report, supra note 197, at 51; see also supra notes 136-37, 147-48 and accompanying text.

206 See OTA Report, supra note 197, at 48-49.

207 See id. at 48-50. Although the report recognized the limited protection for records stored by third parties after Miller, it did not find that it worked to reduce an individual's expectation of privacy in her electronic communications. See id. at 50; cf. supra notes 65-75.

208 See OTA Report, supra note 197, at 49.

209 See id. at 50.

210 See id.

211 See id.; Slobogin, supra note 89, at 153; see also supra Part I.A.2.

212 See OTA Report, supra note 197, at 51-52.

213 See id. at 50; cf. supra notes 12-16 and accompanying text.

214 See OTA Report, supra note 197, at 51; cf. Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting) (anticipating technology would evolve to permit “the Government, without removing papers from secret drawers, [to] reproduce them in court”).

215 See OTA Report, supra note 197, at 51.


217 Id. at 2.

218 Id. at 18 (statement of Sen. Leahy, Vice Chairman S. Select Comm. on Intelligence).

219 Id.


221 Id. at 14,886.

222 Id. Senator Leahy worked with Representative Kastenmeier to craft the bill and, recognizing the importance of protecting communications, noted that “the law must advance with the technology to ensure the continued vitality of the fourth amendment.” S. Rep. No. 99-541, at 5 (1986), as reprinted in 1986 U.S.C.C.A.N. 3555, 3559.

223 See Kerr, supra note 200, at 1214-15.

224 See 132 Cong. Rec. 14,886 (statement of Rep. Kastenmeier); New Law To Protect Computer Data Sought, supra note 194; Houses Approves Privacy Measure To Help Electronic Communications, Boston Globe, Oct. 3, 1986, at 71. However, some commentators writing shortly after the bill was enacted noted that the protection accorded was not as broad as it appeared at first glance. See, e.g., Robert Corn, New Law Offers Easy Listening, The Nation, Dec. 20, 1986, at 696.

225 See supra notes 217-19 and accompanying text.

The most significant changes were caused by the USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of 18 U.S.C.), but this did not modify the protections afforded to electronic communications at issue in this Note.


Id. §§ 2701-12.

Id. §§ 3121-27.

Most circuit courts to address this issue found that in order for the Wiretap Act to apply, the communication must be intercepted contemporaneously with transmission. See Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2004); Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002). But see United States v. Councilman, 418 F.3d 67, 79 (1st Cir. 2005) (en banc). In United States v. Councilman, the SCA was arguably inapplicable because the e-mail had been intercepted by the user's ISP and fell within the statutory exemption. 418 F.3d at 81. Sitting en banc, the U.S. Court of Appeals for the First Circuit concluded that Congress intended “electronic communication” to be defined broadly to cover transient electronic storage and the interception of e-mail in such storage. Id. at 85.

Kerr, supra note 200, at 1208. Kerr also notes that “[t]he uncertainty has made it difficult for legislators to legislate in the field, reporters to report about it, and scholars to offer scholarly guidance in this very important area of law.” Id.


Id. § 2711(2). For example, a provider that allows users to upload files for remote storage would be an RCS under the statute. See Kerr, supra note 200, at 1216.

See S. Rep. No. 99-541, at 3, as reprinted in 1986 U.S.C.C.A.N. at 3557. Although increasingly sophisticated computers have decreased the need for consumers to rely on external sites for data processing and storage, many have begun to once again store records on remote servers and are increasingly using “cloud computers” for processing because of their convenience. See, e.g., Let it Rise, The Economist, Oct. 25, 2008, at 1, 1-2.

See Kerr, supra note 200, 1216-17.


Id. § 2703(b)(1)(B).

Id. § 2703(d). The court may quash or modify the order on motion from the provider if the “records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.” Id.

Id. § 2703(b)(1)(B).

Id. § 2705(a); see also id. § 2705(a)(2) (defining “adverse result”).
PROTECTIONS FOR ELECTRONIC COMMUNICATIONS:..., 78 Fordham L. Rev. 349

244  Id. § 2703(b)(1)(A).
245  Id. § 2703(c)(2).
247  H.R. Rep. No. 99-647, at 68. This does not appear to account for the fact that the record keeper was not the intended recipient of the message and probably did not look at the records.
248  See Mulligan supra, note 31, at 1584.
249  See id. at 1584-85.
250  See 18 U.S.C. § 2703(b); see also supra note 239 and accompanying text. While internally consistent, this does not explain why remotely stored records are afforded less protection than electronic records stored on premises. Cf., e.g., United States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Cir. 2007) (finding legitimate expectation of privacy in personal computer in dorm room connected to university network); United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007) (discussing privacy interest in personal computer).
254  See id. at 5.
255  See id. at 7.
256  See id. This survey is not immediately applicable to determining whether a search is reasonable under the Fourth Amendment because the respondents would likely factor in whether they had any potentially incriminating information in their accounts when assessing how concerned they, personally, would be if law enforcement were allowed to access their accounts. However, for a more detailed discussion of societal expectations of privacy, see Slobogin, supra note 89.
257  This was nearly five hundred times the space provided on comparable free services at the time. See David Pogue, What Big Brother? Gmail from Google Wins a Fan, Despite Its Ads Review, Int'l Herald Trib., May 15, 2004, at 16; Katie Hafner, In Google We Trust? When the Subject Is E-mail, Maybe Not, N.Y. Times, Apr. 8, 2004, at G1.
259  Pogue, supra note 257 (noting “[o]ne gigabyte changes everything”); Hafner, supra note 257.


H.R. 5018.


Cf., e.g., supra notes 259-60 and accompanying text.


945 A.2d 26 (N.J. 2008).

Id. at 28.

Id. at 29.

Id.

Id. at 29-30. IP addresses are unique addresses assigned to each computer connected to the Internet. Most individuals connect to the Internet through an ISP that is assigned a fixed range of IP addresses to distribute to its users. It is possible to look up which ISP a particular IP address belongs to on a public service, but generally impossible to determine the user with which a particular IP address is associated without contacting the ISP. See, e.g., United States v. Carter, 549 F. Supp. 2d 1257, 1262-63 (D. Nev. 2008); Reid, 945 A.2d at 29-30.

Reid, 945 A.2d at 31-32.

Id. (collecting cases).

Id. at 32 (citing State v. McAllister, 875 A.2d 866 (N.J. 2005) (bank records); State v. Hunt, 450 A.2d 952 (N.J. 1982) (dialed telephone numbers)); cf. supra notes 49, 65 and accompanying text.

Reid, 945 A.2d at 33.

Id.

Id. (citing Daniel J. Solove, The Future of Internet Surveillance Law, 72 Geo. Wash. L. Rev. 1264, 1287 (2004)).

Id. at 33-34.


Cf., e.g., supra notes 129-32, 151-53 and accompanying text.
But see generally Kerr, supra note 34 (advocating for retaining the broad third-party doctrine).


Id. § 2703(b).

Id. § 2703(d).

Id. § 2705.

490 F.3d 455, 460 (6th Cir. 2007), vacated en banc, 532 F.3d 521 (6th Cir. 2008) (finding claim was not ripe for judicial review).

Id. at 460.

Id.

Id. See supra notes 12-20 and accompanying text.

Cf. 18 U.S.C. §§ 2703(a)-(b).


Id. at 362.

Id. at 365-66; cf. Cooley, supra note 179, at 73 (drawing an analogy between telegrams and postal mail).


See, e.g., Saul Hansell, You've Got Mail (and Court Says Others Can Read It), N.Y. Times, July 6, 2004, at C1.

418 F.3d 67 (1st Cir. 2005).

See id. at 69-70.


490 F.3d 455, 460 (6th Cir. 2007), vacated en banc, 532 F.3d 521 (6th Cir. 2008) (finding claim was not ripe for judicial determination); see infra Part II.B.1.

529 F.3d 892 (9th Cir. 2008).

Id. at 903; see infra Part II.B.2.

See infra Part II.B.3.

Warshak, 490 F.3d at 460.

Id. Identical orders were presented to NuVox Communications and Yahoo!, where Warshak held e-mail accounts. Id.

Id. at 460-61.

Id. at 461.

Id. at 470.

Id.

315 *Warshak*, 490 F.3d at 470.

316 Id. at 471; see also *Katz v. United States*, 389 U.S. 347, 353 (1967).

317 *Warshak*, 490 F.3d at 471.

318 Id.

319 Id.; see also supra note 132 and accompanying text.

320 *Warshak*, 490 F.3d at 471.

321 Id.; cf. supra note 261 and accompanying text.

322 *Warshak*, 490 F.3d at 475-76.

323 Id. at 476.

324 *Warshak v. United States*, 532 F.3d 521, 526 (6th Cir. 2008) (en banc).

325 Id. at 531.

326 See id. at 533.

327 Id. at 535 (Martin, J., dissenting).

328 Id. at 538.

329 See supra notes 317-22 and accompanying text.

330 *529 F.3d 892, 903 (9th Cir. 2008)*. A similar issue appeared before the U.S. Court of Appeals for the Ninth Circuit several months before *Quon* in *United States v. McCreary*, No. 05-10818, 2008 WL 399148, at *1 (9th Cir. Feb. 12, 2008). The defendant in McCreary challenged the government's use of § 2703 of the SCA to obtain transcripts of text messages he sent. Id. However, the court found there was substantial independent evidence of McCreary's guilt and did not reach the constitutional issue. Id.

331 *Quon*, 529 F.3d at 895.

332 Id. at 896.

333 Id. (quoting the City of Ontario Computer Usage, Internet and E-Mail Policy).

334 Id. at 897.

335 Id. at 898.

336 Id.


339 Id. at 1209-10.
Quon, 529 F.3d at 899. The district court then held a jury trial on the officers' intent in reviewing the messages to determine if the review was reasonable, and the jury concluded it was, absolving the police department of liability. Id.

Id. at 911.

Id. at 902-03.

Id. at 900.

Id. at 900-01. The Ninth Circuit also reached a similar result when it found that a provider of e-mail services was an ECS even though it retained e-mails for backup protection. See Theofel v. Farey-Jones, 359 F.3d 1066, 1070 (9th Cir. 2004).

Quon, 529 F.3d at 903.

Id. at 904.

Id. at 907; see also, e.g., Haynes v. Attorney Gen., No. 03-4209, 2005 WL 2704956, at *4 (D. Kan. Aug. 26, 2005) (discussing fact-specific inquiry to determine whether employee had legitimate expectation of privacy and collecting cases).


Quon, 529 F.3d at 904-05. The Court also noted that there was no meaningful difference between the text messages at issue and the e-mail messages at issue in United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008), where the Ninth Circuit concluded that there was no privacy in the to/from address of e-mail messages because users should be aware that information is available to ISPs for routing. Quon, 529 F.3d at 904-05.

Id. at 905.

Id. at 906.

Id. This is similar to the panel's decision in Warshak, which found that the government may be able to access the messages from the ISP with just a court order or subpoena if the ISP had a practice of reviewing the messages. See Warshak v. United States, 490 F.3d 455, 475-76 (6th Cir. 2007), vacated en banc, 532 F.3d 521 (6th Cir. 2008).

Quon, 529 F.3d at 906. The court also rejected the police department's argument that Sergeant Quon lacked a reasonable expectation of privacy because the California Public Records Act, Cal. Gov't Code § 6253 (West 2008), makes public records open to inspection by the public. Quon, 529 F.3d at 907.

See supra Part II.B.1-2.

See Quon, 529 F.3d at 905-06.


See supra Part II.A-B.

See supra Part II.A-B.

Katz, 389 U.S. at 351.

PROTECTIONS FOR ELECTRONIC COMMUNICATIONS:..., 78 Fordham L. Rev. 349

363 See supra note 274 and accompanying text.

364 For example, in United States v. Perrine, 518 F.3d 1196 (10th Cir. 2008), the government was able to locate an individual distributing pornography in an Internet chat room by tracing the user's IP address back to his ISP and requiring the ISP to disclose the user's true identity and address. Id. at 1199-200.

365 See, e.g., id. at 1204-05 (collecting cases). But cf. supra notes 270-81 and accompanying text.


368 515 F. Supp. 2d at 336.

369 Id. at 337.

370 Id. at 337-38. The court noted that even though it is not their usual practice, because the telephone company has the ability to listen in to phone conversations, only considering this factor would eliminate the Fourth Amendment protections for telephone calls that the U.S. Supreme Court expressly noted existed in Katz. Id.; see Katz v. United States, 389 U.S. 347, 353 (1967).

371 See, e.g., In re U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 612 (W.D. Pa. 2008); In re Applications of the U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d) to Disclose Subscriber Info. and Historical Cell Site Info. for Mobile Identification Nos.: (XXX) XXX-AAAA, (XXX) XXX-BBBB, (XXX) XXX-CCCC, 509 F. Supp. 2d 64, 74 (D. Mass. 2007).


373 See, e.g., In re U.S. for an Order, 534 F. Supp. 2d at 612; In re Applications of the U.S. for Orders, 509 F. Supp. 2d at 74-75.

374 509 F. Supp. 2d at 74 & n.6.

375 See supra Part I.A.2.

376 See supra notes 266-69 and accompanying text.

377 See supra Part I.B.3.

378 See Coe, supra note 155, at 105-22; see also, e.g., Peterson v. W. Union Tel. Co., 74 N.W. 1022, 1022 (Minn. 1898) (describing the process of sending a telegraph).

379 See supra notes 167-72 and accompanying text.


381 2008 WL 2961316.

382 Id. at *5. However, in United States v. Long, 64 M.J. 57 (C.A.A.F. 2006), the use policy did not clearly indicate that employees should not expect privacy, and the court found that the other circumstances surrounding the use, including regularly changing passwords, contributed to a finding that the defendant did have an objectively reasonable expectation of privacy in the system.

383 See Warshak v. United States, 490 F.3d 455, 475-76 (6th Cir. 2007), vacated en banc, 532 F.3d 521 (6th Cir. 2008) (finding claim was not ripe for judicial determination).

384 E.g., Haynes, 2005 WL 2704956, at *4 (finding no expectation of privacy based on “splash screen” that warned “that information flowing through or stored on the computer could not be considered confidential”).

385 E.g., Mosby, 2008 WL 2961316, at *5.

386 E.g., Haynes, 2005 WL 2704956, at *4.

387 See supra Part II.B.1-2.

388 See supra Part I.C.1.

389 See supra notes 20, 23-28, 200, 206 and accompanying text.

390 See supra Part I.A.

391 See supra Part II.B.1-2.

392 See supra notes 31-33 and accompanying text. In Quon, for example, the provider retained copies of all the text messages it carried. See supra note 335 and accompanying text.

393 Supra notes 315-22, 350-56 and accompanying text.

394 See supra notes 31-33, 81 and accompanying text.


396 See supra Part I.A.1.

397 Providers and customers are, of course, free to contract for greater protections and require that the phone company not freely disclose this information. Additionally, although not protected under the Fourth Amendment to the U.S. Constitution, the analogous provision in the New Jersey State Constitution has been interpreted to cover this information. See supra notes 275-81 and accompanying text.

398 See supra notes 123-24 and accompanying text.

399 See supra notes 129-32 and accompanying text.

400 See supra Part I.B.2.

401 See supra notes 138-41 and accompanying text.

402 See supra notes 136-37 and accompanying text.

403 See supra notes 147-49 and accompanying text.

404 See supra notes 129-32, 147-49 and accompanying text.

405 See supra notes 136-37 and accompanying text.

406 See supra note 31.
Additional restrictions on disclosure can be enforced contractually.

See supra notes 31-33, 81 and accompanying text.

Supra notes 315-22, 350-56 and accompanying text.

See supra Part I.B.1.b, I.B.2. Similarly, while considering the level of protection that should be afforded to telegrams, Judge Thomas M. Cooley remarked on the analogy between telegrams and postal mail, noting that the two types of communication should be similarly protected by the Fourth Amendment. See supra notes 179-83 and accompanying text.

Ex parte Jackson, 96 U.S. 727, 733 (1877).

Cf. supra notes 70-75 and accompanying text.

See supra notes 70-75 and accompanying text.

See supra notes 35-38, 70-75 and accompanying text.

See, e.g., supra notes 216-19 and accompanying text.

See supra notes 126-27 and accompanying text.

See supra notes 143-46 and accompanying text.

See supra notes 160-62, 191-93 and accompanying text.

See supra notes 180-81 and accompanying text.

See supra Part I.C.1.

See supra Part I.C.3.

See supra Part II.B.1-2.

See supra notes 246-50 and accompanying text.

See generally supra Part I.C.2.

Cf. supra notes 14-16 and accompanying text.

See supra Part I.A; supra note 245 and accompanying text.

See supra Part I.A.2; but cf. supra notes 275-81 and accompanying text.

See supra note 81 and accompanying text.

See supra notes 246-50 and accompanying text.

See supra notes 322-24 and accompanying text.

78 FDMLR 349
To amend title 18, United States Code, with respect to the interception of certain communications, other forms of surveillance, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “Electronic Communications Privacy Act of 1986”.

TITLE I—INTERCEPTION OF COMMUNICATIONS AND RELATED MATTERS

SEC. 101. FEDERAL PENALTIES FOR THE INTERCEPTION OF COMMUNICATIONS.

(a) DEFINITIONS.—(1) Section 2510(1) of title 18, United States Code, is amended—

(A) by striking out “any communication” and inserting “any aural transfer” in lieu thereof;

(B) by inserting “(including the use of such connection in a switching station)” after “reception”;

(C) by striking out “as a common carrier” and

(D) by inserting before the semicolon at the end the following:

“or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication, but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit”.

(2) Section 2510(2) of title 18, United States Code, is amended by inserting before the semicolon at the end the following: “, but such term does not include any electronic communication”.

(3) Section 2510(4) of title 18, United States Code, is amended—

(A) by inserting “or other” after “aural”; and

(B) by inserting “electronic,” after “wire”.

(4) Section 2510(5) of title 18, United States Code, is amended in clause (a)(i) by inserting before the semicolon the following: “or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business”.

(5) Section 2510(8) of title 18, United States Code, is amended by striking out “identity of the parties to such communication or the existence”.

(6) Section 2510 of title 18, United States Code, is amended—

(A) by striking out “and” at the end of paragraph (10);

(B) by striking out the period at the end of paragraph (11) and inserting a semicolon in lieu thereof; and

(C) by adding at the end the following:

“(12) ‘electronic communication’ means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any
nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

(A) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;

(B) any wire or oral communication;

(C) any communication made through a tone-only paging device; or

(D) any communication from a tracking device (as defined in section 3117 of this title);

(13) 'user' means any person or entity who—

(A) uses an electronic communication service; and

(B) is duly authorized by the provider of such service to engage in such use;

(14) 'electronic communications system' means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

(15) 'electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications;

(16) 'readily accessible to the general public' means, with respect to a radio communication, that such communication is not—

(A) scrambled or encrypted;

(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

(17) 'electronic storage' means—

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication; and

(18) 'aural transfer' means a transfer containing the human voice at any point between and including the point of origin and the point of reception.

(b) EXCEPTIONS WITH RESPECT TO ELECTRONIC COMMUNICATIONS.—

(1) Section 2511(2)(a)(ii) of title 18, United States Code, is amended—
(A) by striking out "violation of this subparagraph by a communication common carrier or an officer, employee, or agent thereof" and inserting in lieu thereof "such disclosure";
(B) by striking out "the carrier" and inserting in lieu thereof "such person"; and
(C) by striking out "an order or certification under this subparagraph" and inserting in lieu thereof "a court order or certification under this chapter".

(2) Section 2511(2)(d) of title 18, United States Code, is amended by striking out "or for the purpose of committing any other injurious act".

(3) Section 2511(2)(f) of title 18, United States Code, is amended—
(A) by inserting "or chapter 121" after "this chapter"; and
(B) by striking out "by the second place it appears and inserting in lieu thereof ", or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing".

(4) Section 2511(2) of title 18, United States Code, is amended by adding at the end the following:
"(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—
"(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;
"(ii) to intercept any radio communication which is transmitted—
"(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;
"(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;
"(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or
"(IV) by any marine or aeronautical communications system;
"(iii) to engage in any conduct which—
"(I) is prohibited by section 633 of the Communications Act of 1934; or
"(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;
"(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or
"(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted."
"(h) It shall not be unlawful under this chapter—

"(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or

"(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service."

(c) TECHNICAL AND CONFORMING AMENDMENTS.—(1) Chapter 119 of title 18, United States Code, is amended—

(A) in each of sections 2510(5), 2510(8), 2510(9)(b), 2510(11), and 2511 through 2519 (except sections 2515, 2516(1) and 2518(10)), by striking out “wire or oral” each place it appears (including in any section heading) and inserting “wire, oral, or electronic” in lieu thereof; and

(B) in section 2511(2)(b), by inserting “or electronic” after “wire”.

(2) The heading of chapter 119 of title 18, United States Code, is amended by inserting “and electronic communications” after “wire”.

(3) The item relating to chapter 119 in the table of chapters at the beginning of part I of title 18 of the United States Code is amended by inserting “and electronic communications” after “Wire”.

(4) Section 2510(5a) of title 18, United States Code, is amended by striking out “communications common carrier” and inserting “provider of wire or electronic communication service” in lieu thereof.

(5) Section 2511(2a) of title 18, United States Code, is amended—

(A) by striking out “any communication common carrier” and inserting “a provider of wire or electronic communication service” in lieu thereof;

(B) by striking out “of the carrier of such communication” and inserting “of the provider of that service” in lieu thereof; and

(C) by striking out “: Provided, That said communication common carriers” and inserting “, except that a provider of wire communication service to the public” in lieu thereof.

(6) Section 2511(2a)(ii) of title 18, United States Code, is amended—

(A) by striking out “communication common carriers” and inserting “providers of wire or electronic communication service” in lieu thereof;

(B) by striking out “communication common carrier” each place it appears and inserting “provider of wire or electronic communication service” in lieu thereof; and

(C) by striking out “if the common carrier” and inserting “if such provider” in lieu thereof.

(7) Section 2512(2a) of title 18, United States Code, is amended—

(A) by striking out “a communications common carrier” the first place it appears and inserting “a provider of wire or electronic communication service” in lieu thereof; and

(B) by striking out “a communications common carrier” the second place it appears and inserting “such a provider” in lieu thereof; and
(C) by striking out "communications common carrier's business" and inserting "business of providing that wire or electronic communication service" in lieu thereof.

(8) Section 2518(4) of title 18, United States Code, is amended—
(A) by striking out "communication common carrier" in both places it appears and inserting "provider of wire or electronic communication service" in lieu thereof; and
(B) by striking out "carrier" and inserting in lieu thereof "service provider".

(d) PENALTIES MODIFICATION.—(1) Section 2511(1) of title 18, United States Code, is amended by striking out "shall be" and all that follows through "or both" and inserting in lieu thereof "shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5)".

(2) Section 2511 of title 18, United States Code, is amended by adding after the material added by section 102 the following:
"(4Xa) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.
(b) If the offense is a first offense under paragraph (a) of this subsection and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) is a radio communication that is not scrambled or encrypted, then—
(i) if the communication is not the radio portion of a cellular telephone communication, a public land mobile radio service communication or a paging service communication, and the conduct is not that described in subsection (5), the offender shall be fined under this title or imprisoned not more than one year, or both; and
(ii) if the communication is the radio portion of a cellular telephone communication, a public land mobile radio service communication or a paging service communication, the offender shall be fined not more than $500.
(c) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted—
(i) to a broadcasting station for purposes of retransmission to the general public; or
(ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,
is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.
(5Xa) If the communication is—
(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or
(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for
a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain,
then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.
"(ii) In an action under this subsection—
"(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and
"(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine.
"(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction.”.
(e) EXCLUSIVITY OF REMEDIES WITH RESPECT TO ELECTRONIC COMMUNICATIONS.—Section 2518(10) of title 18, United States Code, is amended by adding at the end the following:
"(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.”.
(f) STATE OF MIND.—Paragraphs (a), (b), (c), and (d) of subsection (1) of section 2511 of title 18, United States Code, are amended by striking out “willfully” and inserting in lieu thereof “intentionally”.
(2) Subsection (1) of section 2512 of title 18, United States Code, is amended in the matter before paragraph (a) by striking out “willfully” and inserting in lieu thereof “intentionally”.
SEC. 102. REQUIREMENTS FOR CERTAIN DISCLOSURES.
Section 2511 of title 18, United States Code, is amended by adding at the end the following:
"(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.
"(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication—
"(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;
"(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;
"(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or
"(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.”.
SEC. 103. RECOVERY OF CIVIL DAMAGES.
Section 2520 of title 18, United States Code, is amended to read as follows:
"§ 2520. Recovery of civil damages authorized

(a) IN GENERAL.—Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

(b) RELIEF.—In an action under this section, appropriate relief includes—

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c) and punitive damages in appropriate cases; and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) COMPUTATION OF DAMAGES.—(1) In an action under this section, if the conduct in violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the court shall assess damages as follows:

(A) If the person who engaged in that conduct has not previously been enjoined under section 2511(5) and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $50 and not more than $500.

(B) If, on one prior occasion, the person who engaged in that conduct has been enjoined under section 2511(5) or has been found liable in a civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $100 and not more than $1000.

(2) In any other action under this section, the court may assess as damages whichever is the greater of—

(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

(d) DEFENSE.—A good faith reliance on—

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of; is a complete defense against any civil or criminal action brought under this chapter or any other law.

(e) LIMITATION.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation."
SEC. 104. CERTAIN APPROVALS BY JUSTICE DEPARTMENT OFFICIALS.

Section 2516(1) of title 18 of the United States Code is amended by striking out "or any Assistant Attorney General" and inserting in lieu thereof "any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division".

SEC. 105. ADDITION OF OFFENSES TO CRIMES FOR WHICH INTERCEPTION IS AUTHORIZED.

(a) WIRE AND ORAL INTERCEPTIONS.—Section 2516(1) of title 18 of the United States Code is amended—

(1) in paragraph (c)—

(A) by inserting "section 751 (relating to escape)," after "wagering information),";

(B) by striking out "2314" and inserting "2312, 2313, 2314," in lieu thereof;

(C) by inserting "the second section 2320 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities)," after "stolen property),";

(D) by inserting "section 1952A (relating to use of interstate commerce facilities in the commission of murder for hire), section 1952B (relating to violent crimes in aid of racketeering activity)," after "1952 (interstate and foreign travel or transportation in aid of racketeering enterprises),";

(E) by inserting ", section 115 (relating to threatening or retaliating against a Federal official), the section in chapter 65 relating to destruction of an energy facility, and section 1341 (relating to mail fraud)," after "section 1963 (violations with respect to racketeer influenced and corrupt organizations); and

(F) by—

(i) striking out "or" before "section 351" and inserting in lieu thereof a comma; and

(ii) inserting before the semicolon at the end thereof the following: ", section 831 (relating to prohibited transactions involving nuclear materials), section 33 (relating to destruction of motor vehicles or motor vehicle facilities), or section 1992 (relating to wrecking trains);

(2) by striking out "or" at the end of paragraph (g);

(3) by inserting after paragraph (g) the following:

"(h) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain intercepting devices) of this title;

(i) any violation of section 1679a(c)(2) (relating to destruction of a natural gas pipeline) or subsection (i) or (n) of section 1472 (relating to aircraft piracy) of title 49, of the United States Code;

(j) any criminal violation of section 2778 of title 22 (relating to the Arms Export Control Act); or"

"(k) the location of any fugitive from justice from an offense described in this section;"
(4) by redesignating paragraph (h) as paragraph (l); and
(5) in paragraph (a) by—
(A) inserting after “Atomic Energy Act of 1954),” the following: “section 2284 of title 42 of the United States Code
(relating to sabotage of nuclear facilities or fuel);”;
(B) striking out “or” after “(relating to treason),”; and
(C) inserting before the semicolon at the end thereof the following: “chapter 65 (relating to malicious mischief),
chapter 111 (relating to destruction of vessels), or chapter 81 (relating to piracy)”.

(b) INTERCEPTION OF ELECTRONIC COMMUNICATIONS.—Section 2516
of title 18 of the United States Code is amended by adding at the end the following:
“(3) Any attorney for the Government (as such term is defined for
the purposes of the Federal Rules of Criminal Procedure) may
authorize an application to a Federal judge of competent jurisdiction
for, and such judge may grant, in conformity with section 2518 of
this title, an order authorizing or approving the interception of
electronic communications by an investigative or law enforcement
officer having responsibility for the investigation of the offense as to
which the application is made, when such interception may provide
or has provided evidence of any Federal felony.”.

SEC. 106. APPLICATIONS, ORDERS, AND IMPLEMENTATION OF ORDERS.

(a) PLACE OF AUTHORIZED INTERCEPTION.—Section 2518(3) of title
18 of the United States Code is amended by inserting “(and outside
that jurisdiction but within the United States in the case of a mobile
interception device authorized by a Federal court within such juris­
diction)” after “within the territorial jurisdiction of the court in
which the judge is sitting”.

(b) REIMBURSEMENT FOR ASSISTANCE.—Section 2518(4) of title 18 of
the United States Code is amended by striking out “at the prevail­
ing rates” and inserting in lieu thereof “for reasonable expenses
incurred in providing such facilities or assistance”.

(c) COMMENCEMENT OF THIRTY-DAY PERIOD AND POSTPONEMENT OF
MINIMIZATION.—Section 2518(5) of title 18 of the United States Code
is amended—
(1) by inserting after the first sentence the following: “Such
thirty-day period begins on the earlier of the day on which the
investigative or law enforcement officer first begins to conduct
an interception under the order or ten days after the order is
entered.”; and
(2) by adding at the end the following: “In the event the
intercepted communication is in a code or foreign language, and
an expert in that foreign language or code is not reasonably
available during the interception period, minimization may be
accomplished as soon as practicable after such interception. An
interception under this chapter may be conducted in whole or in
part by Government personnel, or by an individual operating
under a contract with the Government, acting under the super­
vision of an investigative or law enforcement officer authorized
to conduct the interception.”.

(d) ALTERNATIVE TO DESIGNATING SPECIFIC FACILITIES FROM WHICH
COMMUNICATIONS ARE TO BE INTERCEPTED.—(1) Section 2518(1)(b)(ii)
of title 18 of the United States Code is amended by inserting “except
as provided in subsection (11),” before “a particular description”.

Hazardous materials.

18 USC 1361 et seq.
18 USC 2271 et seq.
Maritime affairs.
18 USC 1651 et seq.
18 USC app.
(2) Section 2518(3)(d) of title 18 of the United States Code is amended by inserting "except as provided in subsection (11)," before "there is".

(3) Section 2518 of title 18 of the United States Code is amended by adding at the end the following:

"(11) The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if—

"(a) in the case of an application with respect to the interception of an oral communication—

"(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

"(ii) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

"(iii) the judge finds that such specification is not practical; and

"(b) in the case of an application with respect to a wire or electronic communication—

"(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

"(ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing of a purpose, on the part of that person, to thwart interception by changing facilities; and

"(iii) the judge finds that such purpose has been adequately shown.

"(12) An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11) shall not begin until the facilities from which, or the place where, the communication is to be intercepted is ascertained by the person implementing the interception order. A provider of wire or electronic communications service that has received an order as provided for in subsection (11)(b) may move the court to modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the government, shall decide such a motion expeditiously.

(4) Section 2519(1)(b) of title 18, United States Code, is amended by inserting "(including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of this title did not apply by reason of section 2518(11) of this title)" after "applied for".
SEC. 107. INTELLIGENCE ACTIVITIES.

(a) IN GENERAL.—Nothing in this Act or the amendments made by this Act constitutes authority for the conduct of any intelligence activity.

(b) CERTAIN ACTIVITIES UNDER PROCEDURES APPROVED BY THE ATTORNEY GENERAL.—Nothing in chapter 119 or chapter 121 of title 18, United States Code, shall affect the conduct, by officers or employees of the United States Government in accordance with other applicable Federal law, under procedures approved by the Attorney General of activities intended to—

1. intercept encrypted or other official communications of United States executive branch entities or United States Government contractors for communications security purposes;
2. intercept radio communications transmitted between or among foreign powers or agents of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978; or
3. access an electronic communication system used exclusively by a foreign power or agent of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978.

SEC. 108. MOBILE TRACKING DEVICES.

(a) IN GENERAL.—Chapter 205 of title 18, United States Code, is amended by adding at the end the following:

"§ 3117. Mobile tracking devices

(a) IN GENERAL.—If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction.

(b) DEFINITION.—As used in this section, the term 'tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object."

(b) CLERICAL AMENDMENT.—The table of contents at the beginning of chapter 205 of title 18, United States Code, is amended by adding at the end the following:

"3117. Mobile tracking devices."

SEC. 109. WARNING SUBJECT OF SURVEILLANCE.

Section 2232 of title 18, United States Code, is amended—

1. by inserting "(a) PHYSICAL INTERFERENCE WITH SEARCH.—" before "Whoever" the first place it appears;
2. by inserting "(b) NOTICE OF SEARCH.—" before "Whoever" the second place it appears; and
3. by adding at the end the following:

"(c) NOTICE OF CERTAIN ELECTRONIC SURVEILLANCE.—Whoever, having knowledge that a Federal investigative or law enforcement officer has been authorized or has applied for authorization under chapter 119 to intercept a wire, oral, or electronic communication, in order to obstruct, impede, or prevent such interception, gives notice or attempts to give notice of the possible interception to any person shall be fined under this title or imprisoned not more than five years, or both.

Whoever, having knowledge that a Federal officer has been authorized or has applied for authorization to conduct electronic surveillance under the Foreign Intelligence Surveillance Act (50
U.S.C. 1801, et seq.), in order to obstruct, impede, or prevent such activity, gives notice or attempts to give notice of the possible activity to any person shall be fined under this title or imprisoned not more than five years, or both.”.

SEC. 110. INJUNCTIVE REMEDY.

(a) IN GENERAL.—Chapter 119 of title 18, United States Code, is amended by adding at the end the following:

“§ 2521. Injunction against illegal interception

“Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.”.

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 119 of title 18, United States Code, is amended by adding at the end thereof the following:

“2521. Injunction against illegal interception.”.

SEC. 111. EFFECTIVE DATE.

(a) IN GENERAL.—Except as provided in subsection (b) or (c), this title and the amendments made by this title shall take effect 90 days after the date of the enactment of this Act and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

(b) SPECIAL RULE FOR STATE AUTHORIZATIONS OF INTERCEPTIONS.—Any interception pursuant to section 2516(2) of title 18 of the United States Code which would be valid and lawful without regard to the amendments made by this title shall be valid and lawful notwithstanding such amendments if such interception occurs during the period beginning on the date such amendments take effect and ending on the earlier of—

(1) the day before the date of the taking effect of State law conforming the applicable State statute with chapter 119 of title 18, United States Code, as so amended; or

(2) the date two years after the date of the enactment of this Act.

(c) EFFECTIVE DATE FOR CERTAIN APPROVALS BY JUSTICE DEPARTMENT OFFICIALS.—Section 104 of this Act shall take effect on the date of enactment of this Act.
TITLE II—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

SEC. 201. TITLE 18 AMENDMENT.

Title 18, United States Code, is amended by inserting after chapter 119 the following:

“CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

“Sec.

2701. Unlawful access to stored communications.

2702. Disclosure of contents.

2703. Requirements for governmental access.

2704. Backup preservation.

2705. Delayed notice.

2706. Cost reimbursement.

2707. Civil action.

2708. Exclusivity of remedies.

2709. Counterintelligence access to telephone toll and transactional records.

2710. Definitions.

18 USC 2701. "§ 2701. Unlawful access to stored communications

“(a) Offense.—Except as provided in subsection (c) of this section whoever—

“(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

“(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

“(b) Punishment.—The punishment for an offense under subsection (a) of this section is—

“(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain—

“(A) a fine of not more than $250,000 or imprisonment for not more than one year, or both, in the case of a first offense under this subparagraph; and

“(B) a fine under this title or imprisonment for not more than two years, or both, for any subsequent offense under this subparagraph; and

“(2) a fine of not more than $5,000 or imprisonment for not more than six months, or both, in any other case.

“(c) Exceptions.—Subsection (a) of this section does not apply with respect to conduct authorized—

“(1) by the person or entity providing a wire or electronic communications service;

“(2) by a user of that service with respect to a communication of or intended for that user; or

“(3) in section 2703, 2704 or 2518 of this title.

18 USC 2702. "§ 2702. Disclosure of contents

“(a) Prohibitions.—Except as provided in subsection (b)—
“(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
“(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—
“(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and
“(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.
“(b) EXCEPTIONS.—A person or entity may divulge the contents of a communication—
“(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
“(2) as otherwise authorized in section 2516, 2511(2Xa), or 2703 of this title;
“(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;
“(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;
“(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or
“(6) to a law enforcement agency, if such contents—
“(A) were inadvertently obtained by the service provider; and
“(B) appear to pertain to the commission of a crime.

§ 2703. Requirements for governmental access

“(a) CONTENTS OF ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

“(b) CONTENTS OF ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—
“(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the
Federal Rules of Criminal Procedure or equivalent State warrant; or “(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—
“(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena; or
“(ii) obtains a court order for such disclosure under subsection (d) of this section;
except that delayed notice may be given pursuant to section 2705 of this title.
“(2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service—
“(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and
“(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.
“(c) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE.—(1)(A) Except as provided in subparagraph (B), a provider of electronic communication service or remote computing service may disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to any person other than a governmental entity.
“(B) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity only when the governmental entity—
“(i) uses an administrative subpoena authorized by a Federal or State statute, or a Federal or State grand jury subpoena; 
“(ii) obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; 
“(iii) obtains a court order for such disclosure under subsection (d) of this section; or
“(iv) has the consent of the subscriber or customer to such disclosure.
“(2) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.
“(d) REQUIREMENTS FOR COURT ORDER.—A court order for disclosure under subsection (b) or (c) of this section shall issue only if the governmental entity shows that there is reason to believe the contents of a wire or electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if
the information or records requested are unusually voluminous in
nature or compliance with such order otherwise would cause an
undue burden on such provider.

"(e) No Cause of Action Against a Provider Disclosing
Information Under This Chapter.—No cause of action shall lie in
any court against any provider of wire or electronic communication
service, its officers, employees, agents, or other specified persons for
providing information, facilities, or assistance in accordance with
the terms of a court order, warrant, subpoena, or certification under
this chapter.

"§ 2704. Backup preservation

"(a) Backup Preservation.—(1) A governmental entity acting
under section 2703(b)(2) may include in its subpoena or court order a
requirement that the service provider to whom the request is
directed create a backup copy of the contents of the electronic
communications sought in order to preserve those communications.
Without notifying the subscriber or customer of such subpoena or
court order, such service provider shall create such backup copy as
soon as practicable consistent with its regular business practices and
shall confirm to the governmental entity that such backup copy has
been made. Such backup copy shall be created within two business
days after receipt by the service provider of the subpoena or court
order.

"(2) Notice to the subscriber or customer shall be made by the
governmental entity within three days after receipt of such con­
firmation, unless such notice is delayed pursuant to section 2705(a).

"(3) The service provider shall not destroy such backup copy until
the later of—

"(A) the delivery of the information; or

"(B) the resolution of any proceedings (including appeals of
any proceeding) concerning the government's subpoena or court
order.

"(4) The service provider shall release such backup copy to the
requesting governmental entity no sooner than fourteen days after
the governmental entity's notice to the subscriber or customer if
such service provider—

"(A) has not received notice from the subscriber or customer
that the subscriber or customer has challenged the govern­
mental entity's request; and

"(B) has not initiated proceedings to challenge the request of
the governmental entity.

"(5) A governmental entity may seek to require the creation of a
backup copy under subsection (a)(1) of this section if in its sole
discretion such entity determines that there is reason to believe that
notification under section 2703 of this title of the existence of the
subpoena or court order may result in destruction of or tampering
with evidence. This determination is not subject to challenge by the
subscriber or customer or service provider.

"(b) Customer Challenges.—(1) Within fourteen days after notice
by the governmental entity to the subscriber or customer under
subsection (a)(2) of this section, such subscriber or customer may file
a motion to quash such subpoena or vacate such court order, with
copies served upon the governmental entity and with written notice
of such challenge to the service provider. A motion to vacate a court
order shall be filed in the court which issued such order. A motion to
quash a subpoena shall be filed in the appropriate United States
district court or State court. Such motion or application shall contain an affidavit or sworn statement—

(A) stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and

(B) stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect.

(2) Service shall be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter. For the purposes of this section, the term 'delivery' has the meaning given that term in the Federal Rules of Civil Procedure.

(3) If the court finds that the customer has complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the governmental entity's response.

(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed.

(5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the customer.

§ 2705. Delayed notice

(a) DELAY OF NOTIFICATION.—(1) A governmental entity acting under section 2703(b) of this title may—

(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the
(2) An adverse result for the purposes of paragraph (1) of this subsection is—

(A) endangering the life or physical safety of an individual;
(B) flight from prosecution;
(C) destruction of or tampering with evidence;
(D) intimidation of potential witnesses; or
(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

(4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.

(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that—

(A) states with reasonable specificity the nature of the law enforcement inquiry; and
(B) informs such customer or subscriber—
(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;
(ii) that notification of such customer or subscriber was delayed;
(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and
(iv) which provision of this chapter allowed such delay.

(b) Preclusion of Notice to Subject of Governmental Access.—A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—

(1) endangering the life or physical safety of an individual;
(2) flight from prosecution;
(3) destruction of or tampering with evidence;
§ 2706. Cost reimbursement

"(a) PAYMENT.—Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

"(b) AMOUNT.—The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

"(c) The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

§ 2707. Civil action

"(a) CAUSE OF ACTION.—Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or customer aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity which engaged in that violation such relief as may be appropriate.

"(b) RELIEF.—In a civil action under this section, appropriate relief includes—

"(1) such preliminary and other equitable or declaratory relief as may be appropriate;

"(2) damages under subsection (c); and

"(3) a reasonable attorney’s fee and other litigation costs reasonably incurred.

"(c) DAMAGES.—The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000.

"(d) DEFENSE.—A good faith reliance on—

"(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

"(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or
"(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;
   is a complete defense to any civil or criminal action brought under this chapter or any other law.
"(c) LIMITATION.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

§ 2708. Exclusivity of remedies
"The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.

§ 2709. Counterintelligence access to telephone toll and transactional records
"(a) DUTY TO PROVIDE.—A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) REQUIRED CERTIFICATION.—The Director of the Federal Bureau of Investigation (or an individual within the Federal Bureau of Investigation designated for this purpose by the Director) may request any such information and records if the Director (or the Director's designee) certifies in writing to the wire or electronic communication service provider to which the request is made that—

(1) the information sought is relevant to an authorized foreign counterintelligence investigation; and

(2) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(c) PROHIBITION OF CERTAIN DISCLOSURE.—No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(d) DISSEMINATION BY BUREAU.—The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) REQUIREMENT THAT CERTAIN CONGRESSIONAL BODIES BE INFORMED.—On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee
on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests made under subsection (b) of this section.

§ 2710. Definitions for chapter

As used in this chapter—

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and

(2) the term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system.''.

(b) CLERICAL AMENDMENT.—The table of chapters at the beginning of part I of title 18, United States Code, is amended by adding at the end the following:

"121. Stored Wire and Electronic Communications and Transactional Records Access 2701".

SEC. 202. EFFECTIVE DATE.

This title and the amendments made by this title shall take effect ninety days after the date of the enactment of this Act and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

TITLE III—PEN REGISTERS AND TRAP AND TRACE DEVICES

SEC. 301. TITLE 18 AMENDMENT.

(a) IN GENERAL.—Title 18 of the United States Code is amended by inserting after chapter 205 the following new chapter:

"CHAPTER 206—PEN REGISTERS AND TRAP AND TRACE DEVICES

§ 3121. General prohibition on pen register and trap and trace device use; exception

(a) IN GENERAL.—Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(b) EXCEPTION.—The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service—
"(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

"(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or (3) where the consent of the user of that service has been obtained.

"(c) PENALTY.—Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

"§ 3122. Application for an order for a pen register or a trap and trace device

"(a) APPLICATION.—(1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.

"(2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.

"(b) CONTENTS OF APPLICATION.—An application under subsection (a) of this section shall include—

"(1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and

"(2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

"§ 3123. Issuance of an order for a pen register or a trap and trace device

"(a) IN GENERAL.—Upon an application made under section 3122 of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court if the court finds that the attorney for the Government or the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

"(b) CONTENTS OF ORDER.—An order issued under this section—

"(1) shall specify—

"(A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached;

"(B) the identity, if known, of the person who is the subject of the criminal investigation;
“(C) the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits of the trap and trace order; and

“(D) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and

“(2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device under section 3124 of this title.

“(c) **TIME PERIOD AND EXTENSIONS.**—(1) An order issued under this section shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days.

“(2) Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed sixty days.

“(d) **NONDISCLOSURE OF EXISTENCE OF PEN REGISTER OR A TRAP AND TRACE DEVICE.**—An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that—

“(1) the order be sealed until otherwise ordered by the court; and

“(2) the person owning or leasing the line to which the pen register or a trap and trace device is attached, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

§ 3124. Assistance in installation and use of a pen register or a trap and trace device

“(a) **PEN REGISTERS.**—Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish such investigative or law enforcement officer with all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in section 3123(b)(2) of this title.

“(b) **TRAP AND TRACE DEVICE.**—Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to receive the results of a trap and trace device under this chapter, a provider of a wire or electronic communication service, landlord, custodian, or other person shall install such device forthwith on the appropriate line and shall furnish such investigative or law enforcement officer all additional information, facilities and technical assistance including installation and operation of the
device unobtrusively and with a minimum of interference with the
services that the person so ordered by the court accords the party
with respect to whom the installation and use is to take place, if
such installation and assistance is directed by a court order as
provided in section 3123(b)(2) of this title. Unless otherwise ordered
by the court, the results of the trap and trace device shall be
furnished to the officer of a law enforcement agency, designated in
the court, at reasonable intervals during regular business hours for
the duration of the order.

"(c) COMPENSATION.—A provider of a wire or electronic commu­
ication service, landlord, custodian, or other person who furnishes
facilities or technical assistance pursuant to this section shall be
reasonably compensated for such reasonable expenses incurred in
providing such facilities and assistance.

"(d) NO CAUSE OF ACTION AGAINST A PROVIDER DISCLOSING
INFORMATION UNDER THIS CHAPTER.—No cause of action shall lie in
any court against any provider of a wire or electronic communica­
tion service, its officers, employees, agents, or other specified per­
sons for providing information, facilities, or assistance in accordance
with the terms of a court order under this chapter.

"(e) DEFENSE.—A good faith reliance on a court order, a legislative
authorization, or a statutory authorization is a complete defense
against any civil or criminal action brought under this chapter or
any other law.

"§ 3125. Reports concerning pen registers and trap and trace
devices

"The Attorney General shall annually report to Congress on the
number of pen register orders and orders for trap and trace devices
applied for by law enforcement agencies of the Department of
Justice.

"§ 3126. Definitions for chapter

"As used in this chapter—

"(1) the terms 'wire communication', 'electronic communica­
tion', and 'electronic communication service' have the meanings
set forth for such terms in section 2510 of this title;

"(2) the term 'court of competent jurisdiction' means—

"(A) a district court of the United States (including a
magistrate of such a court) or a United States Court of
Appeals; or

"(B) a court of general criminal jurisdiction of a State
authorized by the law of that State to enter orders authoriz­
ing the use of a pen register or a trap and trace device;

"(3) the term 'pen register' means a device which records or
decodes electronic or other impulses which identify the numbers
dialed or otherwise transmitted on the telephone line to which
such device is attached, but such term does not include any
device used by a provider or customer of a wire or electronic
communication service for billing, or recording as an incident to
billing, for communications services provided by such provider
or any device used by a provider or customer of a wire commu­
nication service for cost accounting or other like purposes in the
ordinary course of its business;
“(4) the term ‘trap and trace device’ means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted;
“(5) the term ‘attorney for the Government’ has the meaning given such term for the purposes of the Federal Rules of Criminal Procedure; and
“(6) the term ‘State’ means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States.”

(b) Clerical Amendment.—The table of chapters for part II of title 18 of the United States Code is amended by inserting after the item relating to chapter 205 the following new item:

“206. Pen Registers and Trap and Trace Devices 3121”.

18 USC 3121 note.

SEC. 302. EFFECTIVE DATE.

(a) IN GENERAL.—Except as provided in subsection (b), this title and the amendments made by this title shall take effect ninety days after the date of the enactment of this Act and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

(b) Special Rule for State Authorizations of Interceptions.—Any pen register or trap and trace device order or installation which would be valid and lawful without regard to the amendments made by this title shall be valid and lawful notwithstanding such amendments if such order or installation occurs during the period beginning on the date such amendments take effect and ending on the earlier of—

(1) the day before the date of the taking effect of changes in State law required in order to make orders or installations under Federal law as amended by this title; or
(2) the date two years after the date of the enactment of this Act.

SEC. 303. INTERFERENCE WITH THE OPERATION OF A SATELLITE.

(a) Offense.—Chapter 65 of title 18, United States Code, is amended by inserting at the end the following:

“§ 1367. Interference with the operation of a satellite

“(a) Whoever, without the authority of the satellite operator, intentionally or maliciously interferes with the authorized operation of a communications or weather satellite or obstructs or hinders any satellite transmission shall be fined in accordance with this title or imprisoned not more than ten years or both.
“(b) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency or of an intelligence agency of the United States.”
(b) CONFORMING AMENDMENT.—The table of sections for chapter 65 of title 18, United States Code, is amended by adding at the end the following new item:

"1367. Interference with the operation of a satellite."

Approved October 21, 1986.

LEGISLATIVE HISTORY—H.R. 4952 (S. 2575):

HOUSE REPORTS: No. 99-647 (Comm. on the Judiciary).
CONGRESSIONAL RECORD, Vol. 132 (1986):

June 23, considered and passed House.
Oct. 1, considered and passed Senate, amended.
Oct. 2, House concurred in Senate amendments.
PANEL IX:

LOOKING FORWARD: NATIONAL SECURITY LAW BEYOND 2020

MODERATOR:
JILL RHODES

DISCUSSANTS:
CARRIE CORDERO
MICHAEL DAVIS
ORDE KITTRIE
JAMES MCJUNKIN
This chapter contains Department of Justice policy on the use of electronic surveillance. The Federal electronic surveillance statutes (commonly referred to collectively as "Title III") are codified at 18 U.S.C. § 2510, et seq. Because of the well-recognized intrusive nature of many types of electronic surveillance, especially wiretaps and "bugs," and the Fourth Amendment implications of the government's use of these devices in the course of its investigations, the relevant statutes (and related Department of Justice guidelines) provide restrictions on the use of most electronic surveillance, including the requirement that a high-level Department official specifically approve the use of many of these types of electronic surveillance prior to an Assistant United States Attorney obtaining a court order authorizing interception.

Chapter 7 contains the specific mechanisms, including applicable approval requirements, for the use of wiretaps, "bugs" (oral interception devices), roving taps, video surveillance, and the consensual monitoring of wire or oral communications, as well as emergency interception procedures and restrictions on the disclosure and evidentiary use of information obtained through electronic surveillance. Additional information
Attorneys in the Criminal Division's Electronic Surveillance Unit of the Office of Enforcement Operations are available to provide assistance concerning both the interpretation of Title III and the review process necessitated thereunder. The procedures are described in the Criminal Resource Manual at 27-37 and 89-92. The Electronic Surveillance Unit has developed a user-friendly DOJNet site that contains training materials and sample Title III documents for review. Interceptions conducted pursuant to the Foreign Intelligence Surveillance Act of 1978, which is codified at 50 U.S.C. § 1801, et seq., are specifically excluded from the coverage of Title III. See 18 U.S.C. § 2511(2)(a)(ii), (2)(e), and (2)(f).

[revised July 2012]

9-7.100 - Authorization of Applications for Wire, Oral, and Electronic Interception Orders—Overview and History of Legislation

To understand the core concepts of the legislative scheme of Title III, one must appreciate the history of this legislation and the goals of Congress in enacting this comprehensive law. By enacting Title III in 1968, Congress prohibited private citizens from using certain electronic surveillance techniques. Congress exempted law enforcement from this prohibition, but required compliance with explicit directives that controlled the circumstances under which law enforcement's use of electronic surveillance would be permitted. Many of the restrictions upon the use of electronic surveillance by law enforcement agents were enacted in recognition of the strictures against unlawful searches and seizures contained in the Fourth Amendment to the United States Constitution. See, e.g., Katz v. United States, 389 U.S. 347 (1967). Still, several of Title III's provisions are more restrictive than what is required by the Fourth Amendment. At the same time, Congress preempted State law in this area, and mandated that States that sought to enact electronic surveillance laws would have to make their laws at least as restrictive as the Federal law.

One of Title III's most restrictive provisions is the requirement that Federal investigative agencies submit requests for the use of certain types of electronic surveillance (primarily the non-consensual interception of wire and oral communications) to the Department of Justice for review and approval before applications for such interception may be submitted to a court of competent jurisdiction for an order authorizing the interception. Specifically, in 18 U.S.C. § 2516(1), Title III explicitly assigns such review and approval powers to the Attorney General, but allows the Attorney General to delegate this review and approval authority to a limited number of high-level Justice Department officials, including Deputy Assistant Attorneys General for the Criminal Division ("DAAGs"). The DAAGs review and approve or deny proposed applications to conduct "wiretaps" (to intercept wire [telephone] communications, 18 U.S.C. § 2510(1)) and to install and monitor "bugs" (the use of microphones to intercept oral [face-to-face] communications, 18 U.S.C. § 2510(2)). It should be noted that only those crimes enumerated in 18 U.S.C. § 2516(1) may be investigated through the interception of wire or oral communications. On those rare occasions when the government seeks to intercept oral or wire communications within premises or over a facility that cannot be identified with any particularity, and a "roving" interception of wire or oral communications is therefore being requested, the Assistant Attorney General or the Acting Assistant Attorney General for the Criminal Division must be the one to review and approve or deny the application. (See the roving interception provision at 18 U.S.C. § 2518(11), discussed at USAM 9-7.111.)

In 1986, Congress amended Title III by enacting the Electronic Communications Privacy Act of 1986. Specifically, Congress added "electronic communications" as a new category of communications whose interception is covered by Title III. Electronic communications are non-voice communications made over a network in or affecting interstate commerce, and include text messages, electronic mail ("email"), facsimiles ("faxes"), other non-voice Internet traffic, and communications over digital-display pagers. See 18 U.S.C. § 2510(12).
Although the 1986 amendments permit any government attorney to authorize the making of an application to a Federal court to intercept electronic communications to investigate any Federal felony (18 U.S.C. § 2516(3)), the Department of Justice and Congress agreed informally at the time of ECPA's enactment that, for a three-year period, Department approval would nonetheless be required before applications could be submitted to a court to conduct interceptions of electronic communications. After that period, the Department rescinded the prior approval requirement for the interception of electronic communications over digital-display paging devices, but continued the need for Department approval prior to application to the court for the interception of any other type of electronic communications, including text messages, faxes, emails, and other non-voice communications over a computer. Applications to the court for authorization to intercept electronic communications over digital-display pagers may be made based solely upon the authorization of a United States Attorney. See 18 U.S.C. § 2516(3).

Because there are severe penalties for the improper and/or unlawful use and disclosure of electronic surveillance evidence, including criminal, civil, and administrative sanctions, as well as the suppression of evidence, it is essential that Federal prosecutors and law enforcement agents clearly understand when Departmental review and approval are required, and what such a process entails. See 18 U.S.C. §§ 2511, 2515, 2518(10), and 2520.

See the Criminal Resource Manual at 31 for citations to relevant legislation.

[revised July 2012]

9-7.110 - Format for the Authorization Request

When Justice Department review and approval of a proposed application for electronic surveillance is required, the Electronic Surveillance Unit (ESU) of the Criminal Division's Office of Enforcement Operations will conduct the initial review of the necessary pleadings, which include:

A. The affidavit of an "investigative or law enforcement officer" of the United States who is empowered by law to conduct investigations of, or to make arrests for, offenses enumerated in 18 U.S.C. § 2516(1) or (3) (which, for any application involving the interception of electronic communications, includes any Federal felony offense), with such affidavit setting forth the facts of the investigation that establish the basis for those probable cause (and other) statements required by Title III to be included in the application;

B. The application by any United States Attorney or his/her Assistant, or any other attorney authorized by law to prosecute or participate in the prosecution of offenses enumerated in 18 U.S.C. § 2516(1) or (3) that provides the basis for the court's jurisdiction to sign an order authorizing the requested interception of wire, oral, and/or electronic communications; and

C. The order to be signed by the court authorizing the government to intercept, or approving the interception of, the wire, oral, and/or electronic communications that are the subject of the application.

D. A completed Title III cover sheet that includes the signature of a supervising attorney who reviewed and approved the Title III papers. As of March 19, 2012, Department policy requires that all Title III submissions be approved by a supervising attorney other than the attorney submitting the application. That supervisory attorney must sign the Title III cover sheet, demonstrating that he or she has reviewed the affidavit, application, and draft order included in the submission packet, and that, in light of the overall investigative plan for the matter, and taking into account applicable Department policies and procedures, he or she supports the request and approves of it. The Title III cover sheet, with a space for the supervisor's signature, may be found on ESU's DOJNet site.

[revised July 2012] [cited in Criminal Resource Manual 90]

9-7.111 - Roving Interception
Pursuant to 18 U.S.C. § 2518(11)(a) and (b), the government may obtain authorization to intercept wire, oral, and electronic communications of specifically named subjects without specifying with particularity the premises within, or the facilities over which, the communications will be intercepted. (Such authorization is commonly referred to as "roving" authorization.) As to the interception of oral communications, the government may seek authorization without specifying the location(s) of the interception when it can be shown that it is not practical to do so. See United States v. Bianco, 998 F.2d 1112 (2d Cir. 1993), cert. denied, 114 S. Ct. 1644 (1994); United States v. Orena, 883 F. Supp. 849 (E.D.N.Y. 1995). An application for the interception of wire and/or electronic communications of specifically named subjects may be made without specifying the facility or facilities over which the communications will be intercepted when it can be shown that there is probable cause to believe that the target subject's actions could have the effect of thwarting interception from a specified facility. 18 U.S.C. § 2518(11)(b)(ii).

When the government seeks authorization for roving interception, the Department's authorization must be made by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an Acting Assistant Attorney General. See 18 U.S.C. § 2518(11)(a)(i) and (b)(i). Further guidance on roving interception may be found on ESU's DOJNet site.

[revised July 2012] [cited in USAM 9-7.100; Criminal Resource Manual 28]

9-7.112 - Emergency Interception

Title III contains a provision which allows for the warrantless, emergency interception of wire, oral, and/or electronic communications. Specifically, under 18 U.S.C. § 2518(7), the Attorney General (AG), the Deputy Attorney General (DAG), or the Associate Attorney General (AssocAG) may specially designate a law enforcement or investigative officer to determine whether an emergency situation exists that requires the interception of wire, oral, and/or electronic communications before a court order authorizing such interception can, with due diligence, be obtained. As defined by 18 U.S.C. § 2518(7), an emergency situation involves either: (1) immediate danger of death or serious bodily injury to any person; (2) conspiratorial activities threatening the national security interest; or (3) conspiratorial activities characteristic of organized crime. The only situations which will likely constitute an emergency are those involving an imminent threat to life, i.e., a kidnapping or hostage taking. See United States v. Crouch, 666 F. Supp. 1414 (N.D. Cal. 1987)(wiretap evidence suppressed because there was no imminent threat of death or serious injury); Nabozny v. Marshall, 781 F.2d 83 (6th Cir.)(kidnapping and extortion scenario constituted an emergency situation), cert. denied, 476 U.S. 1161 (1986). The emergency provision also requires that grounds must exist under which an order could be entered (viz., probable cause, necessity, specificity of target location/facility) to authorize the interception. Once the AG, the DAG, or the AssocAG authorizes the law enforcement agency to proceed with the emergency Title III, the government then has forty-eight (48) hours, from the time the authorization was granted, to obtain a court order approving the emergency interception. 18 U.S.C. § 2518(7). The affidavit supporting the application for the order must contain only those facts known to the AG, the DAG, or the AssocAG at the time his or her approval was given, and must be accompanied by a written verification from the requesting agency noting the date and time of the authorization. Failure to obtain the court order within the forty-eight-hour period will render any interceptions obtained during the emergency illegal.

Prior to the agency's contact with the AG, the DAG, or the Associate AG, oral approval to make the request must first be obtained from the Assistant Attorney General (AAG) or a Deputy Assistant Attorney General (DAAG) of the Criminal Division. This approval is facilitated by the Office of Enforcement Operation's Electronic Surveillance Unit, which is the initial contact for the requesting United States Attorney's Office and the requesting agency. Once the Electronic Surveillance Unit attorney briefs and obtains oral approval from the AAG or the DAAG, the attorney notifies the agency representative and the Assistant United States Attorney that the Criminal Division recommends that the emergency authorization proceed. The agency then contacts the AG, the DAG, or the AssocAG and seeks permission to proceed with the emergency Title III.
Please contact ESU prior to submitting a request for emergency authorization. In many situations, expedited review of a standard Title III application will better serve the needs of the investigation than would a emergency authorization.

[revised July 2012] [cited in Criminal Resource Manual 90]

9-7.200 - Video Surveillance—Closed Circuit Television—Department of Justice Approval Required When There Is A Reasonable Expectation of Privacy

Pursuant to Department of Justice Order No. 985-82, dated August 6, 1982, certain officials of the Criminal Division have been delegated authority to review requests to use video surveillance for law enforcement purposes when there is a constitutionally protected expectation of privacy requiring judicial authorization. This authority was delegated to the Assistant Attorney General, any Deputy Assistant Attorney General, and the Director and Associate Directors of the Office of Enforcement Operations.

When court authorization for video surveillance is deemed necessary, it should be obtained by way of an application and order predicated on Fed. R. Crim. P. 41(b) and the All Writs Act (28 U.S.C. § 1651). The application and order should be based on an affidavit that establishes probable cause to believe that evidence of a Federal crime will be obtained by the surveillance. In addition, the affidavit should comply with certain provisions of the Federal electronic surveillance statutes. See the Criminal Resource Manual at 32 for additional discussion of video surveillance warrants.

Department policy requires that the video surveillance application and order be filed separately from, and not incorporated in, an application and order for electronic surveillance pursuant to 18 U.S.C. § 2518. When appropriate, the same affidavit may be submitted in support of both applications/orders.

[cited in Criminal Resource Manual 32]

9-7.250 - Use and Unsealing of Title III Affidavits

When the government terminates a Title III electronic surveillance investigation, it must maintain under seal all of the Title III applications and orders (including affidavits and accompanying material) that were filed in support of the electronic surveillance. See 18 U.S.C. § 2518(8)(b); In re Grand Jury Proceedings, 841 F.2d 1048, 1053 n.9 (11th Cir. 1988) (although 18 U.S.C. § 2518(8)(b) refers only to "applications" and "orders," "applications" is construed to include affidavits and any other related documentation).

The purpose of this sealing requirement is to ensure the integrity of the Title III materials and to protect the privacy rights of those individuals implicated in the Title III investigation. See S.Rep. No. 1097, reprinted in 1968 U.S. Code Cong. & Admin. News 2112, 2193-2194. The applications may be unsealed only pursuant to a court order and only upon a showing of good cause under 18 U.S.C. § 2518(8)(b) or in the interest of justice under 18 U.S.C. § 2518(8)(d).

Thus, the government attorney should not attach Title III affidavits or other application material as exhibits to any search warrant affidavit, complaint, indictment, or trial brief. The government attorney may, nevertheless, use information from these materials or the Title III interceptions in documents such as search warrant affidavits, complaints, indictments, and trial briefs. See 18 U.S.C. § 2517(8)(a); 18 U.S.C. § 2517(1) and (2); and S.Rep. No. 1097 at 2188. In using this information, however, the government attorney must use care not to disclose publicly information from the Title III affidavits or interceptions that would either abridge the privacy interests of persons not charged with any crime or jeopardize ongoing investigations.

When Title III materials are sought by defense counsel or other persons and the privacy interests of uncharged persons are implicated by the contents of those materials, the government attorney should seek
a protective order pursuant to Rule 16(d)(1), Fed. R. Crim. P., that will forbid public disclosure of the contents of the materials. Likewise, a Rule 16 protective order should be sought to deny or defer discovery of those portions of the affidavits and applications that reveal ongoing investigations when disclosure would jeopardize the success of any such investigation.

For discussion about disclosure of intercepted communications in civil litigation see the Criminal Resource Manual at 33-34.

9-7.301 - Consensual Monitoring—General Use

Section 2511(2)(c) of Title 18 provides that "It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception." See United States v. White, 401 U.S. 745 (1971). As such, consensual interceptions need not be made under Title III procedures, interception orders under § 2518 are not available, and should not be sought in cases falling within § 2511(2)(c).

The Fourth Amendment to the U.S. Constitution, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986 (18 U.S.C. § 2510, et seq.), and the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801, et seq.) permit government agents, acting with the consent of a party to a communication, to engage in warrantless interceptions of telephone communications, as well as oral and electronic communications. White, supra; United States v. Caceres, 440 U.S. 741 (1979). Similarly, Title III, by its definition of oral communications, permits Federal agents to engage in warrantless interceptions of oral communications when the communicating parties have no justifiable expectation of privacy. 18 U.S.C. § 2510(2). (No similar exception is contained in the definition of wire communications and, therefore, the nonconsensual interception of wire communications violates 18 U.S.C. § 2511 regardless of the communicating parties' expectation of privacy, unless the interceptor complies with the court authorization procedures of Title III or with the provisions of the Foreign Intelligence Surveillance Act of 1978.) Since such interception techniques are particularly effective and reliable, the Department of Justice encourages their use by Federal agents for the purpose of gathering evidence of violations of Federal law, protecting the safety of informants and undercover law enforcement agents, or fulfilling other compelling needs. While these techniques are lawful and helpful, their use is frequently sensitive, so they must remain the subject of careful self-regulation by the agencies employing them.

The Department developed guidelines for the investigative use of consensual monitoring, which were promulgated most recently by the Attorney General on May 30, 2002. The guidelines do not apply to consensual monitoring of telephone conversations or radio transmissions. It was left to the enforcement agencies to develop adequate internal guidelines for the use of those aspects of this investigative tool. The following guidelines cover the investigative use of devices which intercept and record certain consensual verbal conversations where a body transmitter or recorder or a fixed location transmitter or recorder is used during a face-to-face conversation. In certain specified sensitive situations, under the regulations, the agencies must obtain advance written authorization from the Department of Justice. The guidelines on consensual monitoring set forth in the Attorney General's Memorandum of May 30, 2002, on that subject are contained in USAM 9-7.302.

[updated September 2004]

9-7.302 - Consensual Monitoring—"Procedures for Lawful, Warrantless Monitoring of Verbal Communications"

The following text was taken from a memorandum on "Procedures for Lawful, Warrantless Monitoring of Verbal Communications" issued by the Attorney General on May 30, 2002:
I. DEFINITIONS

As used in this Memorandum, the term "agency" means all of the Executive Branch departments and agencies, and specifically includes United States Attorneys' Offices which utilize their own investigators, and the Offices of the Inspectors General.

As used in this Memorandum, the terms "interception" and "monitoring" mean the aural acquisition of oral communications by use of an electronic, mechanical, or other device. Cf. 18 U.S.C. §2510(4).

As used in this Memorandum, the term "public official" means an official of any public entity of government, including special districts, as well as all federal, state, county, and municipal governmental units.

II. NEED FOR WRITTEN AUTHORIZATION

A. Investigations Where Written Department of Justice Approval is Required. A request for authorization to monitor an oral communication without the consent of all parties to the communication must be approved in writing by the Director or Associate Directors of the Office of Enforcement Operations, Criminal Division, U.S. Department of Justice, when it is known that:

(1) the monitoring relates to an investigation of a member of Congress, a federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years;
(2) the monitoring relates to an investigation of the Governor, Lieutenant Governor, or Attorney General of any State or Territory, or a judge or justice of the highest court of any State or Territory, and the offense investigated is one involving bribery, conflict of interest, or extortion relating to the performance of his or her official duties;
(3) any party to the communication is a member of the diplomatic corps of a foreign country;
(4) any party to the communication is or has been a member of the Witness Security Program and that fact is known to the agency involved or its officers;
(5) the consenting or nonconsenting person is in the custody of the Bureau of Prisons or the United States Marshals Service; or
(6) the Attorney General, Deputy Attorney General, Associate Attorney General, any Assistant Attorney General, or the United States Attorney in the district where an investigation is being conducted has requested the investigating agency to obtain prior written consent before conducting consensual monitoring in a specific investigation.

In all other cases, approval of consensual monitoring will be in accordance with the procedures set forth in part V. below.

B. Monitoring Not Within Scope of Memorandum. Even if the interception falls within one of the six categories above, the procedures and rules in this Memorandum do not apply to:

(1) extraterritorial interceptions;
(2) foreign intelligence interceptions, including interceptions pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. §1801, et seq.);
(4) routine Bureau of Prisons monitoring of oral communications that are not attended by a justifiable expectation of privacy;

(5) interceptions of radio communications; and

(6) interceptions of telephone communications.

III. AUTHORIZATION PROCEDURES AND RULES

A. Required Information. The following information must be set forth in any request to monitor an oral communication pursuant to part II.A.:

(1) Reasons for the Monitoring. The request must contain a reasonably detailed statement of the background and need for the monitoring.

(2) Offense. If the monitoring is for investigative purposes, the request must include a citation to the principal criminal statute involved.

(3) Danger. If the monitoring is intended to provide protection to the consenting party, the request must explain the nature of the danger to the consenting party.

(4) Location of Devices. The request must state where the monitoring device will be hidden: on the person, in personal effects, or in a fixed location.

(5) Location of Monitoring. The request must specify the location and primary judicial district where the monitoring will take place. A monitoring authorization is not restricted to the original district. However, if the location of monitoring changes, notice should be promptly given to the approving official. The record maintained on the request should reflect the location change.

(6) Time. The request must state the length of time needed for the monitoring. Initially, an authorization may be granted for up to 90 days from the day the monitoring is scheduled to begin. If there is the need for continued monitoring, extensions for additional periods of up to 90 days may be granted. In special cases (e.g., "fencing" operations run by law enforcement agents or long-term investigations that are closely supervised by the Department's Criminal Division), authorization for up to 180 days may be granted with similar extensions.

(7) Names. The request must give the names of persons, if known, whose communications the department or agency expects to monitor and the relation of such persons to the matter under investigation or to the need for the monitoring.

(8) Attorney Advice. The request must state that the facts of the surveillance have been discussed with the United States Attorney, an Assistant United States Attorney, or the previously designated Department of Justice attorney responsible for a particular investigation, and that such attorney advises that the use of consensual monitoring is appropriate under this Memorandum (including the date of such advice). The attorney must also advise that the use of consensual monitoring under the facts of the investigation does not raise the issue of entrapment. Such statements may be made orally. If the attorneys described above cannot provide the advice for reasons unrelated to the legality or propriety of the consensual monitoring, the advice must be sought and obtained from an attorney of the Criminal Division of the Department of Justice designated by the Assistant Attorney General in charge of that Division. Before providing such advice, a designated Criminal Division attorney shall notify the appropriate United
States Attorney or other attorney who would otherwise be authorized to provide the
required advice under this paragraph.

(9) Renewals. A request for renewal authority to monitor oral communications must
contain all the information required for an initial request. The renewal request must also
refer to all previous authorizations and explain why an additional authorization is needed,
as well as provide an updated statement that the attorney advice required under
paragraph (8) has been obtained in connection with the proposed renewal.

B. Oral Requests. Unless a request is of an emergency nature, it must be in written form and contain all
of the information set forth above. Emergency requests in cases in which written Department of
Justice approval is required may be made by telephone to the Director or an Associate Director of the
Criminal Division's Office of Enforcement Operations, or to the Assistant Attorney General, the Acting
Assistant Attorney General, or a Deputy Assistant Attorney General for the Criminal Division, and
should later be reduced to writing and submitted to the appropriate headquarters official as soon as
practicable after authorization has been obtained. An appropriate headquarters filing system is to be
maintained for consensual monitoring requests that have been received and approved in this manner.
Oral requests must include all the information required for written requests as set forth above.

C. Authorization. Authority to engage in consensual monitoring in situations set forth in part II.A. of this
Memorandum may be given by the Attorney General, the Deputy Attorney General, the Associate
Attorney General, the Assistant Attorney General or Acting Assistant Attorney General in charge of
the Criminal Division, a Deputy Assistant Attorney General in the Criminal Division, or the Director or
an Associate Director of the Criminal Division's Office of Enforcement Operations. Requests for
authorization will normally be submitted by the headquarters of the department or agency requesting
the consensual monitoring to the Office of Enforcement Operations for review.

D. Emergency Monitoring. If an emergency situation requires consensual monitoring at a time when
one of the individuals identified in part III.B. above cannot be reached, the authorization may be given
by the head of the responsible department or agency, or his or her designee. Such department or
agency must then notify the Office of Enforcement Operations as soon as practicable after the
emergency monitoring is authorized, but not later than three working days after the emergency
authorization.
The notification shall explain the emergency and shall contain all other items required for a
nonemergency request for authorization set forth in part III.A. above.

IV. SPECIAL LIMITATIONS

When a communicating party consents to the monitoring of his or her oral communications, the monitoring
device may be concealed on his or her person, in personal effects, or in a fixed location. Each department
and agency engaging in such consensual monitoring must ensure that the consenting party will be present
at all times when the device is operating.

In addition, each department and agency must ensure: (1) that no agent or person cooperating with the
department or agency trespasses while installing a device in a fixed location, unless that agent or person is
acting pursuant to a court order that authorizes the entry and/or trespass, and (2) that as long as the device
is installed in the fixed location, the premises remain under the control of the government or of the
consenting party. See United States v. Yonn, 702 F.2d 1341, 1347 (11th Cir.), cert denied, 464 U.S. 917
(1983) (rejecting the First Circuit's holding in United States v. Padilla 520 F.2d 526 (1st Cir. 1975), and
approving use of fixed monitoring devices that are activated only when the consenting party is present). But
Outside the scope of this Memorandum are interceptions of oral, nonwire communications when no party to the communication has consented. To be lawful, such interceptions generally may take place only when no party to the communication has a justifiable expectation of privacy—for example, burglars, while committing a burglary, have no justifiable expectation of privacy. Cf. United States v. Pui Kan Lam, 483 F.2d 1202 (2d. Cir. 1973), cert. denied, 415 U.S. 984 (1974) —or when authorization to intercept such communications has been obtained pursuant to Title III or the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. § 2510, et seq.) or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801, et seq. Each department or agency must ensure that no communication of any party who has a justifiable expectation of privacy is intercepted unless proper authorization has been obtained.

V. PROCEDURES FOR CONSENSUAL MONITORING WHERE NO WRITTEN APPROVAL IS REQUIRED

Prior to receiving approval for consensual monitoring from the head of the department or agency or his or her designee, a representative of the department or agency must obtain advice that the consensual monitoring is both legal and appropriate from the United States Attorney, an Assistant United States Attorney, or the Department of Justice attorney responsible for a particular investigation. The advice may be obtained orally from the attorney. If the attorneys described above cannot provide the advice for reasons unrelated to the legality or propriety of the consensual monitoring, the advice must be sought and obtained from an attorney of the Criminal Division of the Department of Justice designated by the Assistant Attorney General in charge of that Division. Before providing such advice, a designated Criminal Division attorney shall notify the appropriate United States Attorney or other attorney who would otherwise be authorized to provide the required advice under this paragraph.

Even in cases in which no written authorization is required because they do not involve the sensitive circumstances discussed above, each agency must continue to maintain internal procedures for supervising, monitoring, and approving all consensual monitoring of oral communications. Approval for consensual monitoring must come from the head of the agency or his or her designee. Any designee should be a high-ranking supervisory official at headquarters level, but in the case of the FBI may be a Special Agent in Charge or Assistant Special Agent in Charge.

Similarly, each department or agency shall establish procedures for emergency authorizations in cases involving non-sensitive circumstances similar to those that apply with regard to cases that involve the sensitive circumstances described in part III.D., including obtaining follow-up advice of an appropriate attorney as set forth above concerning the legality and propriety of the consensual monitoring.

Records are to be maintained by the involved departments or agencies for each consensual monitoring that they have conducted. These records are to include the information set forth in part III.A. above.

VI. GENERAL LIMITATIONS

This Memorandum relates solely to the subject of consensual monitoring of oral communications except where otherwise indicated. This Memorandum does not alter or supersede any current policies or directives relating to the subject of obtaining necessary approval for engaging in nonconsensual electronic surveillance or any other form of nonconsensual interception.

[cited in USAM 9-7.301]

[updated September 2004]

9-7.400 - Defendant Motion or Discovery Request for Disclosure of Defendant Overhearings and Attorney Overhearings
See the Criminal Resource Manual at 35 for a discussion of the law related to disclosure of defendant overhearings and attorney overhearings.

9-7.500 - Prior Consultation with the Computer Crime and Intellectual Property Section of the Criminal Division (CCIPS) for Applications for Pen Register and Trap and Trace Orders Capable of Collecting Uniform Resource Locators (URLs)

In 2001, the USA PATRIOT Act (P.L. 107-56) amended the Pen Register and Trap and Trace Statute (pen/trap statute), 18 U.S.C. § 3121 et seq., to clarify that courts may issue pen/trap orders to collect the non-content information associated with Internet communications. One issue that has been raised in this regard is whether a pen register order may be used to collect (URLs), the terms that a person uses to request information on the World Wide Web (e.g., www.cybercrime.gov/PatriotAct.htm). Because of privacy and other concerns relating to the use of pen register orders in this fashion, use of pen registers to collect all or part of a URL is prohibited without prior consultation with CCIPS. Among the factors that should be considered in deciding whether to apply for such a pen register are (1) the investigative need for the pen register order, (2) the litigation risk in the individual case, (3) how much of any given URL would be obtained, and (4) the impact of the order on the Department's policy goals.

Consultation with CCIPS can help resolve these issues, as well as ensuring that the contemplated use of a pen register would be consistent with the Deputy Attorney General's May 24, 2002 Memorandum on "Avoiding Collection and Investigative Use of 'Content' in the Operation of Pen Registers and Trap and Trace Devices."

This policy does not apply to applications for pen register orders that would merely authorize collection of Internet Protocol (IP) addresses, even if such IP addresses can be readily translated into URLs or portions of URLs. Similarly, this policy does not apply to the collection, at a web server, of tracing information indicating the source of requests to view a particular URL using a trap and trace order.

No employee of the Department will use the pen register authority to collect URLs without first consulting with the CCIPS of the Criminal Division. Absent emergency circumstances, such an employee will submit a memorandum to CCIPS that contains (a) the basic facts of the investigation, (b) the proposed application and order, (c) the investigative need for the collection of URLs, (d) an analysis of the litigation risk associated with obtaining the order in the context of the particular case, and (e) any other information relevant to evaluating the propriety of the application. In an emergency, such an employee may telephone CCIPS at (202) 514-1026 or, after hours at (202) 514-5000, and be prepared to describe the above information.

[new September 2003]
Opinion No. 16-06
October 2016

Subject: Client Files; Confidentiality; Law Firms

Digest: A lawyer may use cloud-based services in the delivery of legal services provided that the lawyer takes reasonable measures to ensure that the client information remains confidential and is protected from breaches. The lawyer’s obligation to protect the client information does not end once the lawyer has selected a reputable provider.

References: Illinois Rules of Professional Conduct, Rules 1.1, 1.6, 5.1 and 5.3
Illinois Rules of Professional Conduct, Rule 1.1, Comment 8 (amended effective Jan. 1, 2016)
Iowa Ethics Opinion 11-01 (2011)

FACTS
A lawyer wants to use cloud-based services in her delivery of legal services by contracting with a third party provider. The cloud service will include storage, processing and transmission of information in a shared infrastructure and a shared application, multi-tenant environment. The data will include client personal identifiable information, opposing party documents, financial information, health information and any other confidential and public information relevant to the delivery of legal services. The lawyer plans to conduct due diligence when selecting a third party provider to ensure the controls are in place to maintain confidentiality of the client information and data.

**QUESTION**

May the lawyer use a third party provider for cloud-based services? If so, is the lawyer's due diligence at the time of entering into an agreement with the provider adequate to avoid an ethical violation if a breach of confidentiality should occur through a failure of the provider or through the action of hackers?

**ANALYSIS**

Cloud-based services allow a lawyer to store and access software and data in the “cloud,” a remote location which is not controlled by the lawyer but is controlled by a third party internet service provider. Lawyers are increasingly choosing to use cloud-based services because the services offer increased flexibility and ease of access to data.

We have previously determined that a lawyer may retain or work with a private vendor to monitor the firm’s computer server and network, provided that the lawyer takes reasonable steps to ensure that the vendor protects the confidentiality of client information. See, ISBA Op. 10-01 (2009). A similar approach is appropriate when choosing and using cloud-based services. We believe that a lawyer may use cloud-based services. However, because cloud-based services store client data on remote servers outside the lawyer’s direct control, the use of such services raises ethics concerns of competence, confidentiality and the proper supervision of non-lawyers.

Rule 1.1 provides that lawyers must provide competent representation to their clients. The Illinois Supreme Court recently amended Comment 8 to Rule 1.1 to provide that as part of a lawyer’s duty of competence, lawyers must keep abreast of changes in law and its practice “including the benefits and risks associated with relevant technology.” Accordingly, lawyers who use cloud-based services must obtain and maintain a sufficient understanding of the technology they are using to properly assess the risks of unauthorized access and/or disclosures of confidential information.

Lawyers must protect as confidential “all information relating to the representation of the client” pursuant to Rule 1.6. Rule 1.6(e), as recently adopted, provides that a lawyer must make “reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to,” confidential information. Factors to be considered in determining the reasonableness of the lawyer’s efforts are set forth in Comment 18 to the Rule.
A lawyer’s use of an outside provider for cloud-based services is not, in and of itself, a violation of Rule 1.6, provided that the lawyer employs, supervises and oversees the outside provider. See, e.g., Rule 5.3, Comment 3. As stated in a Nevada opinion that discussed a lawyer’s use of an outside agency to store electronic client information:

The use of an outside data storage or server does not necessarily require the revelation of the data to anyone outside the attorney’s employ. The risk, from an ethical consideration, is that a rogue employee of the third party agency, or a “hacker” who gains access through the third party’s server or network, will access and perhaps disclose the information without authorization. In terms of the client’s confidence, this is no different in kind or quality than the risk that a rogue employee of the attorney, or for that matter a burglar, will gain unauthorized access to his confidential paper files. The question in either case is whether the attorney acted reasonable (sic) and competently to protect the confidential information.


Because technology changes so rapidly, we decline to provide specific requirements for lawyers when choosing and utilizing an outside provider for cloud-based services. Lawyers must insure that the provider reasonably safeguards client information and, at the same time, allows the attorney access to the data.

At the outset, as recognized by the inquiring lawyer here, lawyers must conduct a due diligence investigation when selecting a provider. Reasonable inquiries and practices could include:

1. Reviewing cloud computing industry standards and familiarizing oneself with the appropriate safeguards that should be employed;
2. Investigating whether the provider has implemented reasonable security precautions to protect client data from inadvertent disclosures, including but not limited to the use of firewalls, password protections, and encryption;
3. Investigating the provider’s reputation and history;
4. Inquiring as to whether the provider has experienced any breaches of security and if so, investigating those breaches;
5. Requiring an agreement to reasonably ensure that the provider will abide by the lawyer’s duties of confidentiality and will immediately notify the lawyer of any breaches or outside requests for client information;
6. Requiring that all data is appropriately backed up completely under the lawyer’s control so that the lawyer will have a method for retrieval of the data;
7. Requiring provisions for the reasonable retrieval of information if the agreement is terminated or if the provider goes out of business.

Our opinion is consistent with the advisory opinions issued by other state bar associations. Other states that have addressed the issue of cloud computing have also generally concluded that
lawyers may use cloud-based services if they take reasonable steps to protect client information and address the potential risks. See e.g., Alabama Ethics Opinion 2010-2 (2010)(lawyer may outsource storage of client files through cloud computing if the lawyer takes reasonable steps to make sure data is protected); Iowa Ethics Opinion 11-01 (2011)(lawyer should conduct appropriate due diligence before storing files electronically); Tennessee Formal Ethics Opinion 2015-F-159 (2015)(a lawyer may allow client information to be stored in the cloud provided the lawyer takes reasonable care to assure that the information remains confidential and that reasonable safeguards are employed to protect the information from breaches, loss or other risks). See generally, “Cloud Ethics Opinions Around the U.S.”, American Bar Association, Legal Technology Resource Center, www.americanbar.org.

The inquiring lawyer also asks whether the lawyer's due diligence at the time of entering into an agreement with the provider will be adequate to avoid an ethical violation if a breach of confidentiality should occur through a failure of the provider or through the action of hackers. We do not believe that the lawyer’s obligations end when the lawyer selects a reputable provider. Pursuant to Rules 1.6 and 5.3, a lawyer has ongoing obligations to protect the confidentiality of client information and data and to supervise non-lawyers. Future advances in technology may make a lawyer’s current reasonable protective measures obsolete. Accordingly, a lawyer must conduct periodic reviews and regularly monitor existing practices to determine if the client information is adequately secured and protected. See, e.g., Arizona Ethics Op. 09-04 (2009); Washington State Bar Association Advisory Op. 2215 (2012).

CONCLUSION

A lawyer may use cloud-based services to store confidential client information provided the attorney uses reasonable care to ensure that client confidentiality is protected and client data is secure. A lawyer must comply with his or her duties of competence in selecting a provider, assessing the risks, reviewing existing practices, and monitoring compliance with the lawyer’s professional obligations.

Professional Conduct Advisory Opinions are provided by the ISBA as an educational service to the public and the legal profession and are not intended as legal advice. The opinions are not binding on the courts or disciplinary agencies, but they are often considered by them in assessing lawyer conduct.

© Copyright 2016 Illinois State Bar Association
28. Electronic Surveillance—Title III Applications

The Application should meet the following requirements:

A. It must be prepared by an applicant identified as a law enforcement or investigative officer. The application must be in writing, signed by the United States Attorney, an Assistant United States Attorney, and made under oath. It must be presented to a Federal district court or court of appeals judge and be accompanied by the Department's authorization memorandum signed by an appropriate Department official and a copy of the most recent Attorney General's Order designating that official to authorize Title III applications. The application may not be presented to a magistrate. See 18 U.S.C. §§ 2510(9) and 2516(1); see also In re United States of America, 10 F.3d 931, 935-38 (2d Cir. 1993).

B. It must identify the type of communications to be intercepted. "Wire communications" include "aural transfers" (involving the human voice) that are transmitted, at least in part by wire, between the point of origin and the point of reception, i.e., telephone calls. 18 U.S.C. § 2510(1). This includes cellular phones, cordless phones, voice mail, and voice pagers, as well as traditional landline telephones. "Oral communications" are communications between people who are together under circumstances where the parties enjoy a reasonable expectation of privacy. 18 U.S.C. § 2510(2). "Electronic communications" include text messages, email, non-voice computer and Internet transmissions, faxes, communications over digital-display paging devices, and, in some cases, satellite transmissions. Communications over tone-only paging devices, data from tracking devices (as defined by 18 U.S.C. § 3117), and electronic funds transfer information are not electronic communications under Title III. 18 U.S.C. § 2510(12).

C. It must identify the specific Federal offenses for which there is probable cause to believe are being committed. The offenses that may be the predicate for a wire or oral interception order are limited to only those set forth in 18 U.S.C. § 2516(1). In the case of electronic communications, a request for interception may be based on any Federal felony, pursuant to 18 U.S.C. § 2516(3).

D. It must provide a particular description of the nature and location of the facilities from which, or the place where, the interception is to occur. An exception to this is the roving interception provision set forth in 18 U.S.C. § 2518(11)(a) and (b). The specific requirements of the roving provision are discussed in USAM 9-7.111. Briefly, in the case of a roving oral interception, the application must show, and the court order must indicate, that it is impractical to specify the location(s) where oral communications of a particular named subject are to be intercepted. 18 U.S.C. § 2518(11)(a)(ii) and (iii). In the case of a roving wire or electronic interception, the application must state, and the court order must indicate, that a particular named subject's actions could have the effect of thwarting interception from a specified facility. 18 U.S.C. § 2518(11)(b)(ii) and (iii). The accompanying DOJ document authorizing the roving interception must be signed by an official at the level of an Assistant Attorney General (including Acting AAG) or higher. 18 U.S.C. § 2518(11)(a)(i) and (b)(i). Further guidance on roving interceptions may be found on the DOJNet site of the Electronic Surveillance Unit (ESU), Office of Enforcement Operations (OEO).
E. It must identify, with specificity, those persons known to be committing the offenses and whose communications are to be intercepted. In *United States v. Donovan*, 429 U.S. 413, 422-32 (1977), the Supreme Court held that 18 U.S.C. § 2518(1)(b)(iv) requires the government to name all individuals whom it has probable cause to believe are engaged in the offenses under investigation, and whose conversations it expects to intercept over or from within the targeted facilities. It is the Criminal Division’s policy to name as subjects all persons whose involvement in the alleged offenses is indicated, even if not all those persons are expected to be intercepted over the target facility or at the target location.

F. It must contain a statement affirming that normal investigative procedures have been tried and failed, are reasonably unlikely to succeed if tried, or are too dangerous to employ. 18 U.S.C. § 2518(1)(c). The applicant may then state that a complete discussion of attempted alternative investigative techniques is set forth in the accompanying affidavit.

G. It must contain a statement affirming that the affidavit contains a complete statement of the facts—to the extent known to the applicant and the official approving the application—concerning all previous applications that have been made to intercept the oral, wire, or electronic communications of any of the named subjects or involving the target facility or location. 18 U.S.C. § 2518(1)(e).

H. In an oral (and occasionally in a wire or electronic) interception, it must contain a request that the court issue an order authorizing investigative agents to make all necessary surreptitious and/or forcible entries to install, maintain, and remove electronic interception devices in or from the targeted premises (or device). When effecting this portion of the order, the applicant should notify the court as soon as practicable after each surreptitious entry.

I. When requesting the interception of wire communications over a cellular telephone, it should contain a request that the authorization and court order apply not only to the target telephone identified therein, but also to: 1) any change in *one* of several potential identifying numbers for the phone, including the electronic serial number (ESN), International Mobile Subscriber Identity (IMSI) number, International Mobile Equipment Identification (IMEI) number, Mobile Equipment Identifier (MEID) number, or Urban Fleet Mobile Identification (UFMI) number; and 2) any changed target telephone number when the other identifying number has remained the same. Model continuity language for each type of identifier may be obtained from ESU. With regard to a landline phone, it should request that the authorization and court order apply not only to the target telephone number identified therein, but also to any changed telephone number subsequently assigned to the same cable, pair, and binding posts used by the target landline telephone. No continuity language should be included when the target telephone is a Voice Over Internet Protocol (VoIP) phone. The application should also request that the authorization apply to background conversations intercepted in the vicinity of the target phone while the phone is in use. *See United States v. Baranek*, 903 F.2d 1068, 1070-72 (6th Cir. 1990).

J. It must contain, when concerning the interception of wire communications, a request that the court issue an order directly to the service provider, as defined in 18 U.S.C. § 2510(15), to furnish the investigative agency with all information, facilities, and technical assistance necessary to facilitate the ordered interception. 18 U.S.C. § 2511(2)(a)(ii). The application should also request that the court direct service providers and their agents and employees not to disclose the contents of the court order or the existence of the investigation. *Id.*

K. For original and spinoff applications, it should contain a request that the court's order authorize the requested interception until all relevant communications have been intercepted, not to exceed a period of thirty (30) days from the earlier of the day on which the interception begins or ten (10) days after the order is entered. 18 U.S.C. § 2518(5). For extensions, it should contain a request that the thirty-day period be measured from the date of the court's order.

L. It should contain a statement affirming that all interceptions will be minimized in accordance with Chapter 119 of Title 18, United States Code, as described further in the affidavit. 18 U.S.C. § 2518(5).

[updated October 2012]
29. Electronic Surveillance—Title III Affidavits

The Affidavit must meet the following requirements:

A. It must be sworn and attested to by an investigative or law enforcement officer as defined in 18 U.S.C. § 2510(7). Criminal Division policy requires that the affiant be a member of one of the following agencies: FBI, DEA, ICE/HSI, ATF, U.S. Secret Service, U.S. Marshals Service, or U.S. Postal Inspection Service. Criminal Division policy precludes the use of multiple affiants except when it is indicated clearly which affiant swears to which part of the affidavit, or states that each affiant swears to the entire affidavit. If a State or local law enforcement officer is the affiant in a Federal electronic surveillance affidavit, the enforcement officer must be deputized as a Federal officer of the agency responsible for the offenses under investigation. 18 U.S.C. § 2516(1).

B. It must identify the target subjects, describe the facility or location that is the subject of the proposed electronic surveillance, and list the alleged offenses. 18 U.S.C. § 2518(1). If any of the alleged offenses are not listed predicate offenses under 18 U.S.C. § 2516(1), that fact should be noted.

C. It must establish probable cause that the named subjects are using the targeted facility or location to commit the stated offenses. Any background information needed to understand fully the instant investigation should be set forth briefly at the beginning of this section. The focus, however, should be on recent and current criminal activity by the subjects, with an emphasis on their use of the target facility or location. This is generally accomplished through information from a confidential informant, cooperating witness, or undercover agent, combined with pen register or telephone toll information for the target phone or physical surveillance of the target premises. Criminal Division policy requires that the affidavit demonstrate criminal use of the target facility or premises within six months from the date of Department approval. For wire communications, where probable cause is demonstrated by consensually recorded calls or calls intercepted over another wiretap, the affidavit should include some direct quotes of the calls, with appropriate characterization. Criminal Division policy dictates that that pen register or telephone toll information for the target telephone, or physical surveillance of the targeted premises, standing alone, is generally insufficient to establish probable cause. Generally, probable cause to establish criminal use of the facilities or premises requires independent evidence of use of the facilities or premises in addition to pen register or surveillance information, often in the form of informant or undercover information. It is preferable that all informants used in the affidavit to establish probable cause be qualified according to the "Aguilar-Spinelli" standards (Aguilar v. Texas, 378 U.S. 108 (1964) and Spinelli v. United States, 393 U.S. 410 (1969)), rather than those set forth in the Supreme Court decision of Illinois v. Gates, 463 U.S. 1237 (1983). Under some circumstances, criminal use of the target facility within six months of Department approval may be established in the absence of consensually recorded communications or prior interceptions when use of the phone may be tied to a significant event, such as a narcotics transaction or a seizure, through phone records. In addition to criminal use within six months, the affidavit must also show recent use of the facility or premises within 21 days from the date on which the Department authorizes the filing of the application. For wire and electronic communications, the affidavit must contain records showing
contact between the facility and at least one other criminally relevant facility that demonstrates necessity for the wiretap within 21 days of Department approval. The affidavit must clearly and specifically demonstrate how the other facility is criminally relevant and state the date range for the contacts and the date of the most recent contact. The date range for all pen register/phone records data must be updated to within 10 days of submission to OEO. For extension requests, the affidavit should include some direct quotes of wire communications (and/or electronic communications, if applicable), with appropriate characterization, including one from within seven days of Department approval, or an explanation of the failure to obtain such results and the continued need to conduct interceptions. (When the application requests authorization to intercept oral communications within a location, it is often helpful to include a diagram of the target location as an attachment to the affidavit.)

D. It must explain the need for the proposed electronic surveillance and provide a detailed discussion of the other investigative procedures that have been tried and failed, are reasonably unlikely to succeed if tried, or are too dangerous to employ. 18 U.S.C. § 2518(1)(e). This is to ensure that highly intrusive electronic surveillance techniques are not resorted to in situations where traditional investigative techniques would suffice to expose the crime. United States v. Kahn, 415 U.S. 143 (1974). It need not be shown that no other investigative avenues are available, only that they have been tried and proven inadequate or have been considered and rejected for reasons described. See, e.g., United States v. Foy, 641 F.3d 455, 464 (10th Cir. 2011); United States v. Cartagena, 593 F.3d 104, 109-111 (1st Cir. 2010); United States v. Concepcion, 579 F.3d 214, 218-220 (2d Cir. 2009). There should also be a discussion as to why electronic surveillance is the technique most likely to succeed. When drafting this section of the affidavit, the discussion of these and other investigative techniques should be augmented with facts particular to the specific investigation and subjects. General declarations and conclusory statements about the exhaustion of alternative techniques will not suffice.

It is most important that this section be tailored to the facts of the specific case and be more than a recitation of "boiler plate." The affidavit must discuss the particular problems involved in the investigation in order to fulfill the requirement of 18 U.S.C. § 2518(1)(c). The affidavit should explain specifically why other normally utilized investigative techniques, such as physical surveillance or the use of informants and undercover agents, are inadequate in the particular case. For example, if physical surveillance is impossible or unproductive because the suspects live in remote areas or will likely be alerted to law enforcement presence (by counter-surveillance or other means), the affidavit should set forth those facts clearly. If the informants refuse to testify or cannot penetrate the hierarchy of the criminal organization involved, the affidavit should explain why that is so in this particular investigation. If undercover agents cannot be used because the suspects deal only with trusted associates/family, the affidavit must so state and include the particulars. Conclusory generalizations about the difficulties of using a particular investigative technique will not suffice. It is not enough, for example, to state that the use of undercover agents is always difficult in organized crime cases because crime families, in general, deal only with trusted associates. While the affidavit may contain a general statement regarding the impossibility of using undercover agents in organized crime cases, it must also demonstrate that the particular subject or subjects in the instant case deal only with known associates. The key is to tie the inadequacy of a specific investigative technique to the particular facts underlying the investigation. See, e.g., Foy, 641 F.3d at 464 United States v. Blackmon, 273 F.3d 1204, 1210-1212 (9th Cir. 2001); United States v. Uribe, 890 F.2d 554 (1st Cir. 1989).

E. It must contain a full and complete statement of any known previous applications made to any judge (federal, state, or foreign) for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities, or places specified in the application. This statement should include the date, jurisdiction, and disposition of previous applications, as well as their relevance, if any, to the instant investigation. All relevant electronic surveillance ("ELSUR") databases must be checked, including that of the agency conducting the investigation. In narcotics investigations, Criminal Division policy provides that the DEA, FBI, and ICE
databases be searched. In investigations involving firearms offenses, ATF ELSUR databases should be checked. In joint investigations, all participating agencies' databases should be checked; in all other cases when it is likely that more than one agency may have investigated the subjects, multiple indices checks should likewise be made. It is recommended that all ELSUR searches be updated to within 45 days of submission of an application to OEO. The duty to disclose prior applications under 18 U.S.C. § 2518(1)(e) covers all persons named in the application, and not just those designated as "principal targets." United States v. Bianco, 998 F.2d 1112 (2d Cir. 1993).

F. It must contain a statement of the period of time for which the interception is to be maintained. The statute provides that an order may be granted for not more than thirty days or until the objectives of the investigation are achieved, whichever occurs first. 18 U.S.C. § 2518(5). If the violations are continuing, facts sufficient to justify interception for the full thirty-day period must be provided, or the court may order monitoring to cease once initial, criminal conversations are intercepted. This may be accomplished by showing, through informant or undercover investigation, pen register analysis, physical surveillance, or other law enforcement investigation, that a pattern of criminal activity exists and is likely to continue. If it is clear that the interceptions will terminate after a limited number of days, then the time requested should also be so limited in accordance with the facts of the case.

The statute also provides for a ten-day grace period, before the thirty-day period begins to run. 18 U.S.C. § 2518(5). This statutory grace period allows for delays by the service provider in establishing interception capability. The ten-day grace period applies only to the initial installation of equipment or establishment of interceptions, and may not be used in an extension application, or in an original application when the equipment is already installed.

Some courts have consulted Rule 45 of the Federal Rules of Criminal Procedure for guidance on the method to calculate the thirty-day period under the statute, and have held that the thirty-day period begins to run on the date after the order was signed, even if the interception started on the same day that it was signed. See United States v. Smith, 223 F.3d 554, 575 (7th Cir. 2000); United States v. Villegas, 1993 WL 535013, at *11-12 (S.D.N.Y. Dec. 22, 1993); United States v. Gerena, 695 F. Supp. 649, 658 (D. Conn. 1988); United States v. Sklaroff, 323 F. Supp. 296, 317 (S.D. Fla. 1971); but see United States v. Gangi, 33 F. Supp. 2d 303, 310-11 (S.D.N.Y. 1999); United States v. Pichardo, 1999 WL 649020, at * 3 (S.D.N.Y. Aug. 25, 1999). In an abundance of caution, however, OEO recommends that the thirty-day period be calculated from the date and time that the order is signed. OEO further suggests that an applicant adhere to established practice regarding the calculation of the thirty-day period in the applicant's particular district.

G. It must contain a statement affirming that monitoring agents will minimize all non-pertinent interceptions in accordance with Chapter 119 of Title 18, United States Code, as well as additional standard minimization language and other language addressing any specific minimization problems (e.g., steps to be taken to avoid the interception of privileged communications, such as attorney-client communications) in the instant case. (18 U.S.C. § 2518(5) permits non-officer government personnel or individuals acting under contract with the government to monitor conversations pursuant to the interception order. These individuals must be acting under the supervision of an investigative or law enforcement officer when monitoring communications, and the affidavit should note the fact that these individuals will be used as monitors pursuant to 18 U.S.C. § 2518(5).)

When communications are intercepted that relate to any offense not enumerated in the authorization order, the monitoring agent should report it immediately to the Assistant United States Attorney, who should notify the court at the earliest opportunity. Approval by the issuing judge should be sought for the continued interception of such conversations. While 18 U.S.C. § 2517(1) and (2) permit use or disclosure of this information without first obtaining a court order, 18 U.S.C. § 2517(5) requires a disclosure order before the information may be used in any proceeding (e.g., before a grand jury).
All wire and oral communications must be minimized in real time. The statute permits after-the-fact minimization for wire and oral communications only when the intercepted communications are in code, or in a foreign language when a foreign language expert is not reasonably available. 18 U.S.C. § 2518(5). In either event, the minimization must be accomplished as soon as practicable after the interception. Such after-the-fact minimization can be accomplished by an interpreter who listens to and minimizes the communications after they have been recorded, giving only the pertinent communications to the supervising agent. The process utilized must protect the suspect's privacy interests to approximately the same extent as would contemporaneous minimization, properly applied. United States v. David, 940 F.2d 722 (1st Cir. 1991); United States v. Simels, 2009 WL 1924746, at *6-*9 (E.D.N.Y. Jul. 2, 2009). After-the-fact minimization provisions should be applied in light of the "reasonableness" standard established by the Supreme Court in United States v. Scott, 436 U.S. 128 (1978).

After-the-fact minimization is a necessity for the interception of electronic communications, such as those in the form of text messages, email, or faxes. In such cases, all communications should be recorded and then examined by a monitoring agent to determine their relevance to the investigation. Further dissemination is then limited to those communications by the subjects or their confederates that are criminal in nature. Further guidance regarding the minimization of text messages may be found on ESU's DOJNet site.

H. A judge may only enter an order approving interceptions "within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction)." 18 U.S.C. § 2518(3). Interceptions occur at the site of the target facility or location and at the site where the communications are first heard/reviewed and minimized (e.g. the wire room). United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992); see also United States v. Luong, 471 F.3d 1107, 1109 (9th Cir. 2006); United States v. Denman, 100 F.3d 399, 403 (5th Cir. 1996).

For most requests, the affidavit should indicate that either the target facility/location or the place of first review and minimization is within the territorial jurisdiction of the court. Thus, when seeking to wiretap a cellular phone not located within the territorial jurisdiction of the court at the time of application, the place of first hearing and minimization must be within the territorial jurisdiction of the court (i.e. a regional wire room located elsewhere should not be used). When seeking to wiretap a cellular phone that is located within the territorial jurisdiction of the court at the time of application, a regional wire room may be used, but the order should authorize continued interceptions should the phone be taken outside that jurisdiction.

When the request is to intercept communications with a mobile interception device, such as a bug in an automobile, the affidavit should contain a statement that, pursuant to 18 U.S.C. § 2518(3), interception will occur not only within the territorial jurisdiction of the court in which the application is made, but also outside that jurisdiction (but within the United States), if there is any indication that the interception device will be taken outside the jurisdiction of the court issuing the electronic surveillance order. The order should likewise authorize such extra-jurisdictional interception.

[updated October 2012] [cited in Criminal Resource Manual 90]
30. Electronic Surveillance—Title III Orders

The Order must meet the following requirements:

The authorizing language of the order should mirror the requesting language of the application and affidavit, stating that there is probable cause to believe that the named subjects are committing particular Title III predicate offenses (or, in the case of electronic communications, any Federal felony), that particular communications concerning those offenses will be obtained through interception, and that normal investigative techniques have been tried and have failed, or are reasonably unlikely to succeed if tried, or are too dangerous to employ. 18 U.S.C. § 2518(3) and (4). The court then orders (again tracking the language of the application and affidavit) that agents of the investigative agency are authorized to intercept wire, oral, or electronic communications over the described facility or at the described premises. Id. The order should also contain language specifying the length of time the interception may be conducted, and, if necessary, authorizing surreptitious and/or forcible entry to effectuate the purpose of the order. Id. The order may also contain language mandating the government to make periodic progress reports (pursuant to 18 U.S.C. § 2518(6)), and ordering the sealing of those as well as the order, application and affidavit. In the case of a roving interception, the court must make a specific finding that the requirements of 18 U.S.C. § 2518(11)(a) and/or (b) have been demonstrated adequately. Any other special requests, such as extra-jurisdictional interception in the case of mobile interception devices and enforceability of the order as to changed service providers without further order of the court, should also be authorized specifically in the order.

The court should also issue a technical assistance order to the communications service provider. 18 U.S.C. § 2518(4). This is a redacted order that requires the telephone company or other service provider to assist the agents in effecting the electronic surveillance. OEO does not review redacted service provider orders. An order to seal all of the pleadings should also be sought at this time.

The Application, Affidavit, and Order should be sent via email to OEO at ESU.Requests@usdoj.gov. Submissions must include a completed Title III cover sheet that includes the signature of a supervising attorney who reviewed and approved the Title III papers. Criminal Division policy requires that all Title III submissions be approved by a supervising attorney other than the attorney submitting the application. That supervisory attorney must sign the Title III cover sheet, demonstrating that he or she has reviewed the affidavit, application, and draft order included in the submission packet, and that, in light of the overall investigative plan for the matter, and taking into account applicable Department policies and procedures, he or she supports the request and approves of it. The Title III cover sheet, with a space for the supervisor's signature, may be found on ESU's DOJNet site.

Spinoff requests (e.g., additional applications to conduct electronic surveillance over a new facility or at a new location in the same investigation) and extension requests are reviewed in the same manner as described above. While the exigencies of investigative work occasionally make the normally required lead time impossible, the timeliness with which an application is reviewed and authorized is largely under the
control of the Assistant United States Attorney handling the case. When coordinating an investigation or planning extension requests, it is important to allow sufficient time for the Title III application to be reviewed by OEO. OEO strongly recommends that extension requests be submitted up to a week in advance of the date on which the interception period expires.

Questions or requests for assistance may be directed to ESU at (202) 514-6809. Sample Title III forms are available by email from ESU or on ESU's DOJNet site.

[updated October 2012]
OMNIBUS CRIME CONTROL AND SAFE STREETS

For Legislative History of Act, see p. 2112

PUBLIC LAW 90–351; 82 STAT. 197

[H. R. 5037]

An Act to assist State and local governments in reducing the incidence of crime, to increase the effectiveness, fairness, and coordination of law enforcement and criminal justice systems at all levels of government, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That:

This Act may be cited as the “Omnibus Crime Control and Safe Streets Act of 1968”.

TITLE I—LAW ENFORCEMENT ASSISTANCE

DECLARATIONS AND PURPOSE

Congress finds that the high incidence of crime in the United States threatens the peace, security, and general welfare of the Nation and its citizens. To prevent crime and to insure the greater safety of the people, law enforcement efforts must be better coordinated, intensified, and made more effective at all levels of government.

Congress finds further that crime is essentially a local problem that must be dealt with by State and local governments if it is to be controlled effectively.

It is therefore the declared policy of the Congress to assist State and local governments in strengthening and improving law enforcement at every level by national assistance. It is the purpose of this title to (1) encourage States and units of general local government to prepare and adopt comprehensive plans based upon their evaluation of State and local problems of law enforcement; (2) authorize grants to States and units of local government in order to improve and strengthen law enforcement; and (3) encourage research and development directed toward the improvement of law enforcement and the development of new methods for the prevention and reduction of crime and the detection and apprehension of criminals.

PART A—LAW ENFORCEMENT ASSISTANCE ADMINISTRATION

Sec. 101. (a) There is hereby established within the Department of Justice, under the general authority of the Attorney General, a Law Enforcement Assistance Administration (hereafter referred to in this title as “Administration”).

(b) The Administration shall be composed of an Administrator of Law Enforcement Assistance and two Associate Administrators of Law Enforcement Assistance, who shall be appointed by the Presi-
dent, by and with the advice and consent of the Senate. No more
than two members of the Administration shall be the same political
party, and members shall be appointed with due regard to their fit-
ness, knowledge, and experience to perform the functions, powers,
and duties vested in the Administration by this title.

(c) It shall be the duty of the Administration to exercise all of
the functions, powers, and duties created and established by this
title, except as otherwise provided.

PART B—PLANNING GRANTS

Sec. 201. It is the purpose of this part to encourage States and
units of general local government to prepare and adopt compre-
hensive law enforcement plans based on their evaluation of State
and local problems of law enforcement.

Sec. 202. The Administration shall make grants to the States for
the establishment and operation of State law enforcement planning
agencies (hereinafter referred to in this title as “State planning
agencies”) for the preparation, development, and revision of the
State plans required under section 303 of this title. Any State may
make application to the Administration for such grants within six
months of the date of enactment of this Act.

Sec. 203. (a) A grant made under this part to a State shall be
utilized by the State to establish and maintain a State planning
agency. Such agency shall be created or designated by the chief
executive of the State and shall be subject to his jurisdiction. The
State planning agency shall be representative of law enforcement
agencies of the State and of the units of general local government
within the State.

(b) The State planning agency shall—

(1) develop, in accordance with part C, a comprehensive state-
wide plan for the improvement of law enforcement throughout
the State;

(2) define, develop, and correlate programs and projects for
the State and the units of general local government in the State
or combinations of States or units for improvement in law en-
forcement; and

(3) establish priorities for the improvement in law enforce-
ment throughout the State.

(c) The State planning agency shall make such arrangements as
such agency deems necessary to provide that at least 40 per centum
of all Federal funds granted to such agency under this part for any
fiscal year will be available to units of general local government or
combinations of such units to enable such units and combinations of
such units to participate in the formulation of the comprehensive
State plan required under this part. Any portion of such 40 per
centum in any State for any fiscal year not required for the purpose
set forth in the preceding sentence shall be available for expenditure
by such State agency from time to time on dates during such year
as the Administration may fix, for the development by it of the State plan required under this part.

Sec. 204. A Federal grant authorized under this part shall not exceed 90 per centum of the expenses of the establishment and operation of the State planning agency, including the preparation, development, and revision of the plans required by part C. Where Federal grants under this part are made directly to units of general local government as authorized by section 305, the grant shall not exceed 90 per centum of the expenses of local planning, including the preparation, development, and revision of plans required by part C.

Sec. 205. Funds appropriated to make grants under this part for a fiscal year shall be allocated by the Administration among the States for use therein by the State planning agency or units of general local government, as the case may be. The Administration shall allocate $100,000 to each of the States; and it shall then allocate the remainder of such funds available among the States according to their relative populations.

PART C—GRANTS FOR LAW ENFORCEMENT PURPOSES

Sec. 301. (a) It is the purpose of this part to encourage States and units of general local government to carry out programs and projects to improve and strengthen law enforcement.

(b) The Administration is authorized to make grants to States having comprehensive State plans approved by it under this part, for-

(1) Public protection, including the development, demonstration, evaluation, implementation, and purchase of methods, devices, facilities, and equipment designed to improve and strengthen law enforcement and reduce crime in public and private places.

(2) The recruiting of law enforcement personnel and the training of personnel in law enforcement.

(3) Public education relating to crime prevention and encouraging respect for law and order, including education programs in schools and programs to improve public understanding of and cooperation with law enforcement agencies.

(4) Construction of buildings or other physical facilities which would fulfill or implement the purposes of this section.

(5) The organization, education, and training of special law enforcement units to combat organized crime, including the establishment and development of State organized crime prevention councils, the recruiting and training of special investigative and prosecuting personnel, and the development of systems for collecting, storing, and disseminating information relating to the control of organized crime.

(6) The organization, education, and training of regular law enforcement officers, special law enforcement units, and law enforcement reserve units for the prevention, detection, and con-
control of riots and other violent civil disorders, including the acquisition of riot control equipment.

(7) The recruiting, organization, training and education of community service officers to serve with and assist local and State law enforcement agencies in the discharge of their duties through such activities as recruiting; improvement of police-community relations and grievance resolution mechanisms; community patrol activities; encouragement of neighborhood participation in crime prevention and public safety efforts; and other activities designed to improve police capabilities, public safety and the objectives of this section: Provided, That in no case shall a grant be made under this subcategory without the approval of the local government or local law enforcement agency.

(c) The amount of any Federal grant made under paragraph (5) or (6) of subsection (b) of this section may be up to 75 per centum of the cost of the program or project specified in the application for such grant. The amount of any grant made under paragraph (4) of subsection (b) of this section may be up to 50 per centum of the cost of the program or project specified in the application for such grant. The amount of any other grant made under this part may be up to 60 per centum of the cost of the program or project specified in the application for such grant: Provided, That no part of any grant for the purpose of construction of buildings or other physical facilities shall be used for land acquisition.

(d) Not more than one-third of any grant made under this part may be expended for the compensation of personnel. The amount of any such grant expended for the compensation of personnel shall not exceed the amount of State or local funds made available to increase such compensation. The limitations contained in this subsection shall not apply to the compensation of personnel for time engaged in conducting or undergoing training programs.

Sec. 302. Any State desiring to participate in the grant program under this part shall establish a State planning agency as described in part B of this title and shall within six months after approval of a planning grant under part B submit to the Administration through such State planning agency a comprehensive State plan formulated pursuant to part B of this title.

Sec. 303. The Administration shall make grants under this title to a State planning agency if such agency has on file with the Administration an approved comprehensive State plan (not more than one year in age) which conforms with the purposes and requirements of this title. Each such plan shall—

(1) provide for the administration of such grants by the State planning agency;

(2) provide that at least 75 per centum of all Federal funds granted to the State planning agency under this part for any fiscal year will be available to units of general local government or combinations of such units for the development and imple-
CRIME CONTROL

mentation of programs and projects for the improvement of law enforcement;

(3) adequately take into account the needs and requests of the units of general local government in the State and encourage local initiative in the development of programs and projects for improvements in law enforcement, and provide for an appropriately balanced allocation of funds between the State and the units of general local government in the State and among such units;

(4) incorporate innovations and advanced techniques and contain a comprehensive outline of priorities for the improvement and coordination of all aspects of law enforcement dealt with in the plan, including descriptions of: (A) general needs and problems; (B) existing systems; (C) available resources; (D) organizational systems and administrative machinery for implementing the plan; (E) the direction, scope, and general types of improvements to be made in the future; and (F) to the extent appropriate, the relationship of the plan to other relevant State or local law enforcement plans and systems;

(5) provide for effective utilization of existing facilities and permit and encourage units of general local government to combine or provide for cooperative arrangements with respect to services, facilities, and equipment;

(6) provide for research and development;

(7) provide for appropriate review of procedures of actions taken by the State planning agency disapproving an application for which funds are available or terminating or refusing to continue financial assistance to units of general local government or combinations of such units;

(8) demonstrate the willingness of the State and units of general local government to assume the costs of improvements funded under this part after a reasonable period of Federal assistance;

(9) demonstrate the willingness of the State to contribute technical assistance or services for programs and projects contemplated by the statewide comprehensive plan and the programs and projects contemplated by units of general local government;

(10) set forth policies and procedures designed to assure that Federal funds made available under this title will be so used as not to supplant State or local funds, but to increase the amounts of such funds that would in the absence of such Federal funds be made available for law enforcement;

(11) provide for such fiscal control and fund accounting procedures as may be necessary to assure proper disbursement of and accounting of funds received under this part; and

(12) provide for the submission of such reports in such form and containing such information as the Administration may reasonably require.
Any portion of the 75 per centum to be made available pursuant to paragraph (2) of this section in any State in any fiscal year not required for the purposes set forth in such paragraph (2) shall be available for expenditure by such State agency from time to time on dates during such year as the Administration may fix, for the development and implementation of programs and projects for the improvement of law enforcement and in conformity with the State plan.

Sec. 304. State planning agencies shall receive applications for financial assistance from units of general local government and combinations of such units. When a State planning agency determines that such an application is in accordance with the purposes stated in section 301 and is in conformance with any existing statewide comprehensive law enforcement plan, the State planning agency is authorized to disburse funds to the applicant.

Sec. 305. Where a State fails to make application for a grant to establish a State planning agency pursuant to part B of this title within six months after the date of enactment of this Act, or where a State fails to file a comprehensive plan pursuant to part B within six months after approval of a planning grant to establish a State planning agency, the Administration may make grants under part B and part C of this title to units of general local government or combinations of such units: Provided, however, That any such unit or combination of such units must certify that it has submitted a copy of its application to the chief executive of the State in which such unit or combination of such units is located. The chief executive shall be given not more than sixty days from date of receipt of the application to submit to the Administration in writing an evaluation of the project set forth in the application. Such evaluation shall include comments on the relationship of the application to other applications then pending, and to existing or proposed plans in the State for the development of new approaches to and improvements in law enforcement. If an application is submitted by a combination of units of general local government which is located in more than one State, such application must be submitted to the chief executive of each State in which the combination of such units is located. No grant under this section to a local unit of general government shall be for an amount in excess of 60 per centum of the cost of the project or program with respect to which it was made.

Sec. 306. Funds appropriated to make grants under this part for a fiscal year shall be allocated by the Administration among the States for use therein by the State planning agency or units of general local government, as the case may be. Of such funds, 85 per centum shall be allocated among the States according to their respective populations and 15 per centum thereof shall be allocated as the Administration may determine, plus such additional amounts as may be made available by virtue of the application of the provisions of section 509 to the grant to any State.

Sec. 307. (a) In making grants under this part, the Administration and each State planning agency, as the case may be, shall give
special emphasis, where appropriate or feasible, to programs and projects dealing with the prevention, detection, and control of organized crime and of riots and other violent civil disorders.

(b) Notwithstanding the provisions of section 303 of this part, until August 31, 1968, the Administration is authorized to make grants for programs and projects dealing with the prevention, detection, and control of riots and other violent civil disorders on the basis of applications describing in detail the programs, projects, and costs of the items for which the grants will be used, and the relationship of the programs and projects to the applicant's general program for the improvement of law enforcement.

PART D—TRAINING, EDUCATION, RESEARCH, DEMONSTRATION, AND SPECIAL GRANTS

Sec. 401. It is the purpose of this part to provide for and encourage training, education, research, and development for the purpose of improving law enforcement and developing new methods for the prevention and reduction of crime, and the detection and apprehension of criminals.

Sec. 402. (a) There is established within the Department of Justice a National Institute of Law Enforcement and Criminal Justice (hereafter referred to in this part as "Institute"). The Institute shall be under the general authority of the Administration. It shall be the purpose of the Institute to encourage research and development to improve and strengthen law enforcement.

(b) The Institute is authorized—

(1) to make grants to, or enter into contracts with, public agencies, institutions of higher education, or private organizations to conduct research, demonstrations, or special projects pertaining to the purposes described in this title, including the development of new or improved approaches, techniques, systems, equipment, and devices to improve and strengthen law enforcement;

(2) to make continuing studies and undertake programs of research to develop new or improved approaches, techniques, systems, equipment, and devices to improve and strengthen law enforcement, including, but not limited to, the effectiveness of projects or programs carried out under this title;

(3) to carry out programs of behavioral research designed to provide more accurate information on the causes of crime and the effectiveness of various means of preventing crime, and to evaluate the success of correctional procedures;

(4) to make recommendations for action which can be taken by Federal, State, and local governments and by private persons and organizations to improve and strengthen law enforcement;

(5) to carry out programs of instructional assistance consisting of research fellowships for the programs provided under this section, and special workshops for the presentation and dissemi-
nation of information resulting from research, demonstrations, and special projects authorized by this title.

(6) to carry out a program of collection and dissemination of information obtained by the Institute or other Federal agencies, public agencies, institutions of higher education, or private organizations engaged in projects under this title, including information relating to new or improved approaches, techniques, systems, equipment, and devices to improve and strengthen law enforcement; and

(7) to establish a research center to carry out the programs described in this section.

Sec. 403. A grant authorized under this part may be up to 100 per centum of the total cost of each project for which such grant is made. The Administration shall require, whenever feasible, as a condition of approval of a grant under this part, that the recipient contribute money, facilities, or services to carry out the purpose for which the grant is sought.

Sec. 404. (a) The Director of the Federal Bureau of Investigation is authorized to—

(1) establish and conduct training programs at the Federal Bureau of Investigation National Academy at Quantico, Virginia, to provide, at the request of a State or unit of local government, training for State and local law enforcement personnel;

(2) develop new or improved approaches, techniques, systems, equipment, and devices to improve and strengthen law enforcement; and

(3) assist in conducting, at the request of a State or unit of local government, local and regional training programs for the training of State and local law enforcement personnel. Such training shall be provided only for persons actually employed as State police or highway patrol, police of a unit of local government, sheriffs and their deputies, and such other persons as the State or unit may nominate for police training while such persons are actually employed as officers of such State or unit.

(b) In the exercise of the functions, powers, and duties established under this section the Director of the Federal Bureau of Investigation shall be under the general authority of the Attorney General.

Sec. 405. (a) Subject to the provisions of this section, the Law Enforcement Assistance Act of 1965 (79 Stat. 828)\(^2\) is repealed: Provided, That—

(1) The Administration, or the Attorney General until such time as the members of the Administration are appointed, is authorized to obligate funds for the continuation of projects approved under the Law Enforcement Assistance Act of 1965 prior to the date of enactment of this Act to the extent that such approval provided for continuation.
(2) Any funds obligated under subsection (1) of this section and all activities necessary or appropriate for the review under subsection (3) of this section may be carried out with funds previously appropriated and funds appropriated pursuant to this title.

(3) Immediately upon establishment of the Administration, it shall be its duty to study, review, and evaluate projects and programs funded under the Law Enforcement Assistance Act of 1965. Continuation of projects and programs under subsections (1) and (2) of this section shall be in the discretion of the Administration.

Sec. 406. (a) Pursuant to the provisions of subsections (b) and (c) of this section, the Administration is authorized, after appropriate consultation with the Commissioner of Education, to carry out programs of academic educational assistance to improve and strengthen law enforcement.

(b) The Administration is authorized to enter into contracts to make, and make, payments to institutions of higher education for loans, not exceeding $1,800 per academic year to any person, to persons enrolled on a full-time basis in undergraduate or graduate programs approved by the Administration and leading to degrees or certificates in areas directly related to law enforcement or preparing for employment in law enforcement, with special consideration to police or correctional personnel of States or units of general local government on academic leave to earn such degrees or certificates. Loans to persons assisted under this subsection shall be made on such terms and conditions as the Administration and the institution offering such programs may determine, except that the total amount of any such loan, plus interest, shall be canceled for service as a full-time officer or employee of a law enforcement agency at the rate of 25 per centum of the total amount of such loans plus interest for each complete year of such service or its equivalent of such service, as determined under regulations of the Administration.

(c) The Administration is authorized to enter into contracts to make, and make, payments to institutions of higher education for tuition and fees, not exceeding $200 per academic quarter or $300 per semester for any person, to officers of any publicly funded law enforcement agency enrolled on a full-time or part-time basis in courses included in an undergraduate or graduate program which is approved by the Administration and which leads to a degree or certificate in an area related to law enforcement or an area suitable for persons employed in law enforcement. Assistance under this subsection may be granted only on behalf of an applicant who enters into an agreement to remain in the service of the law enforcement agency employing such applicant for a period of two years following completion of any course for which payments are provided under this subsection, and in the event such service is not completed, to repay the full amount of such payments on such terms and in such manner as the Administration may prescribe.
PART E—ADMINISTRATIVE PROVISIONS

Sec. 501. The Administration is authorized, after appropriate consultation with representatives of States and units of general local government, to establish such rules, regulations, and procedures as are necessary to the exercise of its functions, and are consistent with the stated purpose of this title.

Sec. 502. The Administration may delegate to any officer or official of the Administration, or, with the approval of the Attorney General, to any officer of the Department of Justice such functions as it deems appropriate.

Sec. 503. The functions, powers, and duties specified in this title to be carried out by the Administration shall not be transferred elsewhere in the Department of Justice unless specifically hereafter authorized by the Congress.

Sec. 504. In carrying out its functions, the Administration, or upon authorization of the Administration, any member thereof or any hearing examiner assigned to or employed by the Administration, shall have the power to hold hearings, sign and issue subpoenas, administer oaths, examine witnesses, and receive evidence at any place in the United States it may designate.

Sec. 505. Section 5315 of title 5, United States Code, is amended by adding at the end thereof—

“(90) Administrator of Law Enforcement Assistance.”

Sec. 506. Section 5316 of title 5, United States Code, is amended by adding at the end thereof—

“(126) Associate Administrator of Law Enforcement Assistance.”

Sec. 507. Subject to the civil service and classification laws, the Administration is authorized to select, appoint, employ, and fix compensation of such officers and employees, including hearing examiners, as shall be necessary to carry out its powers and duties under this title.

Sec. 508. The Administration is authorized, on a reimbursable basis when appropriate, to use the available services, equipment, personnel, and facilities of the Department of Justice and of other civilian or military agencies and instrumentalities of the Federal Government, and to cooperate with the Department of Justice and such other agencies and instrumentalities in the establishment and use of services, equipment, personnel, and facilities of the Administration. The Administration is further authorized to confer with and avail itself of the cooperation, services, records, and facilities of State, municipal, or other local agencies.

Sec. 509. Whenever the Administration, after reasonable notice and opportunity for hearing to an applicant or a grantee under this
title, finds that, with respect to any payments made or to be made under this title, there is a substantial failure to comply with—

(a) the provisions of this title;
(b) regulations promulgated by the Administration under this title; or
(c) a plan or application submitted in accordance with the provisions of this title;

the Administration shall notify such applicant or grantee that further payments shall not be made (or in its discretion that further payments shall not be made for activities in which there is such failure), until there is no longer such failure.

Sec. 510. (a) In carrying out the functions vested by this title in the Administration, the determination, findings, and conclusions of the Administration shall be final and conclusive upon all applicants, except as hereafter provided.

(b) If the application has been rejected or an applicant has been denied a grant or has had a grant, or any portion of a grant, discontinued, or has been given a grant in a lesser amount than such applicant believes appropriate under the provisions of this title, the Administration shall notify the applicant or grantee of its action and set forth the reason for the action taken. Whenever an applicant or grantee requests a hearing on action taken by the Administration on an application or a grant the Administration, or any authorized officer thereof, is authorized and directed to hold such hearings or investigations at such times and places as the Administration deems necessary, following appropriate and adequate notice to such applicant; and the findings of fact and determinations made by the Administration with respect thereto shall be final and conclusive, except as otherwise provided herein.

(c) If such applicant is still dissatisfied with the findings and determinations of the Administration, following the notice and hearing provided for in subsection (b) of this section, a request may be made for rehearing, under such regulations and procedures as the Administration may establish, and such applicant shall be afforded an opportunity to present such additional information as may be deemed appropriate and pertinent to the matter involved. The findings and determinations of the Administration, following such rehearing, shall be final and conclusive upon all parties concerned, except as hereafter provided.

Sec. 511. (a) If any applicant or grantee is dissatisfied with the Administration's final action with respect to the approval of its application or plan submitted under this title, or any applicant or grantee is dissatisfied with the Administration's final action under section 509 or section 510, such applicant or grantee may, within sixty days after notice of such action, file with the United States court of appeals for the circuit in which such applicant or grantee is located a petition for review of that action. A copy of the petition shall be forthwith transmitted by the clerk of the court to the Administration. The Administration shall thereupon file in the court
the record of the proceedings on which the action of the Administration was based, as provided in section 2112 of title 28, United States Code.

(b) The determinations and the findings of fact by the Administration, if supported by substantial evidence, shall be conclusive; but the court, for good cause shown, may remand the case to the Administration to take further evidence. The Administration may thereupon make new or modified findings of fact and may modify its previous action, and shall file in the court the record of the further proceedings. Such new or modified findings of fact or determinations shall likewise be conclusive if supported by substantial evidence.

(c) Upon the filing of such petition, the court shall have jurisdiction to affirm the action of the Administration or to set it aside, in whole or in part. The judgment of the court shall be subject to review by the Supreme Court of the United States upon certiorari or certification as provided in section 1254 of title 28, United States Code.

Sec. 512. Unless otherwise specified in this title, the Administration shall carry out the programs provided for in this title during the fiscal year ending June 30, 1968, and the five succeeding fiscal years.

Sec. 513. To insure that all Federal assistance to State and local programs under this title is carried out in a coordinated manner, the Administration is authorized to request any Federal department or agency to supply such statistics, data, program reports, and other material as the Administration deems necessary to carry out its functions under this title. Each such department or agency is authorized to cooperate with the Administration and, to the extent permitted by law, to furnish such materials to the Administration. Any Federal department or agency engaged in administering programs related to this title shall, to the maximum extent practicable, consult with and seek advice from the Administration to insure fully coordinated efforts, and the Administration shall undertake to coordinate such efforts.

Sec. 514. The Administration may arrange with and reimburse the heads of other Federal departments and agencies for the performance of any of its functions under this title.

Sec. 515. The Administration is authorized—

(a) to conduct evaluation studies of the programs and activities assisted under this title;

(b) to collect, evaluate, publish, and disseminate statistics and other information on the condition and progress of law enforcement in the several States; and

(c) to cooperate with and render technical assistance to States, units of general local government, combinations of such States or units, or other public or private agencies, organizations, or institutions in matters relating to law enforcement.

Sec. 516. (a) Payments under this title may be made in installments, and in advance or by way of reimbursement, as may be determined by the Administration.
(b) Not more than 12 per centum of the sums appropriated for any fiscal year to carry out the provisions of this title may be used within any one State except that this limitation shall not apply to grants made pursuant to part D.

Sec. 517. The Administration is authorized to appoint such technical or other advisory committees to advise the Administration with respect to the administration of this title as it deems necessary. Members of such committees not otherwise in the employ of the United States, while attending meetings of the committees, shall be entitled to receive compensation at a rate to be fixed by the Administration but not exceeding $75 per diem, and while away from home or regular place of business they may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by section 5703 of title 5, United States Code, for persons in the Government service employed intermittently.

Sec. 518. (a) Nothing contained in this title or any other Act shall be construed to authorize any department, agency, officer, or employee of the United States to exercise any direction, supervision, or control over any police force or any other law enforcement agency of any State or any political subdivision thereof.

(b) Notwithstanding any other provision of law nothing contained in this title shall be construed to authorize the Administration (1) to require, or condition the availability or amount of a grant upon, the adoption by an applicant or grantee under this title of a percentage ratio, quota system, or other program to achieve racial balance or to eliminate racial imbalance in any law enforcement agency, or (2) to deny or discontinue a grant because of the refusal of an applicant or grantee under this title to adopt such a ratio, system, or other program.

Sec. 519. On or before August 31, 1968, and each year thereafter, the Administration shall report to the President and to the Congress on activities pursuant to the provisions of this title during the preceding fiscal year.

Sec. 520. For the purpose of carrying out this title, there is authorized to be appropriated the sums of $100,111,000 for the fiscal years ending June 30, 1968, and June 30, 1969, $300,000,000 for the fiscal year ending June 30, 1970, and for succeeding fiscal years such sums as the Congress might authorize: Provided, however, That of the amount appropriated for the fiscal years ending June 30, 1968, and June 30, 1969—

(a) the sum of $25,000,000 shall be for the purposes of part B;

(b) the sum of $50,000,000 shall be for the purposes of part C, of which amount—

(1) not more than $2,500,000 shall be for the purposes of section 302(b) (3);

(2) not more than $15,000,000 shall be for the purposes of section 302(b) (5), of which not more than $1,000,000 may be used within any one State.
(3) not more than $15,000,000 shall be for the purposes of section 302(b) (6); and
(4) not more than $10,000,000 shall be for the purposes of correction, probation, and parole; and
(c) the sum of $25,111,000 shall be for the purposes of part D, of which $5,111,000 shall be for the purposes of section 404, and not more than $10,000,000 shall be for the purposes of section 406.

Sec. 521. (a) Each recipient of assistance under this Act shall keep such records as the Administration shall prescribe, including records which fully disclose the amount and disposition by such recipient of the proceeds of such assistance, the total cost of the project or undertaking in connection with which such assistance is given or used, and the amount of that portion of the cost of the project or undertaking supplied by other sources, and such other records as will facilitate an effective audit.

(b) The Administration and the Comptroller General of the United States, or any of their duly authorized representatives, shall have access for purpose of audit and examinations to any books, documents, papers, and records of the recipients that are pertinent to the grants received under this title.

Sec. 522. Section 204(a) of the Demonstration Cities and Metropolitan Development Act of 1966 is amended by inserting “law enforcement facilities,” immediately after “transportation facilities.”

PART F—DEFINITIONS

Sec. 601. As used in this title—
(a) “Law enforcement” means all activities pertaining to crime prevention or reduction and enforcement of the criminal law.
(b) “Organized crime” means the unlawful activities of the members of a highly organized, disciplined association engaged in supplying illegal goods and services, including but not limited to gambling, prostitution, loan sharking, narcotics, labor racketeering, and other unlawful activities of members of such organizations.
(c) “State” means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.
(d) “Unit of general local government” means any city, county, township, town, borough, parish, village, or other general purpose political subdivision of a State, or an Indian tribe which performs law enforcement functions as determined by the Secretary of the Interior.
(e) “Combination” as applied to States or units of general local government means any grouping or joining together of such States or units for the purpose of preparing, developing, or implementing a law enforcement plan.
(f) "Construction" means the erection, acquisition, expansion, or repair (but not including minor remodeling or minor repairs) of new or existing buildings or other physical facilities, and the acquisition or installation of initial equipment therefor.

(g) "State organized crime prevention council" means a council composed of not more than seven persons established pursuant to State law or established by the chief executive of the State for the purpose of this title, or an existing agency so designated, which council shall be broadly representative of law enforcement officials within such State and whose members by virtue of their training or experience shall be knowledgeable in the prevention and control of organized crime.

(h) "Metropolitan area" means a standard metropolitan statistical area as established by the Bureau of the Budget, subject, however, to such modifications and extensions as the Administration may determine to be appropriate.

(i) "Public agency" means any State, unit of local government, combination of such States or units, or any department, agency, or instrumentality of any of the foregoing.

(j) "Institution of higher education" means any such institution as defined by section 801(a) of the Higher Education Act of 1965 (79 Stat. 1269; 20 U.S.C. 1141(a)), subject, however, to such modifications and extensions as the Administration may determine to be appropriate.

(k) "Community service officer" means any citizen with the capacity, motivation, integrity, and stability to assist in or perform police work but who may not meet ordinary standards for employment as a regular police officer selected from the immediate locality of the police department of which he is to be a part, and meeting such other qualifications promulgated in regulations pursuant to section 501 as the administration may determine to be appropriate to further the purposes of section 301(b) (7) of this Act.

TITLE II—ADMISSIBILITY OF CONFESSIONS, REVIEWABILITY OF ADMISSION IN EVIDENCE OF CONFESSIONS IN STATE CASES, ADMISSIBILITY IN EVIDENCE OF EYE WITNESS TESTIMONY, AND PROCEDURES IN OBTAINING WRITS OF HABEAS CORPUS

Sec. 701. (a) Chapter 223, title 18, United States Code (relating to witnesses and evidence), is amended by adding at the end thereof the following new sections:

"§ 3501. Admissibility of confessions

"(a) In any criminal prosecution brought by the United States or by the District of Columbia, a confession, as defined in subsection (e) hereof, shall be admissible in evidence if it is voluntarily given. Before such confession is received in evidence, the trial judge shall, out of the presence of the jury, determine any issue as to voluntariness. If the trial judge determines that the confession was volun-
tarily made it shall be admitted in evidence and the trial judge shall permit the jury to hear relevant evidence on the issue of voluntariness and shall instruct the jury to give such weight to the confession as the jury feels it deserves under all the circumstances.

“(b) The trial judge in determining the issue of voluntariness shall take into consideration all the circumstances surrounding the giving of the confession, including (1) the time elapsing between arrest and arraignment of the defendant making the confession, if it was made after arrest and before arraignment, (2) whether such defendant knew the nature of the offense with which he was charged or of which he was suspected at the time of making the confession, (3) whether or not such defendant was advised or knew that he was not required to make any statement and that any such statement could be used against him, (4) whether or not such defendant had been advised prior to questioning of his right to the assistance of counsel; and (5) whether or not such defendant was without the assistance of counsel when questioned and when giving such confession.

“The presence or absence of any of the above-mentioned factors to be taken into consideration by the judge need not be conclusive on the issue of voluntariness of the confession.

“(c) In any criminal prosecution by the United States or by the District of Columbia, a confession made or given by a person who is a defendant therein, while such person was under arrest or other detention in the custody of any law-enforcement officer or law-enforcement agency, shall not be inadmissible solely because of delay in bringing such person before a commissioner or other officer empowered to commit persons charged with offenses against the laws of the United States or of the District of Columbia if such confession is found by the trial judge to have been made voluntarily and if the weight to be given the confession is left to the jury and if such confession was made or given by such person within six hours immediately following his arrest or other detention: Provided, That the time limitation contained in this subsection shall not apply in any case in which the delay in bringing such person before such commissioner or other officer beyond such six-hour period is found by the trial judge to be reasonable considering the means of transportation and the distance to be traveled to the nearest available such commissioner or other officer.

“(d) Nothing contained in this section shall bar the admission in evidence of any confession made or given voluntarily by any person to any other person without interrogation by anyone, or at any time at which the person who made or gave such confession was not under arrest or other detention.

“(e) As used in this section, the term ‘confession’ means any confession of guilt of any criminal offense or any self-incriminating statement made or given orally or in writing.

“§ 3502. Admissibility in evidence of eye witness testimony

“The testimony of a witness that he saw the accused commit or participate in the commission of the crime for which the accused is
being tried shall be admissible in evidence in a criminal prosecution in any trial court ordained and established under article III of the Constitution of the United States.”

(b) The section analysis of that chapter is amended by adding at the end thereof the following new items:

“3501. Admissibility of confessions.  
“3502. Admissibility in evidence of eye witness testimony.”

TITLE III—WIRETAPPING AND ELECTRONIC SURVEILLANCE

FINDINGS

Sec. 801. On the basis of its own investigations and of published studies, the Congress makes the following findings:

(a) Wire communications are normally conducted through the use of facilities which form part of an interstate network. The same facilities are used for interstate and intrastate communications. There has been extensive wiretapping carried on without legal sanctions, and without the consent of any of the parties to the conversation. Electronic, mechanical, and other intercepting devices are being used to overhear oral conversations made in private, without the consent of any of the parties to such communications. The contents of these communications and evidence derived therefrom are being used by public and private parties as evidence in court and administrative proceedings, and by persons whose activities affect interstate commerce. The possession, manufacture, distribution, advertising, and use of these devices are facilitated by interstate commerce.

(b) In order to protect effectively the privacy of wire and oral communications, to protect the integrity of court and administrative proceedings, and to prevent the obstruction of interstate commerce, it is necessary for Congress to define on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized, to prohibit any unauthorized interception of such communications, and the use of the contents thereof in evidence in courts and administrative proceedings.

(c) Organized criminals make extensive use of wire and oral communications in their criminal activities. The interception of such communications to obtain evidence of the commission of crimes or to prevent their commission is an indispensable aid to law enforcement and the administration of justice.

(d) To safeguard the privacy of innocent persons, the interception of wire or oral communications where none of the parties to the communication has consented to the interception should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court. Interception of wire and oral communications should further be limited to certain major types of offenses and specific categories of
crime with assurances that the interception is justified and that the information obtained thereby will not be misused.

Sec. 802. Part I of title 18, United States Code, is amended by adding at the end of the following new chapter:

"Chapter 119. WIRE INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS"

"Sec.
"2510. Definitions.
"2511. Interception and disclosure of wire or oral communications prohibited.
"2512. Manufacture, distribution, possession, and advertising of wire or oral communication intercepting devices prohibited.
"2513. Confiscation of wire or oral communication intercepting devices.
"2514. Immunity of witnesses.
"2515. Prohibition of use as evidence of intercepted wire or oral communications.
"2516. Authorization for interception of wire or oral communications.
"2517. Authorization for disclosure and use of intercepted wire or oral communications.
"2518. Procedure for interception of wire or oral communications.
"2519. Reports concerning intercepted wire or oral communications.
"2520. Recovery of civil damages authorized.

"§ 2510. Definitions
"As used in this chapter—

"(1) 'wire communication' means any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications;

"(2) 'oral communication' means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation;

"(3) 'State' means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

"(4) 'intercept' means the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device.

"(5) 'electronic, mechanical, or other device' means any device or apparatus which can be used to intercept a wire or oral communication other than—

"(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a communications common carrier in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business; or (ii) being used by a communications common carrier in
the ordinary course of its business, or by an investigative
or law enforcement officer in the ordinary course of his
duties;
“(b) a hearing aid or similar device being used to correct
subnormal hearing to not better than normal;
“(6) ‘person’ means any employee, or agent of the United
States or any State or political subdivision thereof, and any in-
dividual, partnership, association, joint stock company, trust, or
corporation;
“(7) ‘Investigative or law enforcement officer’ means any of-
ficer of the United States or of a State or political subdivision
thereof, who is empowered by law to conduct investigations of
or to make arrests for offenses enumerated in this chapter, and
any attorney authorized by law to prosecute or participate in the
prosecution of such offenses;
“(8) ‘contents’, when used with respect to any wire or oral
communication, includes any information concerning the iden-
tity of the parties to such communication or the existence, sub-
stance, purport, or meaning of that communication;
“(9) ‘Judge of competent jurisdiction’ means—
“(a) a judge of a United States district court or a United
States court of appeals; and
“(b) a judge of any court of general criminal jurisdic-
tion of a State who is authorized by a statute of that State
to enter orders authorizing interceptions of wire or oral
communications;
“(10) ‘communication common carrier’ shall have the same
meaning which is given the term ‘common carrier’ by section
153(h) of title 47 of the United States Code; and
“(11) ‘aggrieved person’ means a person who was a party to
any intercepted wire or oral communication or a person against
whom the interception was directed.

§ 2511. Interception and disclosure of wire or oral communica-
tions prohibited
“(1) Except as otherwise specifically provided in this chapter any
person who—
“(a) willfully intercepts, endeavors to intercept, or procures
any other person to intercept or endeavor to intercept, any wire
or oral communication;
“(b) willfully uses, endeavors to use, or procures any other
person to use or endeavor to use any electronic, mechanical, or
other device to intercept any oral communication when—
“(i) such device is affixed to, or otherwise transmits a
signal through, a wire, cable, or other like connection used
in wire communication; or
“(ii) such device transmits communications by radio, or
interferes with the transmission of such communication;
“(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or
“(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment whose operations of which affect interstate or foreign commerce, or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or
“(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;”
“(c) willfully discloses, or endeavors to disclose, to any other person the contents of any wire or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication in violation of this subsection; or
“(d) willfully uses, or endeavors to use, the contents of any wire or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication in violation of this subsection; shall be fined not more than $10,000 or imprisoned not more than five years, or both.
“(2) (a) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of any communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the carrier of such communication: Provided, That said communication common carriers shall not utilize service observing or random monitoring except for mechanical or service quality control checks.
“(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.
“(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire or oral communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.
“(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire or oral communication
where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State or for the purpose of committing any other injurious act.

"(3) Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1143; 47 U.S.C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.

"§ 2512. Manufacture, distribution, possession, and advertising of wire or oral communication intercepting devices prohibited

"(1) Except as otherwise specifically provided in this chapter, any person who willfully—

"(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire or oral communications;

"(b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire or oral communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

"(c) places in any newspaper, magazine, handbill, or other publication any advertisement of—

"(i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire or oral communications; or

"(ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device
for the purpose of the surreptitious interception of wire or oral communications,
knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce,
shall be fined not more than $10,000 or imprisoned not more than five years, or both.
“(2) It shall not be unlawful under this section for—
“(a) a communications common carrier or an officer, agent, or employee of, or a person under contract with, a communications common carrier, in the normal course of the communications common carrier’s business, or
“(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire or oral communications.

“§ 2513. Confiscation of wire or oral communication intercepting devices
“Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. All provisions of law relating to (1) the seizure, summary and judicial forfeiture, and condemnation of vessels, vehicles, merchandise, and baggage for violations of the customs laws contained in title 19 of the United States Code, (2) the disposition of such vessels, vehicles, merchandise, and baggage or the proceeds from the sale thereof, (3) the remission or mitigation of such forfeiture, (4) the compromise of claims, and (5) the award of compensation to informers in respect of such forfeitures, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the provisions of this section; except that such duties as are imposed upon the collector of customs or any other person with respect to the seizure and forfeiture of vessels, vehicles, merchandise, and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be performed with respect to seizure and forfeiture of electronic, mechanical, or other intercepting devices under this section by such officers, agents, or other persons as may be authorized or designated for that purpose by the Attorney General.

“§ 2514. Immunity of witnesses
“Whenever in the judgment of a United States attorney the testimony of any witness, or the production of books, papers, or other
evidence by any witness, in any case or proceeding before any grand jury or court of the United States involving any violation of this chapter or any of the offenses enumerated in section 2516, or any conspiracy to violate this chapter or any of the offenses enumerated in section 2516 is necessary to the public interest, such United States attorney, upon the approval of the Attorney General, shall make application to the court that the witness shall be instructed to testify or produce evidence subject to the provisions of this section, and upon order of the court such witness shall not be excused from testifying or from producing books, papers, or other evidence on the ground that the testimony or evidence required of him may tend to incriminate him or subject him to a penalty or forfeiture. No such witness shall be prosecuted or subjected to any penalty or forfeiture for or on account of any transaction, matter or thing concerning which he is compelled, after having claimed his privilege against self-incrimination, to testify or produce evidence, nor shall testimony so compelled be used as evidence in any criminal proceeding (except in a proceeding described in the next sentence) against him in any court. No witness shall be exempt under this section from prosecution for perjury or contempt committed while giving testimony or producing evidence under compulsion as provided in this section.

"§ 2515. Prohibition of use as evidence of intercepted wire or oral communications

"Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

"§ 2516. Authorization for interception of wire or oral communications

"(1) The Attorney General, or any Assistant Attorney General specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of—

"(a) any offense punishable by death or by imprisonment for more than one year under sections 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), or under the following chapters of this title: chapter 37 (relating to espionage), chapter 105 (relat-
ing to sabotage), chapter 115 (relating to treason), or chapter 102 (relating to riots);

"(b) a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labor organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under this title;

"(c) any offense which is punishable under the following sections of this title: section 201 (bribery of public officials and witnesses), section 224 (bribery in sporting contests), section 1084 (transmission of wagering information), section 1503 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1751 (Presidential assassinations, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), or sections 2314 and 2315 (interstate transportation of stolen property);

"(d) any offense involving counterfeiting punishable under sections 471, 472, or 473 of this title;

"(e) any offense involving bankruptcy fraud or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;

"(f) any offense including extortionate credit transactions under sections 892, 893, or 894 of this title; or

"(g) any conspiracy to commit any of the foregoing offenses.

"(2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire or oral communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute an order authorizing, or approving the interception of wire or oral communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.
§ 2517. Authorization for disclosure and use of intercepted wire or oral communications

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire or oral communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire or oral communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.

(3) Any person who has received, by any means authorized by this chapter, any information concerning a wire or oral communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any criminal proceeding in any court of the United States or of any State or in any Federal or State grand jury proceeding.

(4) No otherwise privileged wire or oral communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire or oral communications in the manner authorized herein, intercepts wire or oral communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

§ 2518. Procedure for interception of wire or oral communications

(1) Each application for an order authorizing or approving the interception of a wire or oral communication shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular
offense that has been, is being, or is about to be committed, (ii) a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

"(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

"(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

"(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire or oral communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

"(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

"(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

"(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire or oral communications within the territorial jurisdiction of the court in which the judge is sitting, if the judge determines on the basis of the facts submitted by the applicant that—

"(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

"(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

"(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

"(d) there is probable cause for belief that the facilities from which, or the place where, the wire or oral communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.
“(4) Each order authorizing or approving the interception of any wire or oral communication shall specify—

“(a) the identity of the person, if known, whose communications are to be intercepted;

“(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

“(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

“(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

“(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

“(5) No order entered under this section may authorize or approve the interception of any wire or oral communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days.

“(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

“(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that—

“(a) an emergency situation exists with respect to conspiratorial activities threatening the national security interest or to conspiratorial activities characteristic of organized crime that requires a wire or oral communication to be intercepted before
an order authorizing such interception can with due diligence be obtained, and

"(b) there are grounds upon which an order could be entered under this chapter to authorize such interception, may intercept such wire or oral communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire or oral communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

"(8) (a) The contents of any wire or oral communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire or oral communication under this subsection shall be done in such way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire or oral communication or evidence derived therefrom under subsection (3) of section 2517.

"(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

"(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

"(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7) (b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge
may determine in his discretion that is in the interest of justice, an inventory which shall include notice of—

“(1) the fact of the entry of the order or the application;

“(2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and

“(3) the fact that during the period wire or oral communications were or were not intercepted.

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

“(9) The contents of any intercepted wire or oral communication or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

“(10) (a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any intercepted wire or oral communication, or evidence derived therefrom, on the grounds that—

“(i) the communication was unlawfully intercepted;

“(ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or

“(iii) the interception was not made in conformity with the order of authorization or approval.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

“(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial
of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.

"§ 2519. Reports concerning intercepted wire or oral communications"

"(1) Within thirty days after the expiration of an order (or each extension thereof) entered under section 2518, or the denial of an order approving an interception, the issuing or denying judge shall report to the Administrative Office of the United States Courts—

"(a) the fact that an order or extension was applied for;

"(b) the kind of order or extension applied for;

"(c) the fact that the order or extension was granted as applied for, was modified, or was denied;

"(d) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;

"(e) the offense specified in the order or application, or extension of an order;

"(f) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and

"(g) the nature of the facilities from which or the place where communications were to be intercepted.

"(2) In January of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Office of the United States Courts—

"(a) the information required by paragraphs (a) through (g) of subsection (1) of this section with respect to each application for an order or extension made during the preceding calendar year;

"(b) a general description of the interceptions made under such order or extension, including (i) the approximate nature and frequency of incriminating communications intercepted, (ii) the approximate nature and frequency of other communications intercepted, (iii) the approximate number of persons whose communications were intercepted, and (iv) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;

"(c) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;

"(d) the number of trials resulting from such interceptions;

"(e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied;

"(f) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained..."
and a general assessment of the importance of the interceptions; and

"(g) the information required by paragraphs (b) through (f) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

"(3) In April of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire or oral communications and the number of orders and extensions granted or denied during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (1) and (2) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (1) and (2) of this section.

"§ 2520. Recovery of civil damages authorized

"Any person whose wire or oral communication is intercepted, disclosed, or used in violation of this chapter shall (1) have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use such communications, and (2) be entitled to recover from any such person—

"(a) actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher;

"(b) punitive damages; and

"(c) a reasonable attorney's fee and other litigation costs reasonably incurred.

A good faith reliance on a court order or on the provisions of section 2518(7) of this chapter shall constitute a complete defense to any civil or criminal action brought under this chapter."

Sec. 803. Section 605 of the Communications Act of 1934 (48 Stat. 1103; 47 U.S.C. 605) is amended to read as follows:

"UNAUTHORIZED PUBLICATION OF COMMUNICATIONS

"Sec. 605. Except as authorized by chapter 119, title 18, United States Code, no person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception, (1) to any person other than the addressee, his agent, or attorney, (2) to a person employed or authorized to forward such communication to its destination, (3) to proper accounting or distributing officers of the various communicating centers over which the communication may be passed, (4) to the master of a ship under whom he is serving, (5) in response
to a subpoena issued by a court of competent jurisdiction, or (6) on
demand of other lawful authority. No person not being authorized
by the sender shall intercept any radio communication and divulge
or publish the existence, contents, substance, purport, effect, or
meaning of such intercepted communication to any person. No per-
son not being entitled thereto shall receive or assist in receiving
any interstate or foreign communication by radio and use such com-
munication (or any information therein contained) for his own ben-
efit or for the benefit of another not entitled thereto. No person hav-
ing received any intercepted radio communication or having become
acquainted with the contents, substance, purport, effect, or meaning
of such communication (or any part thereof) knowing that such
communication was intercepted, shall divulge or publish the exist-
ence, contents, substance, purport, effect, or meaning of such com-
munication (or any part thereof) or use such communication (or
any information therein contained) for his own benefit or for the
benefit of another not entitled thereto. This section shall not apply
to the receiving, divulging, publishing, or utilizing the contents of
any radio communication which is broadcast or transmitted by am-
ateurs or others for the use of the general public, or which relates
to ships in distress."

Sec. 804. (a) There is hereby established a National Commiss-
ion for the Review of Federal and State Laws Relating to Wiretapping
and Electronic Surveillance (hereinafter in this section refer-
ded to as the "Commission").

(b) The Commission shall be composed of fifteen members ap-
pointed as follows:

(A) Four appointed by the President of the Senate from
Members of the Senate;

(B) Four appointed by the Speaker of the House of Repre-
sentatives from Members of the House of Representatives; and

(C) Seven appointed by the President of the United States
from all segments of life in the United States, including lawyers,
teachers, artists, businessmen, newspapermen, jurists, policemen,
and community leaders, none of whom shall be officers of the ex-
ecutive branch of the Government.

(c) The President of the United States shall designate a Chairman
from among the members of the Commission. Any vacancy in the
Commission shall not affect its powers but shall be filled in the same
manner in which the original appointment was made.

(d) It shall be the duty of the Commission to conduct a compre-
hensive study and review of the operation of the provisions of this
title, in effect on the effective date of this section, to determine the
effectiveness of such provisions during the six-year period immedi-
ately following the date of their enactment.

(e) (1) Subject to such rules and regulations as may be adopted by
the Commission, the Chairman shall have the power to—

(A) appoint and fix the compensation of an Executive Direct-
or, and such additional staff personnel as he deems necessary,
without regard to the provisions of title 5, United States Code, governing appointments in the competitive service, and without regard to the provisions of chapter 51 and subchapter III of chapter 53 of such title relating to classification and General Schedule pay rates, but at rates not in excess of the maximum rate for GS-18 of the General Schedule under section 5332 of such title; and

(B) procure temporary and intermittent services to the same extent as is authorized by section 3109 of title 5, United States Code, but at rates not to exceed $100 a day for individuals.

(2) In making appointments pursuant to paragraph (1) of this subsection, the Chairman shall include among his appointment individuals determined by the Chairman to be competent social scientists, lawyers, and law enforcement officers.

(f) (1) A member of the Commission who is a Member of Congress shall serve without additional compensation, but shall be reimbursed for travel, subsistence, and other necessary expenses incurred in the performance of duties vested in the Commission.

(2) A member of the Commission from private life shall receive $100 per diem when engaged in the actual performance of duties vested in the Commission, plus reimbursement for travel, subsistence, and other necessary expenses incurred in the performance of such duties.

(g) Each department, agency, and instrumentality of the executive branch of the Government, including independent agencies, is authorized and directed to furnish to the Commission, upon request made by the Chairman, such statistical data, reports, and other information as the Commission deems necessary to carry out its functions under this section. The Chairman is further authorized to call upon the departments, agencies, and other offices of the several States to furnish such statistical data, reports, and other information as the Commission deems necessary to carry out its functions under this section.

(h) The Commission shall make such interim reports as it deems advisable, and it shall make a final report of its findings and recommendations to the President of the United States and to the Congress within the one-year period following the effective date of this subsection. Sixty days after submission of its final report, the Commission shall cease to exist.

(i) (1) Except as provided in paragraph (2) of this subsection, any member of the Commission is exempted, with respect to his appointment, from the operation of sections 203, 205, 207, and 209 of title 18, United States Code.

(2) The exemption granted by paragraph (1) of this subsection shall not extend—

(A) to the receipt of payment of salary in connection with the appointee's Government service from any source other than the private employer of the appointee at the time of his appointment, or
(B) during the period of such appointment, to the prosecution, by any person so appointed, of any claim against the Government involving any matter with which such person, during such period, is or was directly connected by reason of such appointment.

(j) There is authorized to be appropriated such sum as may be necessary to carry out the provisions of this section.

(k) The foregoing provisions of this section shall take effect upon the expiration of the six-year period immediately following the date of the enactment of this Act.

TITLE IV—STATE FIREARMS CONTROL ASSISTANCE
FINDINGS AND DECLARATION

Sec. 901. (a) The Congress hereby finds and declares—

(1) that there is a widespread traffic in firearms moving in or otherwise affecting interstate or foreign commerce, and that the existing Federal controls over such traffic do not adequately enable the States to control this traffic within their own borders through the exercise of their police power;

(2) that the ease with which any person can acquire firearms other than a rifle or shotgun (including criminals, juveniles without the knowledge or consent of their parents or guardians, narcotics addicts, mental defectives, armed groups who would supplant the functions of duly constituted public authorities, and others whose possession of such weapons is similarly contrary to the public interest) is a significant factor in the prevalence of lawlessness and violent crime in the United States;

(3) that only through adequate Federal control over interstate and foreign commerce in these weapons, and over all persons engaging in the businesses of importing, manufacturing, or dealing in them, can this grave problem be properly dealt with, and effective State and local regulation of this traffic be made possible;

(4) that the acquisition on a mail-order basis of firearms other than a rifle or shotgun by nonlicensed individuals, from a place other than their State of residence, has materially tended to thwart the effectiveness of State laws and regulations, and local ordinances;

(5) that the sale or other disposition of concealable weapons by importers, manufacturers, and dealers holding Federal licenses, to nonresidents of the State in which the licensees' places of business are located, has tended to make ineffective the laws, regulations, and ordinances in the several States and local jurisdictions regarding such firearms;

(6) that there is a causal relationship between the easy availability of firearms other than a rifle or shotgun and youthful criminal behavior, and that such firearms have been widely sold by federally licensed importers and dealers to emotionally immature, or thrill-bent juveniles and minors prone to criminal behavior;
(7) that the United States has become the dumping ground of the castoff surplus military weapons of other nations, and that such weapons, and the large volume of relatively inexpensive pistols and revolvers (largely worthless for sporting purposes), imported into the United States in recent years, has contributed greatly to lawlessness and to the Nation's law enforcement problems;

(8) that the lack of adequate Federal control over interstate and foreign commerce in highly destructive weapons (such as bazookas, mortars, antitank guns, and so forth, and destructive devices such as explosive or incendiary grenades, bombs, missiles, and so forth) has allowed such weapons and devices to fall into the hands of lawless persons, including armed groups who would supplant lawful authority, thus creating a problem of national concern;

(9) that the existing licensing system under the Federal Firearms Act does not provide adequate license fees or proper standards for the granting or denial of licenses, and that this has led to licenses being issued to persons not reasonably entitled thereto, thus distorting the purposes of the licensing system.

(b) The Congress further hereby declares that the purpose of this title is to cope with the conditions referred to in the foregoing subsection, and that it is not the purpose of this title to place any undue or unnecessary Federal restrictions or burdens on law-abiding citizens with respect to the acquisition, possession, or use of firearms appropriate to the purpose of hunting, trap shooting, target shooting, personal protection, or any other lawful activity, and that this title is not intended to discourage or eliminate the private ownership or use of firearms by law-abiding citizens for lawful purposes, or provide for the imposition by Federal regulations of any procedures or requirements other than those reasonably necessary to implement and effectuate the provisions of this title.

Sec. 902. Title 18, United States Code, is amended by inserting after section 917 thereof the following new chapter:

Chapter 44.—FIREARMS

Sec. 921. Definitions.
Sec. 922. Unlawful acts.
Sec. 923. Licensing.
Sec. 924. Penalties.
Sec. 925. Exceptions: Relief from disabilities.
Sec. 926. Rules and regulations.
Sec. 927. Effect on State law.
Sec. 928. Separability clause.

Sec. 921. Definitions
(a) As used in this chapter—

(1) The term 'person' and the term 'whoever' includes any individual, corporation, company, association, firm, partnership, society, or joint stock company.
“(2) The term ‘interstate or foreign commerce’ includes commerce between any State or possession (not including the Canal Zone) and any place outside thereof; or between points within the same State or possession (not including the Canal Zone), but through any place outside thereof; or within any possession or the District of Columbia. The term ‘State’ shall include the Commonwealth of Puerto Rico, the Virgin Islands, and the District of Columbia.

“(3) the term ‘firearm’ means any weapon (including a starter gun) which will or is designed to or may readily be converted to expel a projectile by the action of an explosive; the frame or receiver of any such weapon; or any firearm muffler or firearm silencer; or any destructive device.

“(4) The term ‘destructive device’ means any explosive, incendiary, or poison gas bomb, grenade, mine, rocket, missile, or similar device; and includes any type of weapon which will or is designed to or may readily be converted to expel a projectile by the action of any explosive and having any barrel with a bore of one-half inch or more in diameter.

“(5) The term ‘shotgun’ means a weapon designed or redesigned, made or remade, and intended to be fired from the shoulder and designed or redesigned and made or remade to use the energy of the explosive in a fixed shotgun shell to fire through a smooth bore either a number of ball shot or a single projectile for each single pull of the trigger.

“(6) The term ‘short-barreled shotgun’ means a shotgun having one or more barrels less than eighteen inches in length and any weapon made from a shotgun (whether by alteration, modification, or otherwise) if such weapon as modified has an overall length of less than twenty-six inches.

“(7) The term ‘rifle’ means a weapon designed or redesigned, made or remade, and intended to be fired from the shoulder and designed or redesigned and made or remade to use the energy of the explosive in a fixed metallic cartridge to fire only a single projectile through a rifled bore for each single pull of the trigger.

“(8) The term ‘short-barreled rifle’ means a rifle having one or more barrels less than sixteen inches in length and any weapon made from a rifle (whether by alteration, modification, or otherwise) if such weapon as modified has an overall length of less than twenty-six inches.

“(9) The term ‘importer’ means any person engaged in the business of importing or bringing firearms or ammunition into the United States for purposes of sale or distribution; and the term ‘licensed importer’ means any such person licensed under the provisions of this chapter.

“(10) The term ‘manufacturer’ means any person engaged in the manufacture of firearms or ammunition for purposes of sale or distribution; and the term ‘licensed manufacturer’ means any such person licensed under the provisions of this chapter.
“(11) The term 'dealer' means (A) any person engaged in the business of selling firearms or ammunition at wholesale or retail, (B) any person engaged in the business of repairing such firearms or of making or fitting special barrels, stocks, or trigger mechanisms to firearms or (C) any person who is a pawnbroker. The term 'licensed dealer' means any dealer who is licensed under the provisions of this chapter.

“(12) The term 'pawnbroker' means any person whose business or occupation includes the taking or receiving, by way of pledge or pawn, of any firearm or ammunition as security for the payment or repayment of money.

“(13) The term 'indictment' includes an indictment or an information in any court under which a crime punishable by imprisonment for a term exceeding one year may be prosecuted.

“(14) The term 'fugitive from justice' means any person who has fled from any State or possession to avoid prosecution for a crime punishable by imprisonment for a term exceeding one year or to avoid giving testimony in any criminal proceeding.

“(15) The term 'antique firearm' means any firearm manufactured in or before 1898 (including any matchlock, flintlock, percussion cap, or similar early type of ignition system) or replica thereof, whether actually manufactured before or after the year 1898; and also any firearm using fixed ammunition manufactured in or before 1898, for which ammunition is no longer manufactured in the United States; and is not readily available in the ordinary channels of commercial trade.

“(16) The term 'ammunition' means ammunition for a destructive device; it shall not include shotgun shells or any other ammunition designed for use in a firearm other than a destructive device.

“(17) The term 'Secretary' or 'Secretary of the Treasury' means the Secretary of the Treasury or his delegate.

“(18) The term 'published ordinance' means a published law of any political subdivision of a State which the Secretary of the Treasury determines to be relevant to the enforcement of this chapter and which is contained on a list compiled by the Secretary of the Treasury which list shall be published in the Federal Register, revised annually, and furnished to each licensee under this chapter.

“(b) As used in this chapter—

"(1) The term 'firearm' shall not include an antique firearm.

"(2) The term 'destructive device' shall not include—

"(A) a device which is not designed or redesigned or used or intended for use as a weapon; or

"(B) any device, although originally designed as a weapon, which is redesigned so that it may be used solely as a signaling, linethrowing, safety or similar device; or

"(C) any shotgun other than a short-barreled shotgun; or

"(D) any nonautomatic rifle (other than a short-barreled rifle) generally recognized or particularly suitable for use for the hunting of big game; or

June 19 CRIME CONTROL P.L. 90-351
“(E) surplus obsolete ordnance sold, loaned, or given by the Secretary of the Army pursuant to the provisions of sections 4684(2), 4685, or 4686 of title 1, United States Code; or
“(F) any other device which the Secretary finds is not likely to be used as a weapon.
“(3) The term ‘crime punishable by imprisonment for a term exceeding one year’ shall not include any Federal or State offenses pertaining to antitrust violations, unfair trade practices, restraints of trade, or other similar offenses relating to the regulation of business practices as the Secretary may by regulation designate.

§ 922. Unlawful acts
“(a) It shall be unlawful—
“(1) for any person, except a licensed importer, licensed manufacturer, or licensed dealer, to engage in the business of importing, manufacturing, or dealing in firearms, or ammunition, or in the course of such business to ship, transport, or receive any firearm or ammunition in interstate or foreign commerce.
“(2) for any importer, manufacturer, or dealer licensed under the provisions of this chapter to ship or transport in interstate or foreign commerce, any firearm other than a rifle or shotgun, or ammunition to any person other than a licensed importer, licensed manufacturer, or licensed dealer, except that—
“(A) this paragraph shall not be held to preclude a licensed importer, licensed manufacturer, or licensed dealer from returning a firearm or replacement firearm of the same kind and type to a person from whom it was received;
“(B) this paragraph shall not be held to preclude a licensed importer, licensed manufacturer, or licensed dealer from depositing a firearm for conveyance in the mails to any officer, employee, agent, or watchman who, pursuant to the provisions of section 1715 of title 18 of the United States Code, is eligible to receive through the mails, pistols, revolvers, and other firearms capable of being concealed on the person, for use in connection with his official duty;
“(C) nothing in this paragraph shall be construed as applying in any manner in the District of Columbia, the Commonwealth of Puerto Rico, or any possession of the United States differently than it would apply if the District of Columbia, the Commonwealth of Puerto Rico, or the possession were in fact a State of the United States.
“(3) for any person other than a licensed importer, licensed manufacturer, or licensed dealer to transport into or receive in the State where he resides (or if the person is a corporation or other business entity, in which he maintains a place of business)—
“(A) any firearm, other than a shotgun or rifle, purchased or otherwise obtained by him outside that State;
“(B) any firearm, purchased or otherwise obtained by him outside that State, which it would be unlawful for him to purchase or possess in the State or political subdivision thereof wherein he resides (or if the person is a corporation or other business entity, in which he maintains a place of business).

“(4) for any person, other than a licensed importer, licensed manufacturer, or licensed dealer, to transport in interstate or foreign commerce any destructive device, machinegun (as defined in section 5848 of the Internal Revenue Code of 1954), short-barreled shotgun, or short-barreled rifle, except as specifically authorized by the Secretary.

“(5) for any person to transfer, sell, trade, give, transport, or deliver to any person (other than a licensed importer, licensed manufacturer, or licensed dealer) who resides in any State other than that in which the transferor resides (or in which his place of business is located if the transferor is a corporation or other business entity)—

“(A) any firearm, other than a shotgun or rifle;

“(B) any firearm which the transferee could not lawfully purchase or possess in accord with applicable laws, regulations or ordinances of the State or political subdivision thereof in which the transferee resides (or in which his place of business is located if the transferee is a corporation or other business entity).

“This paragraph shall not apply to transactions between licensed importers, licensed manufacturers, and licensed dealers.

“(6) for any person in connection with the acquisition or attempted acquisition of any firearm from a licensed importer, licensed manufacturer, or licensed dealer, knowingly to make any false or fictitious oral or written statement or to furnish or exhibit any false or fictitious or misrepresented identification, intended or likely to deceive such importer, manufacturer, or dealer with respect to any fact material to the lawfulness of the sale or other disposition of such firearm under the provisions of this chapter.

“(b) It shall be unlawful for any licensed importer, licensed manufacturer, or licensed dealer to sell or deliver—

“(1) any firearm to any individual who the licensee knows or has reasonable cause to believe is less than twenty-one years of age, if the firearm is other than a shotgun or rifle.

“(2) any firearm to any person in any State where the purchase or possession by such person of such firearm would be in violation of any State law or any published ordinance applicable at the place of sale, delivery or other disposition, or in the locality in which such person resides unless the licensee knows or has reasonable cause to believe that the purchase or possession would not be in violation of such State law or such ordinance.
"(3) any firearm to any person who the licensee knows or has reasonable cause to believe does not reside in (or if the person is a corporation or other business entity, does not maintain a place of business in) the State in which the licensee's place of business is located; except that this paragraph shall not apply in the case of a shotgun or rifle.

"(4) to any person any destructive device, machine gun (as defined in section 5848 of the Internal Revenue Code of 1954), short-barreled shotgun, or short-barreled rifle, unless he has in his possession a sworn statement executed by the principal law enforcement officer of the locality wherein the purchaser or person to whom it is otherwise disposed of resides, attesting that there is no provision of law, regulation, or ordinance which would be violated by such person's receipt or possession thereof, and that he is satisfied that it is intended by such person for lawful purposes; and such sworn statement shall be retained by the licensee as a part of the records required to be kept under the provisions of this chapter.

"(5) any firearm to any person unless the licensee notes in his records required to be kept pursuant to section 923 of this chapter, the name, age, and place of residence of such person if the person is an individual, or the identity and principal and local places of business of such person if the person is a corporation or other business entity.

Paragraphs (1), (2), (3) and (4) of this subsection shall not apply to transactions between licensed importers, licensed manufacturers, and licensed dealers.

"(c) It shall be unlawful for any licensed importer, licensed manufacturer, or licensed dealer to sell or otherwise dispose of any firearm or ammunition to any person, knowing or having reasonable cause to believe that such person is a fugitive from justice or is under indictment or has been convicted in any court of a crime punishable by imprisonment for a term exceeding one year. This subsection shall not apply with respect to sale or disposition of a firearm to a licensed importer, licensed manufacturer, or licensed dealer pursuant to subsection (b) of section 925 of this chapter is not precluded from dealing in firearms, or to a person who has been granted relief from disabilities pursuant to subsection (c) of section 925 of this chapter.

"(d) It shall be unlawful for any common or contract carrier to transport or deliver in interstate or foreign commerce any firearm with knowledge or reasonable cause to believe that the shipment, transportation, or receipt thereof would be in violation of the provisions of this chapter.

"(e) It shall be unlawful for any person who is under indictment or who has been convicted in any court of a crime punishable by imprisonment for a term exceeding one year, or who is a fugitive from justice, to ship or transport any firearm or ammunition in interstate or foreign commerce.
“(f) It shall be unlawful for any person who is under indictment or who has been convicted in any court of a crime punishable by imprisonment for a term exceeding one year, or is a fugitive from justice, to receive any firearm or ammunition which has been shipped or transported in interstate or foreign commerce.

“(g) It shall be unlawful for any person to transport or ship in interstate or foreign commerce, any stolen firearm or stolen ammunition, knowing or having reasonable cause to believe the same to have been stolen.

“(h) It shall be unlawful for any person to receive, conceal, store, barter, sell, or dispose of any stolen firearm or stolen ammunition, or pledge or accept as security for a loan any stolen firearm or stolen ammunition, moving as or which is a part of or which constitutes interstate or foreign commerce, knowing or having reasonable cause to believe the same to have been stolen.

“(i) It shall be unlawful for any person knowingly to transport, ship, or receive, in interstate or foreign commerce, any firearm the importer’s or manufacturer’s serial number of which has been removed, obliterated, or altered.

“(j) It shall be unlawful for any person knowingly to import or bring into the United States or any possession thereof any firearm or ammunition, except as provided in subsection (d) of section 925 of this chapter; and it shall be unlawful for any person knowingly to receive any firearm or ammunition which has been imported or brought into the United States or any possession thereof in violation of the provisions of this chapter.

“(k) It shall be unlawful for any licensed importer, licensed manufacturer, or licensed dealer knowingly to make any false entry in, or to fail to make appropriate entry in or to fail to properly maintain, any record which he is required to keep pursuant to section 923 of this chapter or regulations promulgated thereunder.

“§ 923. Licensing

“(a) No person shall engage in business as a firearms or ammunition importer, manufacturer, or dealer until he has filed an application with, and received a license to do so from, the Secretary. The application shall be in such form and contain such information as the Secretary shall by regulation prescribe. Each applicant shall be required to pay a fee for obtaining such a license, a separate fee being required for each place in which the applicant is to do business, as follows:

“(1) If a manufacturer—

“(A) of destructive devices and/or ammunition a fee of $1,000 per year;

“(B) of firearms other than destructive devices a fee of $500 per year.

“(2) If an importer—

“(A) of destructive devices and/or ammunition a fee of $1,000 per year;

“(B) of firearms other than destructive devices a fee of $500 per year.
er for the purpose of inspecting or examining any records or documents required to be kept by such importer or manufacturer or dealer under the provisions of this chapter or regulations issued pursuant thereto, and any firearms or ammunition kept or stored by such importer, manufacturer, or dealer at such premises. Upon the request of any State, or possession, or any political subdivision thereof, the Secretary of the Treasury may make available to such State, or possession, or any political subdivision thereof, any information which he may obtain by reason of the provisions of this chapter with respect to the identification of persons within such State, or possession, or political subdivision thereof, who have purchased or received firearms or ammunition, together with a description of such firearms or ammunition.

"(e) Licenses issued under the provisions of subsection (b) of this section shall be kept posted and kept available for inspection on the business premises covered by the license.

"(f) Licensed importers and licensed manufacturers shall identify in such manner as the Secretary shall by regulations prescribe, each firearm imported or manufactured by such importer or manufacturer.

§ 924. Penalties

"(a) Whoever violates any provision of this chapter or knowingly makes any false statement or representation with respect to the information required by the provisions of this chapter to be kept in the records of a person licensed under this chapter, or in applying for any license or exemption or relief from disability under the provisions of this chapter, shall be fined not more than $5,000 or imprisoned not more than five years, or both.

"(b) Whoever, with intent to commit therewith an offense punishable by imprisonment for a term exceeding one year, or with knowledge or reasonable cause to believe that an offense punishable by imprisonment for a term exceeding one year is to be committed therewith, ships, transports, or receives a firearm in interstate or foreign commerce shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

"(c) Any firearm or ammunition involved in, or used or intended to be used in, any violation of the provisions of this chapter, or a rule or regulation promulgated thereunder, or violation of any other criminal law of the United States, shall be subject to seizure and forfeiture and all provisions of the Internal Revenue Code of 1954 relating to the seizure, forfeiture, and disposition of firearms, as defined in section 5848(1) of said Code, shall, so far as applicable, extend to seizures and forfeitures under the provisions of this chapter.

§ 925. Exceptions: relief from disabilities

"(a) The provisions of this chapter shall not apply with respect to the transportation, shipment, receipt, or importation of any firearm or ammunition imported for, or sold or shipped to, or issued for the use of the United States or any department, or agency thereof;
or any State or possession, or any department, agency, or political subdivision thereof.

"(b) A licensed importer, licensed manufacturer, or licensed dealer who is indicted for a crime punishable by imprisonment for a term exceeding one year, may, notwithstanding any other provisions of this chapter, continue operations pursuant to his existing license (provided that prior to the expiration of the term of the existing license timely application is made for a new license) during the term of such indictment and until any conviction pursuant to the indictment becomes final.

"(c) A person who has been convicted of a crime punishable by imprisonment for a term exceeding one year (other than a crime involving the use of a firearm or other weapon or a violation of this chapter or of the National Firearms Act) may make application to the Secretary for relief from the disabilities under this chapter incurred by reason of such conviction, and the Secretary may grant such relief if it is established to his satisfaction that the circumstances regarding the conviction, and the applicant's record and reputation, are such that the applicant will not be likely to conduct his operations in an unlawful manner, and that the granting of the relief would not be contrary to the public interest. A licensee conducting operations under this chapter, who makes application for relief from the disabilities incurred under this chapter by reason of such a conviction, shall not be barred by such conviction from further operations under his license pending final action on an application for relief filed pursuant to this section. Whenever the Secretary grants relief to any person pursuant to this section he shall promptly publish in the Federal Register notice of such action, together with the reasons therefor.

"(d) The Secretary may authorize a firearm to be imported or brought into the United States or any possession thereof if the person importing or bringing in the firearm establishes to the satisfaction of the Secretary that the firearm—

"(1) is being imported or brought in for scientific or research purposes, or is for use in connection with competition or training pursuant to chapter 401 of title 10 of the United States Code; or

"(2) is an unserviceable firearm, other than a machine gun as defined by 5848(2) of the Internal Revenue Code of 1954 (not readily restorable to firing condition), imported or brought in as a curio or museum piece; or

"(3) is of a type that does not fall within the definition of a firearm as defined in section 5848(1) of the Internal Revenue Code of 1954 and is generally recognized as particularly suitable for or readily adaptable to sporting purposes, and in the case of surplus military firearms is a rifle or shotgun; or

"(4) was previously taken out of the United States or a possession by the person who is bringing in the firearm:

Provided, That the Secretary may permit the conditional importation or bringing in of a firearm for examination and testing in connection
with the making of a determination as to whether the importation or bringing in of such firearm will be allowed under this subsection.

"§ 926. Rules and regulations

The Secretary may prescribe such rules and regulations as he deems reasonably necessary to carry out the provisions of this chapter. The Secretary shall give reasonable public notice, and afford to interested parties opportunity for hearing, prior to prescribing such rules and regulations.

"§ 927. Effect on State law

No provision of this chapter shall be construed as indicating an intent on the part of the Congress to occupy the field in which such provision operates to the exclusion of the law of any State or possession on the same subject matter, unless there is a direct and positive conflict between such provision and the law of the State or possession so that the two cannot be reconciled or consistently stand together.

"§ 928. Separability

If any provision of this chapter or the application thereof to any person or circumstance is held invalid, the remainder of the chapter and the application of such provision to other persons not similarly situated or to other circumstances shall not be affected thereby.

Sec. 903. The administration and enforcement of the amendment made by this title shall be vested in the Secretary of the Treasury.

Sec. 904. Nothing in this title or amendment made thereby shall be construed as modifying or affecting any provision of—

(a) the National Firearms Act (chapter 53 of the Internal Revenue Code of 1954); or

(b) section 414 of the Mutual Security Act of 1954 (22 U.S.C. 1934), as amended, relating to munitions control; or

(c) section 1715 of title 18, United States Code, relating to nonmailable firearms.

Sec. 905. The table of contents to "Part I.—Crimes" of title 18, United States Code, is amended by inserting after

"43. False personation .......................... 911"
a new chapter reference as follows:

"44. Firearms ........................................ 921".


Sec. 907. The amendments made by this title shall become effective one hundred and eighty days after the date of its enactment; except that repeal of the Federal Firearms Act shall not in itself terminate any valid license issued pursuant to that Act and any such license shall be deemed valid until it shall expire according to its terms unless it be sooner revoked or terminated pursuant to applicable provisions of law.
TITLE V—DISQUALIFICATION FOR ENGAGING IN RIOTS AND CIVIL DISORDERS

Sec. 1001. (a) Subchapter II of chapter 73 of title 5, United States Code, is amended by adding immediately after section 7312 the following new section:

"§ 7313. Riots and civil disorders

(a) An individual convicted by any Federal, State, or local court of competent jurisdiction of—

"(1) inciting a riot or civil disorder;
"(2) organizing, promoting, encouraging, or participating in a riot or civil disorder;
"(3) aiding or abetting any person in committing any offense specified in clause (1) or (2); or
"(4) any offense determined by the head of the employing agency to have been committed in furtherance of, or while participating in, a riot or civil disorder;

shall, if the offense for which he is convicted is a felony, be ineligible to accept or hold any position in the Government of the United States or in the government of the District of Columbia for the five years immediately following the date upon which his conviction becomes final. Any such individual holding a position in the Government of the United States or the government of the District of Columbia on the date his conviction becomes final shall be removed from such position.

"(b) For the purposes of this section, ‘felony’ means any offense for which imprisonment is authorized for a term exceeding one year.”

(b) The analysis of chapter 73 of title 5, United States Code, immediately preceding section 7301 of such title, is amended by striking out the analysis of subchapter II and inserting in lieu thereof the following:

"SUBCHAPTER II—EMPLOYMENT LIMITATIONS

"Sec.
"7311. Loyalty and striking.
"7312. Employment and clearance; individuals removed from national security.
"7313. Riots and civil disorders.”

(c) The heading of subchapter II of chapter 73 of title 5, United States Code, immediately preceding section 7311 of such title, is amended to read as follows:

"SUBCHAPTER II—EMPLOYMENT LIMITATIONS”.

Sec. 1002. The provisions of section 1001(a) of this title shall apply only with respect to acts referred to in section 7313(a) (1)-(4) of title 5, United States Code, as added by section 1001 of this title, which are committed after the date of enactment of this title.
TITLE VI—CONFIRMATION OF THE DIRECTOR OF
THE FEDERAL BUREAU OF INVESTIGATION

Sec. 1101. Effective as of the day following the date on which the
present incumbent in the office of Director ceases to serve as such,
the Director of the Federal Bureau of Investigation shall be appoint-
ed by the President, by and with the advice and consent of the Senate,
and shall receive compensation at the rate prescribed for level II of
the Federal Executive Salary Schedule.

TITLE VII—UNLAWFUL POSSESSION OR RECEIPT OF
FIREARMS

Sec. 1201. The Congress hereby find and declares that the receipt,
possession, or transportation of a firearm by felons, veterans who
are other than honorably discharged, mental incompetents, aliens
who are illegally in the country, and former citizens who have re-
nounced their citizenship, constitutes—

(1) a burden on commerce or threat affecting the free flow
of commerce,

(2) a threat to the safety of the President of the United States
and Vice President of the United States,

(3) an impediment or a threat to the exercise of free speech
and the free exercise of a religion guaranteed by the first amend-
ment to the Constitution of the United States, and

(4) a threat to the continued and effective operation of the
Government of the United States and of the government of each
State guaranteed by article IV of the Constitution.

Sec. 1202. (a) Any person who—

(1) has been convicted by a court of the United States or of a
State or any political subdivision thereof of a felony, or

(2) has been discharged from the Armed Forces under other-
than honorable conditions, or

(3) has been adjudged by a court of the United States or of a
State or any political subdivision thereof of being mentally
incompetent, or

(4) having been a citizen of the United States has renounced
his citizenship, or

(5) being an alien is illegally or unlawfully in the United
States,
and who receives, possesses, or transports in commerce or affecting
commerce, after the date of enactment of this Act, any firearm shall
be fined not more than $10,000 or imprisoned for not more than two
years, or both.

(b) Any individual who to his knowledge and while being employed
by any person who—

(1) has been convicted by a court of the United States or of a
State or any political subdivision thereof of a felony, or
plosive in a fixed metallic cartridge to fire only a single projectile through a rifled bore for each single pull of the trigger.

Sec. 1203. This title shall not apply to—

(1) any prisoner who by reason of duties connected with law enforcement has expressly been entrusted with a firearm by competent authority of the prison; and

(2) any person who had been pardoned by the President of the United States or the chief executive of a State and has expressly been authorized by the President or such chief executive, as the case may be, to receive, possess, or transport in commerce a firearm.

TITLE VIII—PROVIDING FOR AN APPEAL BY THE UNITED STATES FROM DECISIONS SUSTAINING MOTIONS TO SUPPRESS EVIDENCE

Sec. 1301. (a) Section 3731 of title 18, United States Code, is amended by inserting after the seventh paragraph the following new paragraph:

"From an order, granting a motion for return of seized property or a motion to suppress evidence, made before the trial of a person charged with a violation of any law of the United States, if the United States attorney certifies to the judge who granted such motion that the appeal is not taken for purpose of delay and that the evidence is a substantial proof of the charge pending against the defendant."

(b) Such section is amended by striking out in the third paragraph from the end "the defendant shall be admitted to bail on his own recognizance" and inserting "the defendant shall be released in accordance with chapter 207 of this title".


(a) by inserting "(a)" immediately before "In all"; and

(b) by adding at the end thereof the following new subsection:

"(b) The United States may also appeal an order of the District of Columbia Court of General Sessions, granting a motion for return of seized property or a motion to suppress evidence, made before the trial of a person charged with a violation of any law of the United States, if the United States attorney conducting the prosecution for such violation certifies to the judge who granted such motion that the appeal is not taken for purpose of delay and that the evidence is a substantial proof of the charge pending against the defendant. Pending the prosecution and determination of such appeal, the defendant, if in custody for such violation, shall be released in accordance with chapter 207 of title 18, United States Code."
TITLE IX—ADDITIONAL GROUNDS FOR ISSUING WARRANT

Sec. 1401. (a) Chapter 204 of title 18, United States Code, is amended by inserting immediately after section 3103 the following new section:

"§ 3103a. Additional grounds for issuing warrant

"In addition to the grounds for issuing a warrant in section 3103 of this title, a warrant may be issued to search for and seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States."

(b) The table of sections for chapter 205 of title 18, United States Code is amended by inserting after the item relating to section 3103 the following:

"3103a. Additional grounds for issuing warrant."

TITLE X—PROHIBITING EXTORTION AND THREATS IN THE DISTRICT OF COLUMBIA

Sec. 1501. Whoever with intent to extort from any person, firm, association, or corporation, any money or other thing of value: (1) transmits within the District of Columbia any communication containing any demand or request for ransom or reward for the release of any kidnapped person, shall be fined not more than $5,000 or imprisoned not more than twenty years, or both; (2) transmits within the District of Columbia any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined not more than $5,000 or imprisoned not more than twenty years, or both; or (3) transmits within the District of Columbia any communication containing any threat to injure the property or reputation of the recipient of the communication or of another or the reputation of a deceased person or any threat to accuse the recipient of the communication or any other person of a crime, shall be fined not more than $5,000 or imprisoned not more than twenty years, or both.

Sec. 1502. Whoever threatens within the District of Columbia to kidnap any person or to injure the person of another or physically damage the property of any person or of another person, in whole or in part, shall be fined not more than $5,000 or imprisoned not more than twenty years, or both.

TITLE XI—GENERAL PROVISIONS

Sec. 1601. If the provisions of any part of this Act or any amendments made thereby or the application thereof to any person or circumstances be held invalid, the provisions of the other parts and their application to other persons or circumstances shall not be affected thereby.

Approved June 19, 1968.
Securing Communication of Protected Client Information

A lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

I. Introduction

In Formal Opinion 99-413 this Committee addressed a lawyer’s confidentiality obligations for email communications with clients. While the basic obligations of confidentiality remain applicable today, the role and risks of technology in the practice of law have evolved since 1999 prompting the need to update Opinion 99-413.

Formal Opinion 99-413 concluded: “Lawyers have a reasonable expectation of privacy in communications made by all forms of e-mail, including unencrypted e-mail sent on the Internet, despite some risk of interception and disclosure. It therefore follows that its use is consistent with the duty under Rule 1.6 to use reasonable means to maintain the confidentiality of information relating to a client’s representation.”

Unlike 1999 where multiple methods of communication were prevalent, today, many lawyers primarily use electronic means to communicate and exchange documents with clients, other lawyers, and even with other persons who are assisting a lawyer in delivering legal services to clients.

Since 1999, those providing legal services now regularly use a variety of devices to create, transmit and store confidential communications, including desktop, laptop and notebook

*The opinion below is a revision of, and replaces Formal Opinion 477 as issued by the Committee May 11, 2017. This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2016. The laws, court rules, regulations, rules of professional conduct, and opinions promulgated in individual jurisdictions are controlling.

computers, tablet devices, smartphones, and cloud resource and storage locations. Each device and each storage location offer an opportunity for the inadvertent or unauthorized disclosure of information relating to the representation, and thus implicate a lawyer’s ethical duties.⁴

In 2012 the ABA adopted “technology amendments” to the Model Rules, including updating the Comments to Rule 1.1 on lawyer technological competency and adding paragraph (c) and a new Comment to Rule 1.6, addressing a lawyer’s obligation to take reasonable measures to prevent inadvertent or unauthorized disclosure of information relating to the representation.

At the same time, the term “cybersecurity” has come into existence to encompass the broad range of issues relating to preserving individual privacy from intrusion by nefarious actors throughout the internet. Cybersecurity recognizes a post-Opinion 99-413 world where law enforcement discusses hacking and data loss in terms of “when,” and not “if.”⁵ Law firms are targets for two general reasons: (1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and (2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client.⁶

The Model Rules do not impose greater or different duties of confidentiality based upon the method by which a lawyer communicates with a client. But how a lawyer should comply with the core duty of confidentiality in an ever-changing technological world requires some reflection.

Against this backdrop we describe the “technology amendments” made to the Model Rules in 2012, identify some of the technology risks lawyers face, and discuss factors other than the Model Rules of Professional Conduct that lawyers should consider when using electronic means to communicate regarding client matters.

II. Duty of Competence

Since 1983, Model Rule 1.1 has read: “A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.”⁶ The scope of this requirement was

---


4. “Cybersecurity” is defined as “measures taken to protect a computer or computer system (as on the internet) against unauthorized access or attack.” CYBERSECURITY, MERRIAM WEBSTER, http://www.merriam-webster.com/dictionary/cybersecurity (last visited Sept. 10, 2016). In 2012 the ABA created the Cybersecurity Legal Task Force to help lawyers grapple with the legal challenges created by cyberspace. In 2013 the Task Force published The ABA Cybersecurity Handbook: A Resource For Attorneys, Law Firms, and Business Professionals.

5. Bradford A. Bleier, Unit Chief to the Cyber National Security Section in the FBI’s Cyber Division, indicated that “[l]aw firms have tremendous concentrations of really critical private information, and breaking into a firm’s computer system is a really optimal way to obtain economic and personal security information.” Ed Finkel, Cyberspace Under Siege, A.B.A. J., Nov. 1, 2010.

clarified in 2012 when the ABA recognized the increasing impact of technology on the practice of law and the duty of lawyers to develop an understanding of that technology. Thus, Comment [8] to Rule 1.1 was modified to read:

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (Emphasis added.)

Regarding the change to Rule 1.1’s Comment, the ABA Commission on Ethics 20/20 explained:

Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [6] [renumbered as Comment [8]] specifies that, to remain competent, lawyers need to “keep abreast of changes in the law and its practice.” The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today’s environment without knowing how to use email or create an electronic document.

III. Duty of Confidentiality

In 2012, amendments to Rule 1.6 modified both the rule and the commentary about what efforts are required to preserve the confidentiality of information relating to the representation. Model Rule 1.6(a) requires that “A lawyer shall not reveal information relating to the representation of a client” unless certain circumstances arise. The 2012 modification added a new duty in paragraph (c) that: “A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.”

7. Id. at 43.
8. ABA COMMISSION ON ETHICS 20/20 REPORT 105A (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf. The 20/20 Commission also noted that modification of Comment [6] did not change the lawyer’s substantive duty of competence: “Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase ‘including the benefits and risks associated with relevant technology,’ would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer’s general ethical duty to remain competent.”
9. MODEL RULES OF PROF’L CONDUCT R. 1.6(a) (2016).
10. Id. at (c).
Amended Comment [18] explains:

Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

At the intersection of a lawyer’s competence obligation to keep “abreast of knowledge of the benefits and risks associated with relevant technology,” and confidentiality obligation to make “reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client,” lawyers must exercise reasonable efforts when using technology in communicating about client matters. What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors. In turn, those factors depend on the multitude of possible types of information being communicated (ranging along a spectrum from highly sensitive information to insignificant), the methods of electronic communications employed, and the types of available security measures for each method.\textsuperscript{11}

Therefore, in an environment of increasing cyber threats, the Committee concludes that, adopting the language in the ABA Cybersecurity Handbook, the reasonable efforts standard:

\textbf{\ldots} rejects requirements for specific security measures (such as firewalls, passwords, and the like) and instead adopts a fact-specific approach to business security obligations that requires a “process” to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments.\textsuperscript{12}

Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c) includes nonexclusive factors to guide lawyers in making a “reasonable efforts” determination. Those factors include:

- the sensitivity of the information,

\textsuperscript{11} The 20/20 Commission’s report emphasized that lawyers are not the guarantors of data safety. It wrote:

“[t]o be clear, paragraph (c) does not mean that a lawyer engages in professional misconduct any time a client’s confidences are subject to unauthorized access or disclosed inadvertently or without authority. A sentence in Comment [16] makes this point explicitly. The reality is that disclosures can occur even if lawyers take all reasonable precautions. The Commission, however, believes that it is important to state in the black letter of Model Rule 1.6 that lawyers have a duty to take reasonable precautions, even if those precautions will not guarantee the protection of confidential information under all circumstances.”

\textsuperscript{12} ABA CYBERSECURITY HANDBOOK, supra note 3, at 48-49.
• the likelihood of disclosure if additional safeguards are not employed,
• the cost of employing additional safeguards,
• the difficulty of implementing the safeguards, and
• the extent to which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

A fact-based analysis means that particularly strong protective measures, like encryption, are warranted in some circumstances. Model Rule 1.4 may require a lawyer to discuss security safeguards with clients. Under certain circumstances, the lawyer may need to obtain informed consent from the client regarding whether to use enhanced security measures, the costs involved, and the impact of those costs on the expense of the representation where nonstandard and not easily available or affordable security methods may be required or requested by the client. Reasonable efforts, as it pertains to certain highly sensitive information, might require avoiding the use of electronic methods or any technology to communicate with the client altogether, just as it warranted avoiding the use of the telephone, fax and mail in Formal Opinion 99-413.

In contrast, for matters of normal or low sensitivity, standard security methods with low to reasonable costs to implement, may be sufficient to meet the reasonable-efforts standard to protect client information from inadvertent and unauthorized disclosure.

In the technological landscape of Opinion 99-413, and due to the reasonable expectations of privacy available to email communications at the time, unencrypted email posed no greater risk of interception or disclosure than other non-electronic forms of communication. This basic premise remains true today for routine communication with clients, presuming the lawyer has implemented basic and reasonably available methods of common electronic security measures. Thus, the use of unencrypted routine email generally remains an acceptable method of lawyer-client communication.

However, cyber-threats and the proliferation of electronic communications devices have changed the landscape and it is not always reasonable to rely on the use of unencrypted email. For example, electronic communication through certain mobile applications or on message boards or via unsecured networks may lack the basic expectation of privacy afforded to email communications. Therefore, lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters, applying the Comment [18] factors to determine what effort is reasonable.

13. MODEL RULES OF PROF’L CONDUCT R. 1.6 cmt. [18] (2016). “The [Ethics 20/20] Commission examined the possibility of offering more detailed guidance about the measures that lawyers should employ. The Commission concluded, however, that technology is changing too rapidly to offer such guidance and that the particular measures lawyers should use will necessarily change as technology evolves and as new risks emerge and new security procedures become available.” ABA COMMISSION REPORT 105A, supra note 8, at 5.
14. See item 3 below.
While it is beyond the scope of an ethics opinion to specify the reasonable steps that lawyers should take under any given set of facts, we offer the following considerations as guidance:

1. Understand the Nature of the Threat.

Understanding the nature of the threat includes consideration of the sensitivity of a client’s information and whether the client’s matter is a higher risk for cyber intrusion. Client matters involving proprietary information in highly sensitive industries such as industrial designs, mergers and acquisitions or trade secrets, and industries like healthcare, banking, defense or education, may present a higher risk of data theft.15 “Reasonable efforts” in higher risk scenarios generally means that greater effort is warranted.

2. Understand How Client Confidential Information is Transmitted and Where It Is Stored.

A lawyer should understand how their firm’s electronic communications are created, where client data resides, and what avenues exist to access that information. Understanding these processes will assist a lawyer in managing the risk of inadvertent or unauthorized disclosure of client-related information. Every access point is a potential entry point for a data loss or disclosure. The lawyer’s task is complicated in a world where multiple devices may be used to communicate with or about a client and then store those communications. Each access point, and each device, should be evaluated for security compliance.


Model Rule 1.6(c) requires a lawyer to make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client. As Comment [18] makes clear, what is deemed to be “reasonable” may vary, depending on the facts and circumstances of each case. Electronic disclosure of, or access to, client communications can occur in different forms ranging from a direct intrusion into a law firm’s systems to theft or interception of information during the transmission process. Making reasonable efforts to protect against unauthorized disclosure in client communications thus includes analysis of security measures applied to both disclosure and access to a law firm’s technology system and transmissions.

A lawyer should understand and use electronic security measures to safeguard client communications and information. A lawyer has a variety of options to safeguard communications including, for example, using secure internet access methods to communicate, access and store client information (such as through secure Wi-Fi, the use of a Virtual Private Network, or another secure internet portal), using unique complex

---

Formal Opinion 477R

passwords, changed periodically, implementing firewalls and anti-Malware/Anti-Spyware/Antivirus software on all devices upon which client confidential information is transmitted or stored, and applying all necessary security patches and updates to operational and communications software. Each of these measures is routinely accessible and reasonably affordable or free. Lawyers may consider refusing access to firm systems to devices failing to comply with these basic methods. It also may be reasonable to use commonly available methods to remotely disable lost or stolen devices, and to destroy the data contained on those devices, especially if encryption is not also being used.

Other available tools include encryption of data that is physically stored on a device and multi-factor authentication to access firm systems.

In the electronic world, “delete” usually does not mean information is permanently deleted, and “deleted” data may be subject to recovery. Therefore, a lawyer should consider whether certain data should ever be stored in an unencrypted environment, or electronically transmitted at all.


Different communications require different levels of protection. At the beginning of the client-lawyer relationship, the lawyer and client should discuss what levels of security will be necessary for each electronic communication about client matters. Communications to third parties containing protected client information requires analysis to determine what degree of protection is appropriate. In situations where the communication (and any attachments) are sensitive or warrant extra security, additional electronic protection may be required. For example, if client information is of sufficient sensitivity, a lawyer should encrypt the transmission and determine how to do so to sufficiently protect it, and consider the use of password protection for any attachments. Alternatively, lawyers can consider the use of a well vetted and secure third-party cloud based file storage system to exchange documents normally attached to emails.

Thus, routine communications sent electronically are those communications that do not contain information warranting additional security measures beyond basic methods. However, in some circumstances, a client’s lack of technological sophistication or the limitations of technology available to the client may require alternative non-electronic forms of communication altogether.

A lawyer also should be cautious in communicating with a client if the client uses computers or other devices subject to the access or control of a third party. If so, the attorney-client privilege and confidentiality of communications and attached documents may be waived. Therefore, the lawyer should warn the client about the risk of sending or receiving electronic communications using a computer or other device, or email account, to which a third party has, or may gain, access.

5. Label Client Confidential Information.

Lawyers should follow the better practice of marking privileged and confidential client communications as “privileged and confidential” in order to alert anyone to whom the communication was inadvertently disclosed that the communication is intended to be privileged and confidential. This can also consist of something as simple as appending a message or “disclaimer” to client emails, where such a disclaimer is accurate and appropriate for the communication.

Model Rule 4.4(b) obligates a lawyer who “knows or reasonably should know” that he has received an inadvertently sent “document or electronically stored information relating to the representation of the lawyer’s client” to promptly notify the sending lawyer. A clear and conspicuous appropriately used disclaimer may affect whether a recipient lawyer’s duty under Model Rule 4.4(b) for inadvertently transmitted communications is satisfied.

---

17. ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 11-459, Duty to Protect the Confidentiality of E-mail Communications with One’s Client (2011). Formal Op. 11-459 was issued prior to the 2012 amendments to Rule 1.6. These amendments added new Rule 1.6(c), which provides that lawyers “shall” make reasonable efforts to prevent the unauthorized or inadvertent access to client information. See, e.g., Scott v. Beth Israel Med. Center, Inc., Civ. A. No. 3:04-CV-139-RJC-DCK, 847 N.Y.S.2d 436 (Sup. Ct. 2007); Mason v. ILS Tech., LLC, 2008 WL 731557, 2008 BL 298576 (W.D.N.C. 2008); Holmes v. Petrovich Dev Co., LLC, 191 Cal. App. 4th 1047 (2011) (employee communications with lawyer over company owned computer not privileged); Bingham v. BayCare Health Sys., 2016 WL 3917513, 2016 BL 233476 (M.D. Fla. July 20, 2016) (collecting cases on privilege waiver for privileged emails sent or received through an employer’s email server).

18. Some state bar ethics opinions have explored the circumstances under which email communications should be afforded special security protections. See, e.g., Tex. Prof’l Ethics Comm. Op. 648 (2015) that identified six situations in which a lawyer should consider whether to encrypt or use some other type of security precaution:
- communicating highly sensitive or confidential information via email or unencrypted email connections;
- sending an email to or from an account that the email sender or recipient shares with others;
- sending an email to a client when it is possible that a third person (such as a spouse in a divorce case) knows the password to the email account, or to an individual client at that client’s work email account, especially if the email relates to a client’s employment dispute with his employer…;
- sending an email from a public computer or a borrowed computer or where the lawyer knows that the emails the lawyer sends are being read on a public or borrowed computer or on an insecure network;
- sending an email if the lawyer knows that the email recipient is accessing the email on devices that are potentially accessible to third persons or are not protected by a password; or
- sending an email if the lawyer is concerned that the NSA or other law enforcement agency may read the lawyer’s email communication, with or without a warrant.

19. See Veteran Med. Prods. v. Bionix Dev. Corp., Case No. 1:05-cv-655, 2008 WL 696546 at *8, 2008 BL 51876 at *8 (W.D. Mich. Mar. 13, 2008) (email disclaimer that read “this email and any files transmitted with are confidential and are intended solely for the use of the individual or entity to whom they are addressed” with nondisclosure constitutes a reasonable effort to maintain the secrecy of its business plan).

Model Rule 5.1 provides that a partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct. Model Rule 5.1 also provides that lawyers having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct. In addition, Rule 5.3 requires lawyers who are responsible for managing and supervising nonlawyer assistants to take reasonable steps to reasonably assure that the conduct of such assistants is compatible with the ethical duties of the lawyer. These requirements are as applicable to electronic practices as they are to comparable office procedures.

In the context of electronic communications, lawyers must establish policies and procedures, and periodically train employees, subordinates and others assisting in the delivery of legal services, in the use of reasonably secure methods of electronic communications with clients. Lawyers also must instruct and supervise on reasonable measures for access to and storage of those communications. Once processes are established, supervising lawyers must follow up to ensure these policies are being implemented and partners and lawyers with comparable managerial authority must periodically reassess and update these policies. This is no different than the other obligations for supervision of office practices and procedures to protect client information.

7. Conduct Due Diligence on Vendors Providing Communication Technology.

Consistent with Model Rule 1.6(c), Model Rule 5.3 imposes a duty on lawyers with direct supervisory authority over a nonlawyer to make “reasonable efforts to ensure that” the nonlawyer’s “conduct is compatible with the professional obligations of the lawyer.”

In ABA Formal Opinion 08-451, this Committee analyzed Model Rule 5.3 and a lawyer’s obligation when outsourcing legal and nonlegal services. That opinion identified several issues a lawyer should consider when selecting the outsource vendor, to meet the lawyer’s due diligence and duty of supervision. Those factors also apply in the analysis of vendor selection in the context of electronic communications. Such factors may include:

- reference checks and vendor credentials;
- vendor’s security policies and protocols;
- vendor’s hiring practices;
- the use of confidentiality agreements;
- vendor’s conflicts check system to screen for adversity; and
the availability and accessibility of a legal forum for legal relief for violations of the vendor agreement.

Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education. 20

Since the issuance of Formal Opinion 08-451, Comment [3] to Model Rule 5.3 was added to address outsourcing, including “using an Internet-based service to store client information.” Comment [3] provides that the “reasonable efforts” required by Model Rule 5.3 to ensure that the nonlawyer’s services are provided in a manner that is compatible with the lawyer’s professional obligations “will depend upon the circumstances.” Comment [3] contains suggested factors that might be taken into account:

- the education, experience, and reputation of the nonlawyer;
- the nature of the services involved;
- the terms of any arrangements concerning the protection of client information; and
- the legal and ethical environments of the jurisdictions in which the services will be performed particularly with regard to confidentiality.

Comment [3] further provides that when retaining or directing a nonlawyer outside of the firm, lawyers should communicate “directions appropriate under the circumstances to give reasonable assurance that the nonlawyer’s conduct is compatible with the professional obligations of the lawyer.” 21 If the client has not directed the selection of the outside nonlawyer vendor, the lawyer has the responsibility to monitor how those services are being performed. 22

Even after a lawyer examines these various considerations and is satisfied that the security employed is sufficient to comply with the duty of confidentiality, the lawyer must periodically reassess these factors to confirm that the lawyer’s actions continue to comply with the ethical obligations and have not been rendered inadequate by changes in circumstances or technology.

21. The ABA’s catalog of state bar ethics opinions applying the rules of professional conduct to cloud storage arrangements involving client information can be found at: http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html.
22. By contrast, where a client directs the selection of a particular nonlawyer service provider outside the firm, “the lawyer ordinarily should agree with the client concerning the allocation of responsibility for monitoring as between the client and the lawyer.” MODEL RULES OF PROF’L CONDUCT R. 5.3 cmt. [4] (2016). The concept of monitoring recognizes that although it may not be possible to “directly supervise” a client directed nonlawyer outside the firm performing services in connection with a matter, a lawyer must nevertheless remain aware of how the nonlawyer services are being performed. ABA COMMISSION ON ETHICS 20/20 REPORT 105C, at 12 (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105c_filed_may_2012.auth.checkdam.pdf.
IV. Duty to Communicate

Communications between a lawyer and client generally are addressed in Rule 1.4. When the lawyer reasonably believes that highly sensitive confidential client information is being transmitted so that extra measures to protect the email transmission are warranted, the lawyer should inform the client about the risks involved. The lawyer and client then should decide whether another mode of transmission, such as high level encryption or personal delivery is warranted. Similarly, a lawyer should consult with the client as to how to appropriately and safely use technology in their communication, in compliance with other laws that might be applicable to the client. Whether a lawyer is using methods and practices to comply with administrative, statutory, or international legal standards is beyond the scope of this opinion.

A client may insist or require that the lawyer undertake certain forms of communication. As explained in Comment [19] to Model Rule 1.6, “A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.”

V. Conclusion

Rule 1.1 requires a lawyer to provide competent representation to a client. Comment [8] to Rule 1.1 advises lawyers that to maintain the requisite knowledge and skill for competent representation, a lawyer should keep abreast of the benefits and risks associated with relevant technology. Rule 1.6(c) requires a lawyer to make “reasonable efforts” to prevent the inadvertent or unauthorized disclosure of or access to information relating to the representation.

A lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.
An Act

To provide congressional review and to counter aggression by the Governments of Iran, the Russian Federation, and North Korea, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the “Countering America’s Adversaries Through Sanctions Act”.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.

TITLE I—SANCTIONS WITH RESPECT TO IRAN

Sec. 101. Short title.
Sec. 102. Definitions.
Sec. 103. Regional strategy for countering conventional and asymmetric Iranian threats in the Middle East and North Africa.
Sec. 104. Imposition of additional sanctions in response to Iran’s ballistic missile program.
Sec. 105. Imposition of terrorism-related sanctions with respect to the IRGC.
Sec. 106. Imposition of additional sanctions with respect to persons responsible for human rights abuses.
Sec. 107. Enforcement of arms embargos.
Sec. 108. Review of applicability of sanctions relating to Iran’s support for terrorism and its ballistic missile program.
Sec. 110. Report on United States citizens detained by Iran.
Sec. 111. Exceptions for national security and humanitarian assistance; rule of construction.
Sec. 112. Presidential waiver authority.

TITLE II—SANCTIONS WITH RESPECT TO THE RUSSIAN FEDERATION AND COMBATING TERRORISM AND ILLICIT FINANCING

Sec. 201. Short title.
Subtitle A—Sanctions and Other Measures With Respect to the Russian Federation
Sec. 211. Findings.
Sec. 212. Sense of Congress.

PART 1—CONGRESSIONAL REVIEW OF SANCTIONS IMPOSED WITH RESPECT TO THE RUSSIAN FEDERATION

Sec. 215. Short title.
Sec. 216. Congressional review of certain actions relating to sanctions imposed with respect to the Russian Federation.

PART 2—SANCTIONS WITH RESPECT TO THE RUSSIAN FEDERATION

Sec. 221. Definitions.
Sec. 222. Codification of sanctions relating to the Russian Federation.
Sec. 223. Modification of implementation of Executive Order No. 13662.
Sec. 224. Imposition of sanctions with respect to activities of the Russian Federation undermining cybersecurity.
Sec. 225. Imposition of sanctions relating to special Russian crude oil projects.
Sec. 226. Imposition of sanctions with respect to Russian and other foreign financial institutions.
Sec. 227. Mandatory imposition of sanctions with respect to significant corruption in the Russian Federation.
Sec. 228. Mandatory imposition of sanctions with respect to certain transactions with foreign sanctions evaders and serious human rights abusers in the Russian Federation.
Sec. 230. Standards for termination of certain sanctions with respect to the Russian Federation.
Sec. 231. Imposition of sanctions with respect to persons engaging in transactions with the intelligence or defense sectors of the Government of the Russian Federation.
Sec. 232. Sanctions with respect to the development of pipelines in the Russian Federation.
Sec. 233. Sanctions with respect to investment in or facilitation of privatization of state-owned assets by the Russian Federation.
Sec. 234. Sanctions with respect to the transfer of arms and related material to Syria.
Sec. 235. Sanctions described.
Sec. 236. Exceptions, waiver, and termination.
Sec. 237. Exception relating to activities of the National Aeronautics and Space Administration.
Sec. 238. Rule of construction.

PART 3—REPORTS

Sec. 242. Report on effects of expanding sanctions to include sovereign debt and derivative products.

Subtitle B—Countering Russian Influence in Europe and Eurasia

Sec. 251. Findings.
Sec. 252. Sense of Congress.
Sec. 253. Statement of policy.
Sec. 254. Coordinating aid and assistance across Europe and Eurasia.
Sec. 255. Report on media organizations controlled and funded by the Government of the Russian Federation.
Sec. 257. Ukrainian energy security.
Sec. 258. Termination.
Sec. 259. Appropriate congressional committees defined.

Subtitle C—Combating Terrorism and Illicit Financing

PART 1—NATIONAL STRATEGY FOR COMBATING TERRORIST AND OTHER ILLICIT FINANCING

Sec. 261. Development of national strategy.
Sec. 262. Contents of national strategy.

PART 2—ENHANCING ANTI-TELEPHONE TOOLS OF THE DEPARTMENT OF THE TREASURY

Sec. 271. Improving anti-terror finance monitoring of funds transfers.
Sec. 272. Sense of Congress on international cooperation regarding terrorist financing intelligence.
Sec. 273. Examining the counter-terror financing role of the Department of the Treasury in embassies.
Sec. 274. Inclusion of Secretary of the Treasury on the National Security Council.
Sec. 275. Inclusion of all funds.

PART 3—DEFINITIONS

Sec. 281. Definitions.

Subtitle D—Rule of Construction

Sec. 291. Rule of construction.
Sec. 292. Sense of Congress on the strategic importance of Article 5 of the North Atlantic Treaty.
TITLE III—SANCTIONS WITH RESPECT TO NORTH KOREA

Sec. 301. Short title.
Sec. 302. Definitions.
Subtitle A—Sanctions to Enforce and Implement United Nations Security Council Sanctions Against North Korea
Sec. 311. Modification and expansion of requirements for the designation of persons.
Sec. 312. Prohibition on indirect correspondent accounts.
Sec. 313. Limitations on foreign assistance to noncompliant governments.
Sec. 314. Amendments to enhance inspection authorities.
Sec. 315. Enforcing compliance with United Nations shipping sanctions against North Korea.
Sec. 316. Report on cooperation between North Korea and Iran.
Sec. 318. Briefing on measures to deny specialized financial messaging services to designated North Korean financial institutions.
Subtitle B—Sanctions With Respect to Human Rights Abuses by the Government of North Korea
Sec. 321. Sanctions for forced labor and slavery overseas of North Koreans.
Sec. 322. Modifications to sanctions suspension and waiver authorities.
Sec. 323. Reward for informants.
Sec. 324. Determination on designation of North Korea as a state sponsor of terrorism.
Subtitle C—General Authorities
Sec. 331. Authority to consolidate reports.
Sec. 332. Rule of construction.
Sec. 333. Regulatory authority.
Sec. 334. Limitation on funds.

TITLE I—SANCTIONS WITH RESPECT TO IRAN

SEC. 101. SHORT TITLE.
This title may be cited as the “Countering Iran’s Destabilizing Activities Act of 2017”.
SEC. 102. DEFINITIONS.
In this title:
(1) ACT OF INTERNATIONAL TERRORISM.—The term “act of international terrorism” has the meaning given that term in section 14 of the Iran Sanctions Act of 1996 (Public Law 104–172; 50 U.S.C. 1701 note).
(2) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term “appropriate congressional committees” has the meaning given that term in section 14 of the Iran Sanctions Act of 1996 (Public Law 104–172; 50 U.S.C. 1701 note).
(3) FOREIGN PERSON.—The term “foreign person” means a person that is not a United States person.
(4) IRANIAN PERSON.—The term “Iranian person” means—
(A) an individual who is a citizen or national of Iran; or
(B) an entity organized under the laws of Iran or otherwise subject to the jurisdiction of the Government of Iran.
(5) IRGC.—The term “IRGC” means Iran’s Islamic Revolutionary Guard Corps.
H. R. 3364—4

(6) KNOWINGLY.—The term “knowingly” has the meaning given that term in section 14 of the Iran Sanctions Act of 1996 (Public Law 104–172; 50 U.S.C. 1701 note).

(7) UNITED STATES PERSON.—The term “United States person” means—

(A) a United States citizen or an alien lawfully admitted for permanent residence to the United States;

or

(B) an entity organized under the laws of the United States or of any jurisdiction within the United States, including a foreign branch of such an entity.

SEC. 103. REGIONAL STRATEGY FOR COUNTERING CONVENTIONAL AND ASYMMETRIC IRANIAN THREATS IN THE MIDDLE EAST AND NORTH AFRICA.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and every 2 years thereafter, the Secretary of State, the Secretary of Defense, the Secretary of the Treasury, and the Director of National Intelligence shall jointly develop and submit to the appropriate congressional committees and leadership a strategy for deterring conventional and asymmetric Iranian activities and threats that directly threaten the United States and key allies in the Middle East, North Africa, and beyond.

(b) ELEMENTS.—The strategy required by subsection (a) shall include at a minimum the following:

(1) A summary of the near- and long-term United States objectives, plans, and means for countering Iran’s destabilizing activities, including identification of countries that share the objective of countering Iran’s destabilizing activities.

(2) A summary of the capabilities and contributions of individual countries to shared efforts to counter Iran’s destabilizing activities, and a summary of additional actions or contributions that each country could take to further contribute.

(3) An assessment of Iran’s conventional force capabilities and an assessment of Iran’s plans to upgrade its conventional force capabilities, including its acquisition, development, and deployment of ballistic and cruise missile capabilities, unmanned aerial vehicles, and maritime offensive and anti-access or area denial capabilities.

(4) An assessment of Iran’s chemical and biological weapons capabilities and an assessment of Iranian plans to upgrade its chemical or biological weapons capabilities.

(5) An assessment of Iran’s asymmetric activities in the region, including—

(A) the size, capabilities, and activities of the IRGC, including the Quds Force;

(B) the size, capabilities, and activities of Iran’s cyber operations;

(C) the types and amount of support, including funding, lethal and nonlethal contributions, and training, provided to Hezbollah, Hamas, special groups in Iraq, the regime of Bashar al-Assad in Syria, Houthi fighters in Yemen, and other violent groups across the Middle East; and

(D) the scope and objectives of Iran’s information operations and use of propaganda.
H. R. 3364—5

(6) A summary of United States actions, unilaterally and in cooperation with foreign governments, to counter destabilizing Iranian activities, including—

(A) interdiction of Iranian lethal arms bound for groups designated as foreign terrorist organizations under section 219 of the Immigration and Nationality Act (8 U.S.C. 1189);
(B) Iran's interference in international commercial shipping lanes;
(C) attempts by Iran to undermine or subvert internationally recognized governments in the Middle East region; and

(D) Iran's support for the regime of Bashar al-Assad in Syria, including—

(i) financial assistance, military equipment and personnel, and other support provided to that regime; and

(ii) support and direction to other armed actors that are not Syrian or Iranian and are acting on behalf of that regime.

(c) FORM OF STRATEGY.—The strategy required by subsection (a) shall be submitted in unclassified form, but may include a classified annex.

(d) APPROPRIATE CONGRESSIONAL COMMITTEES AND LEADERSHIP DEFINED.—In this section, the term “appropriate congressional committees and leadership” means—

(1) the Committee on Finance, the Committee on Banking, Housing, and Urban Affairs, the Committee on Foreign Relations, and the majority and minority leaders of the Senate; and

(2) the Committee on Ways and Means, the Committee on Financial Services, the Committee on Foreign Affairs, and the Speaker, the majority leader, and the minority leader of the House of Representatives.

SEC. 104. IMPOSITION OF ADDITIONAL SANCTIONS IN RESPONSE TO IRAN'S BALLISTIC MISSILE PROGRAM.

(a) SENSE OF CONGRESS.—It is the sense of Congress that the Secretary of the Treasury and the Secretary of State should continue to implement Executive Order No. 13382 (50 U.S.C. 1701 note; relating to blocking property of weapons of mass destruction delivery system proliferators and their supporters).

(b) IMPOSITION OF SANCTIONS.—The President shall impose the sanctions described in subsection (c) with respect to any person that the President determines, on or after the date of the enactment of this Act—

(1) knowingly engages in any activity that materially contributes to the activities of the Government of Iran with respect to its ballistic missile program, or any other program in Iran for developing, deploying, or maintaining systems capable of delivering weapons of mass destruction, including any efforts to manufacture, acquire, possess, develop, transport, transfer, or use such capabilities;

(2) is a successor entity to a person referred to in paragraph (1);

(3) owns or controls or is owned or controlled by a person referred to in paragraph (1);
(4) forms an entity with the purpose of evading sanctions that would otherwise be imposed pursuant to paragraph (3);
(5) is acting for or on behalf of a person referred to in paragraph (1), (2), (3), or (4); or
(6) knowingly provides or attempts to provide financial, material, technological, or other support for, or goods or services in support of, a person referred to in paragraph (1), (2), (3), (4) or (5).

(c) SANCTIONS DESCRIBED.—The sanctions described in this subsection are the following:

(1) BLOCKING OF PROPERTY.—The President shall block, in accordance with the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.), all transactions in all property and interests in property of any person subject to subsection (b) if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

(2) EXCLUSION FROM UNITED STATES.—The Secretary of State shall deny a visa to, and the Secretary of Homeland Security shall exclude from the United States, any person subject to subsection (b) that is an alien.

(d) PENALTIES.—A person that violates, attempts to violate, conspires to violate, or causes a violation of subsection (c)(1) or any regulation, license, or order issued to carry out that subsection shall be subject to the penalties set forth in subsections (b) and (c) of section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705) to the same extent as a person that commits an unlawful act described in subsection (a) of that section.

(e) REPORT ON CONTRIBUTIONS TO IRAN'S BALLISTIC MISSILE PROGRAM.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and every 180 days thereafter, the President shall submit to the appropriate congressional committees a report describing each person that—

(A) has, during the period specified in paragraph (2), conducted any activity that has materially contributed to the activities of the Government of Iran with respect to its ballistic missile program, or any other program in Iran for developing, deploying, or maintaining systems capable of delivering weapons of mass destruction, including any efforts to manufacture, acquire, possess, develop, transport, transfer, or use such capabilities;

(B) is a successor entity to a person referred to in subparagraph (A);

(C) owns or controls or is owned or controlled by a person referred to in subparagraph (A);

(D) forms an entity with the purpose of evading sanctions that could be imposed as a result of a relationship described in subparagraph (C);

(E) is acting for or on behalf of a person referred to in subparagraph (A), (B), (C), or (D); or

(F) is known or believed to have provided, or attempted to provide, during the period specified in paragraph (2), financial, material, technological, or other support for, or goods or services in support of, any material contribution to a program described in subparagraph (A) carried out
by a person described in subparagraph (A), (B), (C), (D), or (E).

(2) PERIOD SPECIFIED.—The period specified in this paragraph is—
(A) in the case of the first report submitted under paragraph (1), the period beginning January 1, 2016, and ending on the date the report is submitted; and
(B) in the case of a subsequent such report, the 180-day period preceding the submission of the report.

(3) FORM OF REPORT.—Each report required by paragraph (1) shall be submitted in unclassified form but may include a classified annex.

SEC. 105. IMPOSITION OF TERRORISM-RELATED SANCTIONS WITH RESPECT TO THE IRGC.

(a) FINDINGS.—Congress makes the following findings:

(1) The IRGC is subject to sanctions pursuant to Executive Order No. 13382 (50 U.S.C. 1701 note; relating to blocking property of weapons of mass destruction delivery system proliferators and their supporters), the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (22 U.S.C. 8501 et seq.), Executive Order No. 13553 (50 U.S.C. 1701 note; relating to blocking property of certain persons with respect to serious human rights abuses by the Government of Iran), and Executive Order No. 13666 (50 U.S.C. 1701 note; relating to blocking the property and suspending entry into the United States of certain persons with respect to grave human rights abuses by the Governments of Iran and Syria via information technology).

(2) The Iranian Revolutionary Guard Corps–Quds Force (in this section referred to as the "IRGC–QF") is the primary arm of the Government of Iran for executing its policy of supporting terrorist and insurgent groups. The IRGC–QF provides material, logistical assistance, training, and financial support to militants and terrorist operatives throughout the Middle East and South Asia and was designated for the imposition of sanctions by the Secretary of the Treasury pursuant to Executive Order No. 13224 (50 U.S.C. 1701 note; relating to blocking property and prohibiting transactions with persons who commit, threaten to commit, or support terrorism) in October 2007 for its support of terrorism.

(3) The IRGC, not just the IRGC–QF, is responsible for implementing Iran’s international program of destabilizing activities, support for acts of international terrorism, and ballistic missile program.

(b) IN GENERAL.—Beginning on the date that is 90 days after the date of the enactment of this Act, the President shall impose the sanctions described in subsection (c) with respect to the IRGC and foreign persons that are officials, agents, or affiliates of the IRGC.

(c) SANCTIONS DESCRIBED.—The sanctions described in this subsection are sanctions applicable with respect to a foreign person pursuant to Executive Order No. 13224 (50 U.S.C. 1701 note; relating to blocking property and prohibiting transactions with persons who commit, threaten to commit, or support terrorism).
SEC. 106. IMPOSITION OF ADDITIONAL SANCTIONS WITH RESPECT TO PERSONS RESPONSIBLE FOR HUMAN RIGHTS ABUSES.

(a) In General.—Not later than 90 days after the date of the enactment of this Act, and annually thereafter, the Secretary of State shall submit to the appropriate congressional committees a list of each person the Secretary determines, based on credible evidence, on or after the date of the enactment of this Act—

(1) is responsible for extrajudicial killings, torture, or other gross violations of internationally recognized human rights committed against individuals in Iran who seek—

(A) to expose illegal activity carried out by officials of the Government of Iran; or

(B) to obtain, exercise, defend, or promote internationally recognized human rights and freedoms, such as the freedoms of religion, expression, association, and assembly, and the rights to a fair trial and democratic elections; or

(2) acts as an agent of or on behalf of a foreign person in a matter relating to an activity described in paragraph (1).

(b) Sanctions Described.—

(1) In General.—The President may, in accordance with the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.), block all transactions in all property and interests in property of a person on the list required by subsection (a) if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

(2) Penalties.—A person that violates, attempts to violate, conspires to violate, or causes a violation of paragraph (1) or any regulation, license, or order issued to carry out paragraph (1) shall be subject to the penalties set forth in subsections (b) and (c) of section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705) to the same extent as a person that commits an unlawful act described in subsection (a) of that section.

SEC. 107. ENFORCEMENT OF ARMS EMBARGOS.

(a) In General.—Except as provided in subsection (d), the President shall impose the sanctions described in subsection (b) with respect to any person that the President determines—

(1) knowingly engages in any activity that materially contributes to the supply, sale, or transfer directly or indirectly to or from Iran, or for the use in or benefit of Iran, of any battle tanks, armored combat vehicles, large caliber artillery systems, combat aircraft, attack helicopters, warships, missiles or missile systems, as defined for the purpose of the United Nations Register of Conventional Arms, or related materiel, including spare parts; or

(2) knowingly provides to Iran any technical training, financial resources or services, advice, other services or assistance related to the supply, sale, transfer, manufacture, maintenance, or use of arms and related materiel described in paragraph (1).

(b) Sanctions Described.—

(1) Blocking of Property.—The President shall block, in accordance with the International Emergency Economic
Powers Act (50 U.S.C. 1701 et seq.), all transactions in all property and interests in property of any person subject to subsection (a) if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

(2) Exclusion from United States.—The Secretary of State shall deny a visa to, and the Secretary of Homeland Security shall exclude from the United States, any person subject to subsection (a) that is an alien.

(c) Penalties.—A person that violates, attempts to violate, conspires to violate, or causes a violation of subsection (b)(1) or any regulation, license, or order issued to carry out that subsection shall be subject to the penalties set forth in subsections (b) and (c) of section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705) to the same extent as a person that commits an unlawful act described in subsection (a) of that section.

(d) Exception.—The President is not required to impose sanctions under subsection (a) with respect to a person for engaging in an activity described in that subsection if the President certifies to the appropriate congressional committees that—

(1) permitting the activity is in the national security interest of the United States;
(2) Iran no longer presents a significant threat to the national security of the United States and to the allies of the United States; and
(3) the Government of Iran has ceased providing operational or financial support for acts of international terrorism and no longer satisfies the requirements for designation as a state sponsor of terrorism.

(e) State Sponsor of Terrorism Defined.—In this section, the term “state sponsor of terrorism” means a country the government of which the Secretary of State has determined to be a government that has repeatedly provided support for acts of international terrorism for purposes of—

(2) section 620A(a) of the Foreign Assistance Act of 1961 (22 U.S.C. 2371(a));
(3) section 40(d) of the Arms Export Control Act (22 U.S.C. 2780(d)); or
(4) any other provision of law.

SEC. 108. REVIEW OF APPLICABILITY OF SANCTIONS RELATING TO IRAN’S SUPPORT FOR TERRORISM AND ITS BALLISTIC MISSILE PROGRAM.

(a) In General.—Not later than 5 years after the date of the enactment of this Act, the President shall conduct a review of all persons on the list of specially designated nationals and blocked persons maintained by the Office of Foreign Assets Control of the Department of the Treasury for activities relating to Iran—

(1) to assess the conduct of such persons as that conduct relates to—
(A) any activity that materially contributes to the activities of the Government of Iran with respect to its ballistic missile program; or
(B) support by the Government of Iran for acts of international terrorism; and
(2) to determine the applicability of sanctions with respect to such persons under—
(A) Executive Order No. 13382 (50 U.S.C. 1701 note; relating to blocking property of weapons of mass destruction delivery system proliferators and their supporters); or
(B) Executive Order No. 13224 (50 U.S.C. 1701 note; relating to blocking property and prohibiting transactions with persons who commit, threaten to commit, or support terrorism).

(b) IMPLEMENTATION OF SANCTIONS.—If the President determines under subsection (a) that sanctions under an Executive order specified in paragraph (2) of that subsection are applicable with respect to a person, the President shall—
(1) impose sanctions with respect to that person pursuant to that Executive order; or
(2) exercise the waiver authority provided under section 112.

SEC. 109. REPORT ON COORDINATION OF SANCTIONS BETWEEN THE UNITED STATES AND THE EUROPEAN UNION.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and every 180 days thereafter, the President shall submit to the appropriate congressional committees a report that includes the following:
(1) A description of each instance, during the period specified in subsection (b)—
(A) in which the United States has imposed sanctions with respect to a person for activity related to the proliferation of weapons of mass destruction or delivery systems for such weapons to or by Iran, support for acts of international terrorism by Iran, or human rights abuses in Iran, but in which the European Union has not imposed corresponding sanctions; and
(B) in which the European Union has imposed sanctions with respect to a person for activity related to the proliferation of weapons of mass destruction or delivery systems for such weapons to or by Iran, support for acts of international terrorism by Iran, or human rights abuses in Iran, but in which the United States has not imposed corresponding sanctions.
(2) An explanation for the reason for each discrepancy between sanctions imposed by the European Union and sanctions imposed by the United States described in subparagraphs (A) and (B) of paragraph (1).

(b) PERIOD SPECIFIED.—The period specified in this subsection is—
(1) in the case of the first report submitted under subsection (a), the period beginning on the date of the enactment of this Act and ending on the date the report is submitted; and
(2) in the case of a subsequent such report, the 180-day period preceding the submission of the report.
H. R. 3364—11

(c) FORM OF REPORT.—The report required by subsection (a) shall be submitted in unclassified form but may include a classified annex.

SEC. 110. REPORT ON UNITED STATES CITIZENS DETAINED BY IRAN.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, and every 180 days thereafter, the President shall submit to the appropriate congressional committees and leadership a report on United States citizens, including United States citizens who are also citizens of other countries, detained by Iran or groups supported by Iran that includes—

(1) information regarding any officials of the Government of Iran involved in any way in the detentions; and

(2) a summary of efforts the United States Government has taken to secure the swift release of those United States citizens.

(b) FORM OF REPORT.—The report required by subsection (a) shall be submitted in unclassified form, but may include a classified annex.

(c) APPROPRIATE CONGRESSIONAL COMMITTEES AND LEADERSHIP DEFINED.—In this section, the term “appropriate congressional committees and leadership” means—

(1) the Committee on Finance, the Committee on Banking, Housing, and Urban Affairs, the Committee on Foreign Relations, and the majority and minority leaders of the Senate; and

(2) the Committee on Ways and Means, the Committee on Financial Services, the Committee on Foreign Affairs, and the Speaker, the majority leader, and the minority leader of the House of Representatives.

SEC. 111. EXCEPTIONS FOR NATIONAL SECURITY AND HUMANITARIAN ASSISTANCE; RULE OF CONSTRUCTION.

(a) IN GENERAL.—The following activities shall be exempt from sanctions under sections 104, 105, 106, and 107:

(1) Any activity subject to the reporting requirements under title V of the National Security Act of 1947 (50 U.S.C. 3091 et seq.), or to any authorized intelligence activities of the United States.

(2) The admission of an alien to the United States if such admission is necessary to comply with United States obligations under the Agreement between the United Nations and the United States of America regarding the Headquarters of the United Nations, signed at Lake Success June 26, 1947, and entered into force November 21, 1947, or under the Convention on Consular Relations, done at Vienna April 24, 1963, and entered into force March 19, 1967, or other applicable international obligations of the United States.

(3) The conduct or facilitation of a transaction for the sale of agricultural commodities, food, medicine, or medical devices to Iran or for the provision of humanitarian assistance to the people of Iran, including engaging in a financial transaction relating to humanitarian assistance or for humanitarian purposes or transporting goods or services that are necessary to carry out operations relating to humanitarian assistance or humanitarian purposes.
(b) IMPLEMENTATION.—The President may exercise all authorities provided under sections 203 and 205 of the International Emergency Economic Powers Act (50 U.S.C. 1702 and 1704) to carry out this Act.

(c) RULE OF CONSTRUCTION.—Nothing in this Act shall be construed to limit the authority of the President under the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.).

(d) DEFINITIONS.—In this section:

(1) AGRICULTURAL COMMODITY.—The term “agricultural commodity” has the meaning given that term in section 102 of the Agricultural Trade Act of 1978 (7 U.S.C. 5602).

(2) GOOD.—The term “good” has the meaning given that term in section 16 of the Export Administration Act of 1979 (50 U.S.C. 4618) (as continued in effect pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.).

(3) MEDICAL DEVICE.—The term “medical device” has the meaning given the term “device” in section 201 of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 321).

(4) MEDICINE.—The term “medicine” has the meaning given the term “drug” in section 201 of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 321).

SEC. 112. PRESIDENTIAL WAIVER AUTHORITY.

(a) CASE-BY-CASE WAIVER AUTHORITY.—

(1) IN GENERAL.—The President may waive, on a case-by-case basis and for a period of not more than 180 days, a requirement under section 104, 105, 106, 107, or 108 to impose or maintain sanctions with respect to a person, and may waive the continued imposition of such sanctions, not less than 30 days after the President determines and reports to the appropriate congressional committees that it is vital to the national security interests of the United States to waive such sanctions.

(2) RENEWAL OF WAIVERS.—The President may, on a case-by-case basis, renew a waiver under paragraph (1) for an additional period of not more than 180 days if, not later than 15 days before that waiver expires, the President makes the determination and submits to the appropriate congressional committees a report described in paragraph (1).

(3) SUCCESSIVE RENEWAL.—The renewal authority provided under paragraph (2) may be exercised for additional successive periods of not more than 180 days if the President follows the procedures set forth in paragraph (2), and submits the report described in paragraph (1), for each such renewal.

(b) CONTENTS OF WAIVER REPORTS.—Each report submitted under subsection (a) in connection with a waiver of sanctions under section 104, 105, 106, 107, or 108 with respect to a person, or the renewal of such a waiver, shall include—

(1) a specific and detailed rationale for the determination that the waiver is vital to the national security interests of the United States;

(2) a description of the activity that resulted in the person being subject to sanctions;

(3) an explanation of any efforts made by the United States, as applicable, to secure the cooperation of the government with primary jurisdiction over the person or the location where
the activity described in paragraph (2) occurred in terminating or, as appropriate, penalizing the activity; and

(4) an assessment of the significance of the activity described in paragraph (2) in contributing to the ability of Iran to threaten the interests of the United States or allies of the United States, develop systems capable of delivering weapons of mass destruction, support acts of international terrorism, or violate the human rights of any person in Iran.

(c) EFFECT OF REPORT ON WAIVER.—If the President submits a report under subsection (a) in connection with a waiver of sanctions under section 104, 105, 106, 107, or 108 with respect to a person, or the renewal of such a waiver, the President shall not be required to impose or maintain sanctions under section 104, 105, 106, 107, or 108, as applicable, with respect to the person described in the report during the 30-day period referred to in subsection (a).

TITLE II—SANCTIONS WITH RESPECT TO THE RUSSIAN FEDERATION AND COMBATING TERRORISM AND ILICIT FINANCING

SEC. 201. SHORT TITLE.

This title may be cited as the “Countering Russian Influence in Europe and Eurasia Act of 2017”.

Subtitle A—Sanctions and Other Measures With Respect to the Russian Federation

SEC. 211. FINDINGS.

Congress makes the following findings:

(1) On March 6, 2014, President Barack Obama issued Executive Order No. 13660 (79 Fed. Reg. 13493; relating to blocking property of certain persons contributing to the situation in Ukraine), which authorizes the Secretary of the Treasury, in consultation with the Secretary of State, to impose sanctions on those determined to be undermining democratic processes and institutions in Ukraine or threatening the peace, security, stability, sovereignty, and territorial integrity of Ukraine. President Obama subsequently issued Executive Order No. 13661 (79 Fed. Reg. 15535; relating to blocking property of additional persons contributing to the situation in Ukraine) and Executive Order No. 13662 (79 Fed. Reg. 16169; relating to blocking property of additional persons contributing to the situation in Ukraine) to expand sanctions on certain persons contributing to the situation in Ukraine.

(2) On December 18, 2014, the Ukraine Freedom Support Act of 2014 was enacted (Public Law 113–272; 22 U.S.C. 8921 et seq.), which includes provisions directing the President to impose sanctions on foreign persons that the President determines to be entities owned or controlled by the Government.
of the Russian Federation or nationals of the Russian Federation that manufacture, sell, transfer, or otherwise provide certain defense articles into Syria.

(3) On April 1, 2015, President Obama issued Executive Order No. 13694 (80 Fed. Reg. 18077; relating to blocking the property of certain persons engaging in significant malicious cyber-enabled activities), which authorizes the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to impose sanctions on persons determined to be engaged in malicious cyber-hacking.

(4) On July 26, 2016, President Obama approved a Presidential Policy Directive on United States Cyber Incident Coordination, which states, “certain cyber incidents that have significant impacts on an entity, our national security, or the broader economy require a unique approach to response efforts”.

(5) On December 29, 2016, President Obama issued an annex to Executive Order No. 13694, which authorized sanctions on the following entities and individuals:

(A) The Main Intelligence Directorate (also known as Glavnoe Razvedyvatel’noe Upravlenie or the GRU) in Moscow, Russian Federation.
(B) The Federal Security Service (also known as Federal’naya Sluzhba Bezopasnosti or the FSB) in Moscow, Russian Federation.
(C) The Special Technology Center (also known as STLC, Ltd. Special Technology Center St. Petersburg) in St. Petersburg, Russian Federation.
(D) Zorsecurity (also known as Esage Lab) in Moscow, Russian Federation.
(E) The autonomous noncommercial organization known as the Professional Association of Designers of Data Processing Systems (also known as ANO PO KSI) in Moscow, Russian Federation.
(F) Igor Valentinovich Korobov.
(G) Sergey Aleksandrovich Gizunov.
(H) Igor Olegovich Kostyukov.
(I) Vladimir Stepanovich Alexseyev.

(6) On January 6, 2017, an assessment of the United States intelligence community entitled, “Assessing Russian Activities and Intentions in Recent U.S. Elections” stated, “Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the United States presidential election.” The assessment warns that “Moscow will apply lessons learned from its Putin-ordered campaign aimed at the U.S. Presidential election to future influence efforts worldwide, including against U.S. allies and their election processes”.

SEC. 212. SENSE OF CONGRESS.

It is the sense of Congress that the President—

(1) should continue to uphold and seek unity with European and other key partners on sanctions implemented against the Russian Federation, which have been effective and instrumental in countering Russian aggression in Ukraine;

(2) should engage to the fullest extent possible with partner governments with regard to closing loopholes, including the allowance of extended prepayment for the delivery of goods
and commodities and other loopholes, in multilateral and uni-
lateral restrictive measures against the Russian Federation, 
with the aim of maximizing alignment of those measures; and

(3) should increase efforts to vigorously enforce compliance 
with sanctions in place as of the date of the enactment of 
this Act with respect to the Russian Federation in response 
to the crisis in eastern Ukraine, cyber intrusions and attacks, 
and human rights violators in the Russian Federation.

PART 1—CONGRESSIONAL REVIEW OF SANC-
TIONS IMPOSED WITH RESPECT TO THE 
RUSSIAN FEDERATION

SEC. 215. SHORT TITLE.

This part may be cited as the “Russia Sanctions Review Act 
of 2017”.

SEC. 216. CONGRESSIONAL REVIEW OF CERTAIN ACTIONS RELATING 
TO SANCTIONS IMPOSED WITH RESPECT TO THE RUSSIAN 
FEDERATION.

(a) SUBMISSION TO CONGRESS OF PROPOSED ACTION.—

(1) IN GENERAL.—Notwithstanding any other provision of 
law, before taking any action described in paragraph (2), the 
President shall submit to the appropriate congressional commit-
tees and leadership a report that describes the proposed action 
and the reasons for that action.

(2) ACTIONS DESCRIBED.—

(A) IN GENERAL.—An action described in this para-
graph is—

(i) an action to terminate the application of any 
sanctions described in subparagraph (B); 
(ii) with respect to sanctions described in subpara-
graph (B) imposed by the President with respect to 
a person, an action to waive the application of those 
sanctions with respect to that person; or 
(iii) a licensing action that significantly alters 
United States’ foreign policy with regard to the Russian 
Federation.

(B) SANCTIONS DESCRIBED.—The sanctions described 
in this subparagraph are—

(i) sanctions provided for under—

(I) this title or any provision of law amended 
by this title, including the Executive orders codi-
fied under section 222; 
(II) the Support for the Sovereignty, Integrity, 
Democracy, and Economic Stability of Ukraine Act 
of 2014 (22 U.S.C. 8901 et seq.); or 
(III) the Ukraine Freedom Support Act of 2014 
(22 U.S.C. 8921 et seq.); and 

(ii) the prohibition on access to the properties of 
the Government of the Russian Federation located in 
Maryland and New York that the President ordered 
vacated on December 29, 2016.

(3) DESCRIPTION OF TYPE OF ACTION.—Each report sub-
mitted under paragraph (1) with respect to an action described
paragraph (2) shall include a description of whether the action—
(A) is not intended to significantly alter United States foreign policy with regard to the Russian Federation; or
(B) is intended to significantly alter United States foreign policy with regard to the Russian Federation.

(4) INCLUSION OF ADDITIONAL MATTER.—
(A) IN GENERAL.—Each report submitted under paragraph (1) that relates to an action that is intended to significantly alter United States foreign policy with regard to the Russian Federation shall include a description of—
(i) the significant alteration to United States foreign policy with regard to the Russian Federation;
(ii) the anticipated effect of the action on the national security interests of the United States; and
(iii) the policy objectives for which the sanctions affected by the action were initially imposed.
(B) REQUESTS FROM BANKING AND FINANCIAL SERVICES COMMITTEES.—The Committee on Banking, Housing, and Urban Affairs of the Senate or the Committee on Financial Services of the House of Representatives may request the submission to the Committee of the matter described in clauses (ii) and (iii) of subparagraph (A) with respect to a report submitted under paragraph (1) that relates to an action that is not intended to significantly alter United States foreign policy with regard to the Russian Federation.

(5) CONFIDENTIALITY OF PROPRIETARY INFORMATION.—Proprietary information that can be associated with a particular person with respect to an action described in paragraph (2) may be included in a report submitted under paragraph (1) only if the appropriate congressional committees and leadership provide assurances of confidentiality, unless such person otherwise consents in writing to such disclosure.

(6) RULE OF CONSTRUCTION.—Paragraph (2)(A)(iii) shall not be construed to require the submission of a report under paragraph (1) with respect to the routine issuance of a license that does not significantly alter United States foreign policy with regard to the Russian Federation.

(b) PERIOD FOR REVIEW BY CONGRESS.—
(1) IN GENERAL.—During the period of 30 calendar days beginning on the date on which the President submits a report under subsection (a)(1)—
(A) in the case of a report that relates to an action that is not intended to significantly alter United States foreign policy with regard to the Russian Federation, the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Financial Services of the House of Representatives should, as appropriate, hold hearings and briefings and otherwise obtain information in order to fully review the report; and
(B) in the case of a report that relates to an action that is intended to significantly alter United States foreign policy with regard to the Russian Federation, the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives should, as appropriate, hold hearings and briefings and
otherwise obtain information in order to fully review the report.

(2) EXCEPTION.—The period for congressional review under paragraph (1) of a report required to be submitted under subsection (a)(1) shall be 60 calendar days if the report is submitted on or after July 10 and on or before September 7 in any calendar year.

(3) LIMITATION ON ACTIONS DURING INITIAL CONGRESSIONAL REVIEW PERIOD.—Notwithstanding any other provision of law, during the period for congressional review provided for under paragraph (1) of a report submitted under subsection (a)(1) proposing an action described in subsection (a)(2), including any additional period for such review as applicable under the exception provided in paragraph (2), the President may not take that action unless a joint resolution of approval with respect to that action is enacted in accordance with subsection (c).

(4) LIMITATION ON ACTIONS DURING PRESIDENTIAL CONSIDERATION OF A JOINT RESOLUTION OF DISAPPROVAL.—Notwithstanding any other provision of law, if a joint resolution of disapproval relating to a report submitted under subsection (a)(1) proposing an action described in subsection (a)(2) passes both Houses of Congress in accordance with subsection (c), the President may not take that action for a period of 12 calendar days after the date of passage of the joint resolution of disapproval.

(5) LIMITATION ON ACTIONS DURING CONGRESSIONAL RECONSIDERATION OF A JOINT RESOLUTION OF DISAPPROVAL.—Notwithstanding any other provision of law, if a joint resolution of disapproval relating to a report submitted under subsection (a)(1) proposing an action described in subsection (a)(2) passes both Houses of Congress in accordance with subsection (c), and the President vetoes the joint resolution, the President may not take that action for a period of 10 calendar days after the date of the President's veto.

(6) EFFECT OF ENACTMENT OF A JOINT RESOLUTION OF DISAPPROVAL.—Notwithstanding any other provision of law, if a joint resolution of disapproval relating to a report submitted under subsection (a)(1) proposing an action described in subsection (a)(2) is enacted in accordance with subsection (c), the President may not take that action.

(c) JOINT RESOLUTIONS OF DISAPPROVAL OR APPROVAL DEFINED.—In this subsection:

(1) JOINT RESOLUTION OF APPROVAL.—The term “joint resolution of approval” means only a joint resolution of either House of Congress—

(A) the title of which is as follows: “A joint resolution approving the President’s proposal to take an action relating to the application of certain sanctions with respect to the Russian Federation.”; and

(B) the sole matter after the resolving clause of which is the following: “Congress approves of the action relating to the application of sanctions imposed with respect to the Russian Federation proposed by the President in the report submitted to Congress under section 218(a)(1) of the Russia Sanctions Review Act of 2017 on ________,”, with the first blank space
being filled with the appropriate date and the second blank space being filled with a short description of the proposed action.

(2) JOINT RESOLUTION OF DISAPPROVAL.—The term “joint resolution of disapproval” means only a joint resolution of either House of Congress—

(A) the title of which is as follows: “A joint resolution disapproving the President’s proposal to take an action relating to the application of certain sanctions with respect to the Russian Federation.”; and

(B) the sole matter after the resolving clause of which is the following: “Congress disapproves of the action relating to the application of sanctions imposed with respect to the Russian Federation proposed by the President in the report submitted to Congress under section 216(a)(1) of the Russia Sanctions Review Act of 2017 on relating to “, with the first blank space being filled with the appropriate date and the second blank space being filled with a short description of the proposed action.

(3) INTRODUCTION.—During the period of 30 calendar days provided for under subsection (b)(1), including any additional period as applicable under the exception provided in subsection (b)(2), a joint resolution of approval or joint resolution of disapproval may be introduced—

(A) in the House of Representatives, by the majority leader or the minority leader; and

(B) in the Senate, by the majority leader (or the majority leader’s designee) or the minority leader (or the minority leader’s designee).

(4) FLOOR CONSIDERATION IN HOUSE OF REPRESENTATIVES.—If a committee of the House of Representatives to which a joint resolution of approval or joint resolution of disapproval has been referred has not reported the joint resolution within 10 calendar days after the date of referral, that committee shall be discharged from further consideration of the joint resolution.

(5) CONSIDERATION IN THE SENATE.—A joint resolution of approval or joint resolution of disapproval introduced in the Senate shall be—

(A) COMMITTEE REFERRAL.—A joint resolution of approval or joint resolution of disapproval introduced in the Senate shall be—

(i) referred to the Committee on Banking, Housing, and Urban Affairs if the joint resolution relates to a report under subsection (a)(3)(A) that relates to an action that is not intended to significantly alter United States foreign policy with regard to the Russian Federation; and

(ii) referred to the Committee on Foreign Relations if the joint resolution relates to a report under subsection (a)(3)(B) that relates to an action that is intended to significantly alter United States foreign policy with respect to the Russian Federation.

(B) REPORTING AND DISCHARGE.—If the committee to which a joint resolution of approval or joint resolution of disapproval was referred has not reported the joint resolution within 10 calendar days after the date of referral of the joint resolution, that committee shall be discharged
from further consideration of the joint resolution and the joint resolution shall be placed on the appropriate calendar.

(C) PROCEEDING TO CONSIDERATION.—Notwithstanding Rule XXII of the Standing Rules of the Senate, it is in order at any time after the Committee on Banking, Housing, and Urban Affairs or the Committee on Foreign Relations, as the case may be, reports a joint resolution of approval or joint resolution of disapproval to the Senate or has been discharged from consideration of such a joint resolution (even though a previous motion to the same effect has been disagreed to) to move to proceed to the consideration of the joint resolution, and all points of order against the joint resolution (and against consideration of the joint resolution) are waived. The motion to proceed is not debatable. The motion is not subject to a motion to postpone. A motion to reconsider the vote by which the motion is agreed to or disagreed to shall not be in order.

(D) RULINGS OF THE CHAIR ON PROCEDURE.—Appeals from the decisions of the Chair relating to the application of the rules of the Senate, as the case may be, to the procedure relating to a joint resolution of approval or joint resolution of disapproval shall be decided without debate.

(E) CONSIDERATION OF VETO MESSAGES.—Debate in the Senate of any veto message with respect to a joint resolution of approval or joint resolution of disapproval, including all debatable motions and appeals in connection with the joint resolution, shall be limited to 10 hours, to be equally divided between, and controlled by, the majority leader and the minority leader or their designees.

(6) RULES RELATING TO SENATE AND HOUSE OF REPRESENTATIVES.—

(A) TREATMENT OF SENATE JOINT RESOLUTION IN HOUSE.—In the House of Representatives, the following procedures shall apply to a joint resolution of approval or a joint resolution of disapproval received from the Senate (unless the House has already passed a joint resolution relating to the same proposed action):

(i) The joint resolution shall be referred to the appropriate committees.

(ii) If a committee to which a joint resolution has been referred has not reported the joint resolution within 2 calendar days after the date of referral, that committee shall be discharged from further consideration of the joint resolution.

(iii) Beginning on the third legislative day after each committee to which a joint resolution has been referred reports the joint resolution to the House or has been discharged from further consideration thereof, it shall be in order to move to proceed to consider the joint resolution in the House. All points of order against the motion are waived. Such a motion shall not be in order after the House has disposed of a motion to proceed on the joint resolution. The previous question shall be considered as ordered on the motion to its adoption without intervening motion. The motion shall not be debatable. A motion to reconsider the
vote by which the motion is disposed of shall not be in order.

(iv) The joint resolution shall be considered as read. All points of order against the joint resolution and against its consideration are waived. The previous question shall be considered as ordered on the joint resolution to final passage without intervening motion except 2 hours of debate equally divided and controlled by the sponsor of the joint resolution (or a designee) and an opponent. A motion to reconsider the vote on passage of the joint resolution shall not be in order.

(B) Treatment of House Joint Resolution in Senate—

(i) If, before the passage by the Senate of a joint resolution of approval or joint resolution of disapproval, the Senate receives an identical joint resolution from the House of Representatives, the following procedures shall apply:

(I) That joint resolution shall not be referred to a committee.

(II) With respect to that joint resolution—

(aa) the procedure in the Senate shall be the same as if no joint resolution had been received from the House of Representatives; but

(bb) the vote on passage shall be on the joint resolution from the House of Representatives.

(ii) If, following passage of a joint resolution of approval or joint resolution of disapproval in the Senate, the Senate receives an identical joint resolution from the House of Representatives, that joint resolution shall be placed on the appropriate Senate calendar.

(iii) If a joint resolution of approval or a joint resolution of disapproval is received from the House, and no companion joint resolution has been introduced in the Senate, the Senate procedures under this subsection shall apply to the House joint resolution.

(C) Application to Revenue Measures—The provisions of this paragraph shall not apply in the House of Representatives to a joint resolution of approval or joint resolution of disapproval that is a revenue measure.

(7) Rules of House of Representatives and Senate—

This subsection is enacted by Congress—

(A) as an exercise of the rulemaking power of the Senate and the House of Representatives, respectively, and as such is deemed a part of the rules of each House, respectively, and supersedes other rules only to the extent that it is inconsistent with such rules; and

(B) with full recognition of the constitutional right of either House to change the rules (so far as relating to the procedure of that House) at any time, in the same manner, and to the same extent as in the case of any other rule of that House.

(d) Appropriate Congressional Committees and Leadership Defined.—In this section, the term “appropriate congressional committees and leadership” means—
(1) the Committee on Banking, Housing, and Urban Affairs, the Committee on Foreign Relations, and the majority and minority leaders of the Senate; and
(2) the Committee on Financial Services, the Committee on Foreign Affairs, and the Speaker, the majority leader, and the minority leader of the House of Representatives.

PART 2—SANCTIONS WITH RESPECT TO THE RUSSIAN FEDERATION

SEC. 221. DEFINITIONS.
In this part:
(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" means—
(A) the Committee on Banking, Housing, and Urban Affairs, the Committee on Foreign Relations, and the Committee on Finance of the Senate; and
(B) the Committee on Foreign Affairs, the Committee on Financial Services, and the Committee on Ways and Means of the House of Representatives.
(2) GOOD.—The term "good" has the meaning given that term in section 16 of the Export Administration Act of 1979 (50 U.S.C. 4618) (as continued in effect pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.).
(3) INTERNATIONAL FINANCIAL INSTITUTION.—The term "international financial institution" has the meaning given that term in section 1701(c) of the International Financial Institutions Act (22 U.S.C. 262r(c)).
(4) KNOWINGLY.—The term "knowingly", with respect to conduct, a circumstance, or a result, means that a person has actual knowledge, or should have known, of the conduct, the circumstance, or the result.
(5) PERSON.—The term "person" means an individual or entity.
(6) UNITED STATES PERSON.—The term "United States person" means—
(A) a United States citizen or an alien lawfully admitted for permanent residence to the United States; or
(B) an entity organized under the laws of the United States or of any jurisdiction within the United States, including a foreign branch of such an entity.

SEC. 222. CODIFICATION OF SANCTIONS RELATING TO THE RUSSIAN FEDERATION.
(a) CODIFICATION.—United States sanctions provided for in Executive Order No. 13660 (79 Fed. Reg. 13493; relating to blocking property of certain persons contributing to the situation in Ukraine), Executive Order No. 13661 (79 Fed. Reg. 15535; relating to blocking property of additional persons contributing to the situation in Ukraine), Executive Order No. 13662 (79 Fed. Reg. 16169; relating to blocking property of additional persons contributing to the situation in Ukraine), Executive Order No. 13685 (79 Fed. Reg. 77357; relating to blocking property of certain persons and prohibiting certain transactions with respect to the Crimea region of Ukraine), Executive Order No. 13694 (80 Fed. Reg. 18077; relating to blocking
the property of certain persons engaging in significant malicious cyber-enabled activities), and Executive Order No. 13757 (82 Fed. Reg. 1; relating to taking additional steps to address the national emergency with respect to significant malicious cyber-enabled activities), as in effect on the day before the date of the enactment of this Act, including with respect to all persons sanctioned under such Executive orders, shall remain in effect except as provided in subsection (b).

(b) TERMINATION OF CERTAIN SANCTIONS.—Subject to section 216, the President may terminate the application of sanctions described in subsection (a) that are imposed on a person in connection with activity conducted by the person if the President submits to the appropriate congressional committees a notice that—

(1) the person is not engaging in the activity that was the basis for the sanctions or has taken significant verifiable steps toward stopping the activity; and
(2) the President has received reliable assurances that the person will not knowingly engage in activity subject to sanctions described in subsection (a) in the future.

(c) APPLICATION OF NEW CYBER SANCTIONS.—The President may waive the initial application under subsection (a) of sanctions with respect to a person under Executive Order No. 13694 or 13757 only if the President submits to the appropriate congressional committees—

(1) a written determination that the waiver—
(A) is in the vital national security interests of the United States; or
(B) will further the enforcement of this title; and
(2) a certification that the Government of the Russian Federation has made significant efforts to reduce the number and intensity of cyber intrusions conducted by that Government.

(d) APPLICATION OF NEW UKRAINE-RELATED SANCTIONS.—The President may waive the initial application under subsection (a) of sanctions with respect to a person under Executive Order No. 13660, 13661, 13662, or 13685 only if the President submits to the appropriate congressional committees—

(1) a written determination that the waiver—
(A) is in the vital national security interests of the United States; or
(B) will further the enforcement of this title; and
(2) a certification that the Government of the Russian Federation is taking steps to implement the Minsk Agreement to address the ongoing conflict in eastern Ukraine, signed in Minsk, Belarus, on February 11, 2015, by the leaders of Ukraine, Russia, France, and Germany, the Minsk Protocol, which was agreed to on September 5, 2014, and any successor agreements that are agreed to by the Government of Ukraine.

SEC. 223. MODIFICATION OF IMPLEMENTATION OF EXECUTIVE ORDER NO. 13662.

(a) DETERMINATION THAT CERTAIN ENTITIES ARE SUBJECT TO SANCTIONS.—The Secretary of the Treasury may determine that a person meets one or more of the criteria in section 1(a) of Executive Order No. 13662 if that person is a state-owned entity operating in the railway or metals and mining sector of the economy of the Russian Federation.
(b) MODIFICATION OF DIRECTIVE 1 WITH RESPECT TO THE FINANCIAL SERVICES SECTOR OF THE RUSSIAN FEDERATION ECONOMY.—Not later than 60 days after the date of the enactment of this Act, the Secretary of the Treasury shall modify Directive 1 (as amended), dated September 12, 2014, issued by the Office of Foreign Assets Control under Executive Order No. 13662, or any successor directive (which shall be effective beginning on the date that is 60 days after the date of such modification), to ensure that the directive prohibits the conduct by United States persons or persons within the United States of all transactions in, provision of financing for, and other dealings in new debt of longer than 14 days maturity or new equity of persons determined to be subject to the directive, their property, or their interests in property.

(c) MODIFICATION OF DIRECTIVE 2 WITH RESPECT TO THE ENERGY SECTOR OF THE RUSSIAN FEDERATION ECONOMY.—Not later than 60 days after the date of the enactment of this Act, the Secretary of the Treasury shall modify Directive 2 (as amended), dated September 12, 2014, issued by the Office of Foreign Assets Control under Executive Order No. 13662, or any successor directive (which shall be effective beginning on the date that is 60 days after the date of such modification), to ensure that the directive prohibits the conduct by United States persons or persons within the United States of all transactions in, provision of financing for, and other dealings in new debt of longer than 60 days maturity of persons determined to be subject to the directive, their property, or their interests in property.

(d) MODIFICATION OF DIRECTIVE 4.—Not later than 90 days after the date of the enactment of this Act, the Secretary of the Treasury shall modify Directive 4, dated September 12, 2014, issued by the Office of Foreign Assets Control under Executive Order No. 13662, or any successor directive (which shall be effective beginning on the date that is 90 days after the date of such modification), to ensure that the directive prohibits the provision, exportation, or reexportation, directly or indirectly, by United States persons or persons within the United States, of goods, services (except for financial services), or technology in support of exploration or production for new deepwater, Arctic offshore, or shale projects—

(1) that have the potential to produce oil; and

(2) that involve any person determined to be subject to the directive or the property or interests in property of such a person who has a controlling interest or a substantial non-controlling ownership interest in such a project defined as not less than a 33 percent interest.

SEC. 224. IMPOSITION OF SANCTIONS WITH RESPECT TO ACTIVITIES OF THE RUSSIAN FEDERATION UNDERMINING CYBERSECURITY.

(a) In General.—On and after the date that is 60 days after the date of the enactment of this Act, the President shall—

(1) impose the sanctions described in subsection (b) with respect to any person that the President determines—

(A) knowingly engages in significant activities undermining cybersecurity against any person, including a democratic institution, or government on behalf of the Government of the Russian Federation; or
(B) is owned or controlled by, or acts or purports to act for or on behalf of, directly or indirectly, a person described in subparagraph (A);
(2) impose five or more of the sanctions described in section 235 with respect to any person that the President determines knowingly materially assists, sponsors, or provides financial, material, or technological support for, or goods or services (except financial services) in support of, an activity described in paragraph (1)(A); and
(3) impose three or more of the sanctions described in section 4(c) of the of the Ukraine Freedom Support Act of 2014 (22 U.S.C. 8923(c)) with respect to any person that the President determines knowingly provides financial services in support of an activity described in paragraph (1)(A).
(b) SANCTIONS DESCRIBED.—The sanctions described in this subsection are the following:
(1) ASSET BLOCKING.—The exercise of all powers granted to the President by the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) to the extent necessary to block and prohibit all transactions in all property and interests in property of a person determined by the President to be subject to subsection (a)(1) if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.
(2) EXCLUSION FROM THE UNITED STATES AND REVOCATION OF VISA OR OTHER DOCUMENTATION.—In the case of an alien determined by the President to be subject to subsection (a)(1), denial of a visa to, and exclusion from the United States of, the alien, and revocation in accordance with section 221(i) of the Immigration and Nationality Act (8 U.S.C. 1201(i)), of any visa or other documentation of the alien.
(c) APPLICATION OF NEW CYBER SANCTIONS.—The President may waive the initial application under subsection (a) of sanctions with respect to a person only if the President submits to the appropriate congressional committees—
(1) a written determination that the waiver—
(A) is in the vital national security interests of the United States; or
(B) will further the enforcement of this title; and
(2) a certification that the Government of the Russian Federation has made significant efforts to reduce the number and intensity of cyber intrusions conducted by that Government.
(d) SIGNIFICANT ACTIVITIES UNDERMINING CYBERSECURITY DEFINED.—In this section, the term “significant activities undermining cybersecurity” includes—
(1) significant efforts—
(A) to deny access to or degrade, disrupt, or destroy an information and communications technology system or network; or
(B) to exfiltrate, degrade, corrupt, destroy, or release information from such a system or network without authorization for purposes of—
(i) conducting influence operations; or
(ii) causing a significant misappropriation of funds, economic resources, trade secrets, personal identifications, or financial information for commercial or competitive advantage or private financial gain; (2) significant destructive malware attacks; and (3) significant denial of service activities.

SEC. 225. IMPOSITION OF SANCTIONS RELATING TO SPECIAL RUSSIAN CRUDE OIL PROJECTS.

Section 4(b)(1) of the Ukraine Freedom Support Act of 2014 (22 U.S.C. 8923(b)(1)) is amended by striking “on and after the date that is 45 days after the date of the enactment of this Act, the President may impose” and inserting “on and after the date that is 30 days after the date of the enactment of the Countering Russian Influence in Europe and Eurasia Act of 2017, the President shall impose, unless the President determines that it is not in the national interest of the United States to do so,”.

SEC. 226. IMPOSITION OF SANCTIONS WITH RESPECT TO RUSSIAN AND OTHER FOREIGN FINANCIAL INSTITUTIONS.

Section 5 of the Ukraine Freedom Support Act of 2014 (22 U.S.C. 8924) is amended— (1) in subsection (a)—  
(A) by striking “may impose” and inserting “shall impose, unless the President determines that it is not in the national interest of the United States to do so,”; and  
(B) by striking “on or after the date of the enactment of this Act” and inserting “on or after the date of the enactment of the Countering Russian Influence in Europe and Eurasia Act of 2017”; and  
(2) in subsection (b)—  
(A) by striking “may impose” and inserting “shall impose, unless the President determines that it is not in the national interest of the United States to do so,”; and  
(B) by striking “on or after the date that is 180 days after the date of the enactment of this Act” and inserting “on or after the date that is 30 days after the date of the enactment of the Countering Russian Influence in Europe and Eurasia Act of 2017”.

SEC. 227. MANDATORY IMPOSITION OF SANCTIONS WITH RESPECT TO SIGNIFICANT CORRUPTION IN THE RUSSIAN FEDERATION.

Section 9 of the Sovereignty, Integrity, Democracy, and Economic Stability of Ukraine Act of 2014 (22 U.S.C. 8908(a)) is amended— (1) in subsection (a)—  
(A) in the matter preceding paragraph (1), by striking “is authorized and encouraged to” and inserting “shall”; and  
(B) in paragraph (1)—  
(i) by striking “President determines is” and inserting “President determines is, on or after the date of the enactment of the Countering Russian Influence in Europe and Eurasia Act of 2017,”; and  
(ii) by inserting “or elsewhere” after “in the Russian Federation”;
(2) by redesignating subsection (d) as subsection (e);
(3) in subsection (c), by striking “The President” and inserting “except as provided in subsection (d), the President”; and
(4) by inserting after subsection (c) the following:

“(d) APPLICATION OF NEW SANCTIONS.—The President may waive the initial application of sanctions under subsection (b) with respect to a person only if the President submits to the appropriate congressional committees—

“(1) a written determination that the waiver—

“(A) is in the vital national security interests of the United States; or

“(B) will further the enforcement of this Act; and

“(2) a certification that the Government of the Russian Federation is taking steps to implement the Minsk Agreement to address the ongoing conflict in eastern Ukraine, signed in Minsk, Belarus, on February 11, 2015, by the leaders of Ukraine, Russia, France, and Germany, the Minsk Protocol, which was agreed to on September 5, 2014, and any successor agreements that are agreed to by the Government of Ukraine.”.

SEC. 228. MANDATORY IMPOSITION OF SANCTIONS WITH RESPECT TO CERTAIN TRANSACTIONS WITH FOREIGN SANCTIONS EVADERS AND SERIOUS HUMAN RIGHTS ABUSERS IN THE RUSSIAN FEDERATION.

(a) In General.—The Support for the Sovereignty, Integrity, Democracy, and Economic Stability of Ukraine Act of 2014 (22 U.S.C. 8901 et seq.) is amended by adding at the end the following:

“SEC. 10. MANDATORY IMPOSITION OF SANCTIONS WITH RESPECT TO CERTAIN TRANSACTIONS WITH PERSONS THAT EVADE SANCTIONS IMPOSED WITH RESPECT TO THE RUSSIAN FEDERATION.

“(a) In General.—The President shall impose the sanctions described in subsection (b) with respect to a foreign person if the President determines that the foreign person knowingly, on or after the date of the enactment of the Countering Russian Influence in Europe and Eurasia Act of 2017—

“(1) materially violates, attempts to violate, conspires to violate, or causes a violation of any license, order, regulation, or prohibition contained in or issued pursuant to any covered Executive order, this Act, or the Ukraine Freedom Support Act of 2014 (22 U.S.C. 8921 et seq.); or

“(2) facilitates a significant transaction or transactions, including deceptive or structured transactions, for or on behalf of—

“(A) any person subject to sanctions imposed by the United States with respect to the Russian Federation; or

“(B) any child, spouse, parent, or sibling of an individual described in subparagraph (A).

“(b) Sanctions Described.—The sanctions described in this subsection are the exercise of all powers granted to the President by the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) to the extent necessary to block and prohibit all transactions in all property and interests in property of a person determined by the President to be subject to subsection (a) if such property and interests in property are in the United States, come
within the United States, or are or come within the possession or control of a United States person.

"(c) IMPLEMENTATION; PENALTIES.—

"(1) IMPLEMENTATION.—The President may exercise all authorities provided to the President under sections 203 and 205 of the International Emergency Economic Powers Act (50 U.S.C. 1702 and 1704) to carry out subsection (b).

"(2) PENALTIES.—A person that violates, attempts to violate, conspires to violate, or causes a violation of subsection (b) or any regulation, license, or order issued to carry out subsection (b) shall be subject to the penalties set forth in subsections (b) and (c) of section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705) to the same extent as a person that commits an unlawful act described in subsection (a) of that section.

"(d) APPLICATION OF NEW SANCTIONS.—The President may waive the initial application of sanctions under subsection (b) with respect to a person only if the President submits to the appropriate congressional committees—

"(1) a written determination that the waiver—

"(A) is in the vital national security interests of the United States; or

"(B) will further the enforcement of this Act;

"(2) in the case of sanctions imposed under this section in connection with a covered Executive order described in subparagraph (A), (B), (C), or (D) of subsection (f)(1), a certification that the Government of the Russian Federation is taking steps to implement the Minsk Agreement to address the ongoing conflict in eastern Ukraine, signed in Minsk, Belarus, on February 11, 2015, by the leaders of Ukraine, Russia, France, and Germany, the Minsk Protocol, which was agreed to on September 5, 2014, and any successor agreements that are agreed to by the Government of Ukraine; and

"(3) in the case of sanctions imposed under this section in connection with a covered Executive order described in subparagraphs (E) or (F) of subsection (f)(1), a certification that the Government of the Russian Federation has made significant efforts to reduce the number and intensity of cyber intrusions conducted by that Government.

"(e) TERMINATION.—Subject to section 216 of the Russia Sanctions Review Act of 2017, the President may terminate the application of sanctions under subsection (b) with respect to a person if the President submits to the appropriate congressional committees—

"(1) a notice of and justification for the termination; and

"(2) a notice that—

"(A) the person is not engaging in the activity that was the basis for the sanctions or has taken significant verifiable steps toward stopping the activity; and

"(B) the President has received reliable assurances that the person will not knowingly engage in activity subject to sanctions under subsection (a) in the future.

"(f) DEFINITIONS.—In this section:

"(1) COVERED EXECUTIVE ORDER.—The term 'covered Executive order' means any of the following:
“(A) Executive Order No. 13660 (79 Fed. Reg. 13493; relating to blocking property of certain persons contributing to the situation in Ukraine).

(B) Executive Order No. 13661 (79 Fed. Reg. 15535; relating to blocking property of additional persons contributing to the situation in Ukraine).

(C) Executive Order No. 13662 (79 Fed. Reg. 16169; relating to blocking property of additional persons contributing to the situation in Ukraine).

(D) Executive Order No. 13685 (79 Fed. Reg. 77357; relating to blocking property of certain persons and prohibiting certain transactions with respect to the Crimea region of Ukraine).

(E) Executive Order No. 13694 (80 Fed. Reg. 18077; relating to blocking the property of certain persons engaging in significant malicious cyber-enabled activities), relating to the Russian Federation.

(F) Executive Order No. 13757 (82 Fed. Reg. 1; relating to taking additional steps to address the national emergency with respect to significant malicious cyber-enabled activities), relating to the Russian Federation.

"(2) FOREIGN PERSON.—The term ‘foreign person’ has the meaning given such term in section 595.304 of title 31, Code of Federal Regulations (as in effect on the date of the enactment of this section).

"(3) STRUCTURED.—The term ‘structured’, with respect to a transaction, has the meaning given the term ‘structure’ in paragraph (xx) of section 1010.100 of title 31, Code of Federal Regulations (or any corresponding similar regulation or ruling).

**SEC. 11. MANDATORY IMPOSITION OF SANCTIONS WITH RESPECT TO TRANSACTIONS WITH PERSONS RESPONSIBLE FOR HUMAN RIGHTS ABUSES.**

“(a) IN GENERAL.—The President shall impose the sanctions described in subsection (b) with respect to a foreign person if the President determines that the foreign person, based on credible information, on or after the date of the enactment of this section—

"(1) is responsible for, complicit in, or responsible for ordering, controlling, or otherwise directing, the commission of serious human rights abuses in any territory forcibly occupied or otherwise controlled by the Government of the Russian Federation;

"(2) materially assists, sponsors, or provides financial, material, or technological support for, or goods or services to, a foreign person described in paragraph (1); or

"(3) is owned or controlled by, or acts or purports to act for or on behalf of, directly or indirectly, a foreign person described in paragraph (1).

"(b) SANCTIONS DESCRIBED.—

"(1) ASSET BLOCKING.—The exercise of all powers granted to the President by the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) to the extent necessary to block and prohibit all transactions in all property and interests in property of a person determined by the President to be subject to subsection (a) if such property and interests in property are in the United States, come within the United
States, or are or come within the possession or control of a United States person.

(2) EXCLUSION FROM THE UNITED STATES AND REVOCATION OF VISA OR OTHER DOCUMENTATION.—In the case of an alien determined by the President to be subject to subsection (a), denial of a visa to, and exclusion from the United States of, the alien, and revocation in accordance with section 221(i) of the Immigration and Nationality Act (8 U.S.C. 1201(i)), of any visa or other documentation of the alien.

(c) APPLICATION OF NEW SANCTIONS.—The President may waive the initial application of sanctions under subsection (b) with respect to a person only if the President submits to the appropriate congressional committees—

(1) a written determination that the waiver—

(A) is in the vital national security interests of the United States; or

(B) will further the enforcement of this Act; and

(2) a certification that the Government of the Russian Federation has made efforts to reduce serious human rights abuses in territory forcibly occupied or otherwise controlled by that Government.

(d) IMPLEMENTATION; PENALTIES.—

(1) IMPLEMENTATION.—The President may exercise all authorities provided to the President under sections 203 and 205 of the International Emergency Economic Powers Act (50 U.S.C. 1702 and 1704) to carry out subsection (b)(1).

(2) PENALTIES.—A person that violates, attempts to violate, conspires to violate, or causes a violation of subsection (b)(1) or any regulation, license, or order issued to carry out subsection (b)(1) shall be subject to the penalties set forth in subsections (b) and (c) of section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705) to the same extent as a person that commits an unlawful act described in subsection (a) of that section.

(e) TERMINATION.—Subject to section 216 of Russia Sanctions Review Act of 2017, the President may terminate the application of sanctions under subsection (b) with respect to a person if the President submits to the appropriate congressional committees—

(1) a notice of and justification for the termination; and

(2) a notice—

(A) that—

(i) the person is not engaging in the activity that was the basis for the sanctions or has taken significant verifiable steps toward stopping the activity; and

(ii) the President has received reliable assurances that the person will not knowingly engage in activity subject to sanctions under subsection (a) in the future; or

(B) that the President determines that insufficient basis exists for the determination by the President under subsection (a) with respect to the person.”.

(b) DEFINITION OF APPROPRIATE CONGRESSIONAL COMMIT-TEES.—Section 2(2) of the Support for the Sovereignty, Integrity, Democracy, and Economic Stability of Ukraine Act of 2014 (22 U.S.C. 8901(2)) is amended—
(1) in subparagraph (A), by inserting “the Committee on Banking, Housing, and Urban Affairs,” before “the Committee on Foreign Relations”; and
(2) in subparagraph (B), by inserting “the Committee on Financial Services” before “the Committee on Foreign Affairs”.

SEC. 229. NOTIFICATIONS TO CONGRESS UNDER UKRAINE FREEDOM SUPPORT ACT OF 2014.

(a) SANCTIONS RELATING TO DEFENSE AND ENERGY SECTORS OF THE RUSSIAN FEDERATION.—Section 4 of the Ukraine Freedom Support Act of 2014 (22 U.S.C. 8923) is amended—
(1) by redesignating subsections (g) and (h) as subsections (h) and (i), respectively;
(2) by inserting after subsection (f) the following:
   "(g) NOTIFICATIONS AND CERTIFICATIONS TO CONGRESS.—
   "(1) IMPOSITION OF SANCTIONS.—The President shall notify the appropriate congressional committees in writing not later than 15 days after imposing sanctions with respect to a foreign person under subsection (a) or (b).
   "(2) TERMINATION OF SANCTIONS WITH RESPECT TO RUSSIAN PRODUCERS, TRANSFERORS, OR BROKERS OF DEFENSE ARTICLES.—Subject to section 216 of the Russia Sanctions Review Act of 2017, the President may terminate the imposition of sanctions under subsection (a)(2) with respect to a foreign person if the President submits to the appropriate congressional committees—
   "(A) a notice of and justification for the termination; and
   "(B) a notice that—
   "(i) the foreign person is not engaging in the activity that was the basis for the sanctions or has taken significant verifiable steps toward stopping the activity; and
   "(ii) the President has received reliable assurances that the foreign person will not knowingly engage in activity subject to sanctions under subsection (a)(2) in the future;"; and
(3) in subparagraph (B)(ii) of subsection (a)(3), by striking "subsection (h)" and inserting "subsection (i)".

(b) SANCTIONS ON RUSSIAN AND OTHER FOREIGN FINANCIAL INSTITUTIONS.—Section 5 of the Ukraine Freedom Support Act of 2014 (22 U.S.C. 8924) is amended—
(1) by redesignating subsections (e) and (f) as subsections (f) and (g), respectively;
(2) by inserting after subsection (d) the following:
   "(e) NOTIFICATION TO CONGRESS ON IMPOSITION OF SANCTIONS.—The President shall notify the appropriate congressional committees in writing not later than 15 days after imposing sanctions with respect to a foreign financial institution under subsection (a) or (b);"; and
(3) in subsection (g), as redesignated by paragraph (1), by striking "section 4(h)" and inserting "section 4(i)".

SEC. 230. STANDARDS FOR TERMINATION OF CERTAIN SANCTIONS WITH RESPECT TO THE RUSSIAN FEDERATION.

(a) SANCTIONS RELATING TO UNDERMINING THE PEACE, SECURITY, SOVEREIGNTY, OR TERRITORIAL INTEGRITY OF UKRAINE.—Section 8 of the Sovereignty, Integrity, Democracy, and
H. R. 3364—31

Economic Stability of Ukraine Act of 2014 (22 U.S.C. 8907) is amended—
(1) by redesignating subsection (d) as subsection (e); and
(2) by inserting after subsection (c) the following:
"(d) TERMINATION.—Subject to section 216 of the Russia Sanctions Review Act of 2017, the President may terminate the application of sanctions under subsection (b) with respect to a person if the President submits to the appropriate congressional committees a notice that—
"(1) the person is not engaging in the activity that was the basis for the sanctions or has taken significant verifiable steps toward stopping the activity; and
"(2) the President has received reliable assurances that the person will not knowingly engage in activity subject to sanctions under subsection (a) in the future.".

(b) SANCTIONS RELATING TO CORRUPTION.—Section 9 of the Sovereignty, Integrity, Democracy, and Economic Stability of Ukraine Act of 2014 (22 U.S.C. 8908) is amended—
(1) by redesignating subsection (d) as subsection (e); and
(2) by inserting after subsection (c) the following:
"(d) TERMINATION.—Subject to section 216 of the Russia Sanctions Review Act of 2017, the President may terminate the application of sanctions under subsection (b) with respect to a person if the President submits to the appropriate congressional committees a notice that—
"(1) the person is not engaging in the activity that was the basis for the sanctions or has taken significant verifiable steps toward stopping the activity; and
"(2) the President has received reliable assurances that the person will not knowingly engage in activity subject to sanctions under subsection (a) in the future.".

SEC. 231. IMPOSITION OF SANCTIONS WITH RESPECT TO PERSONS ENGAGING IN TRANSACTIONS WITH THE INTELLIGENCE OR DEFENSE SECTORS OF THE GOVERNMENT OF THE RUSSIAN FEDERATION.

(a) IN GENERAL.—On and after the date that is 180 days after the date of the enactment of this Act, the President shall impose five or more of the sanctions described in section 235 with respect to a person the President determines knowingly, on or after such date of enactment, engages in a significant transaction with a person that is part of, or operates for or on behalf of, the defense or intelligence sectors of the Government of the Russian Federation, including the Main Intelligence Agency of the General Staff of the Armed Forces of the Russian Federation or the Federal Security Service of the Russian Federation.

(b) APPLICATION OF NEW SANCTIONS.—The President may waive the initial application of sanctions under subsection (a) with respect to a person only if the President submits to the appropriate congressional committees—
(1) a written determination that the waiver—
(A) is in the vital national security interests of the United States; or
(B) will further the enforcement of this title; and
(2) a certification that the Government of the Russian Federation has made significant efforts to reduce the number
and intensity of cyber intrusions conducted by that Government.

(c) Delay of Imposition of Sanctions.—The President may delay the imposition of sanctions under subsection (a) with respect to a person if the President certifies to the appropriate congressional committees, not less frequently than every 180 days while the delay is in effect, that the person is substantially reducing the number of significant transactions described in subsection (a) in which that person engages.

(d) Requirement to Issue Guidance.—Not later than 60 days after the date of the enactment of this Act, the President shall issue regulations or other guidance to specify the persons that are part of, or operate for or on behalf of, the defense and intelligence sectors of the Government of the Russian Federation.

(e) Penalties.—A person that violates, attempts to violate, conspires to violate, or causes a violation of subsection (a) or any regulation, license, or order issued to carry out subsection (a) shall be subject to the penalties set forth in subsections (b) and (c) of section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705) to the same extent as a person that commits an unlawful act described in subsection (a) of that section.


(a) In General.—The President, in coordination with allies of the United States, may impose five or more of the sanctions described in section 235 with respect to a person if the President determines that the person knowingly, on or after the date of the enactment of this Act, makes an investment described in subsection (b) or sells, leases, or provides to the Russian Federation, for the construction of Russian energy export pipelines, goods, services, technology, information, or support described in subsection (c)—

(1) any of which has a fair market value of $1,000,000 or more; or

(2) that, during a 12-month period, have an aggregate fair market value of $5,000,000 or more.

(b) Investment Described.—An investment described in this subsection is an investment that directly and significantly contributes to the enhancement of the ability of the Russian Federation to construct energy export pipelines.

(c) Goods, Services, Technology, Information, or Support Described.—Goods, services, technology, information, or support described in this subsection are goods, services, technology, information, or support that could directly and significantly facilitate the maintenance or expansion of the construction, modernization, or repair of energy export pipelines by the Russian Federation.

SEC. 233. Sanctions with Respect to Investment in or Facilitation of Privatization of State-Owned Assets by the Russian Federation.

(a) In General.—The President shall impose five or more of the sanctions described in section 235 if the President determines that a person, with actual knowledge, on or after the date of the enactment of this Act, makes an investment of $10,000,000 or more (or any combination of investments of not less than $1,000,000 each, which in the aggregate equals or exceeds
$10,000,000 in any 12-month period), or facilitates such an investment, if the investment directly and significantly contributes to the ability of the Russian Federation to privatize state-owned assets in a manner that unjustly benefits—

(1) officials of the Government of the Russian Federation; or

(2) close associates or family members of those officials.

(b) APPLICATION OF NEW SANCTIONS.—The President may waive the initial application of sanctions under subsection (a) with respect to a person only if the President submits to the appropriate congressional committees—

(1) a written determination that the waiver—

(A) is in the vital national security interests of the United States; or

(B) will further the enforcement of this title; and

(2) a certification that the Government of the Russian Federation is taking steps to implement the Minsk Agreement to address the ongoing conflict in eastern Ukraine, signed in Minsk, Belarus, on February 11, 2015, by the leaders of Ukraine, Russia, France, and Germany, the Minsk Protocol, which was agreed to on September 5, 2014, and any successor agreements that are agreed to by the Government of Ukraine.

SEC. 234. SANCTIONS WITH RESPECT TO THE TRANSFER OF ARMS AND RELATED MATERIEL TO SYRIA.

(a) IMPOSITION OF SANCTIONS.—

(1) IN GENERAL.—The President shall impose on a foreign person the sanctions described in subsection (b) if the President determines that such foreign person has, on or after the date of enactment of this Act, knowingly exported, transferred, or otherwise provided to Syria significant financial, material, or technological support that contributes materially to the ability of the Government of Syria to—

(A) acquire or develop chemical, biological, or nuclear weapons or related technologies;

(B) acquire or develop ballistic or cruise missile capabilities;

(C) acquire or develop destabilizing numbers and types of advanced conventional weapons;

(D) acquire significant defense articles, defense services, or defense information (as such terms are defined under the Arms Export Control Act (22 U.S.C. 2751 et seq.)); or

(E) acquire items designated by the President for purposes of the United States Munitions List under section 38(a)(1) of the Arms Export Control Act (22 U.S.C. 2778(a)(1)).

(2) APPLICABILITY TO OTHER FOREIGN PERSONS.—The sanctions described in subsection (b) shall also be imposed on any foreign person that—

(A) is a successor entity to a foreign person described in paragraph (1); or

(B) is owned or controlled by, or has acted for or on behalf of, a foreign person described in paragraph (1).

(b) SANCTIONS DESCRIBED.—The sanctions to be imposed on a foreign person described in subsection (a) are the following:
(1) BLOCKING OF PROPERTY.—The President shall exercise all powers granted by the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (except that the requirements of section 202 of such Act (50 U.S.C. 1701) shall not apply) to the extent necessary to block and prohibit all transactions in all property and interests in property of the foreign person if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

(2) ALIENS INELIGIBLE FOR VISAS, ADMISSION, OR PAROLE.—

(A) EXCLUSION FROM THE UNITED STATES.—If the foreign person is an individual, the Secretary of State shall deny a visa to, and the Secretary of Homeland Security shall exclude from the United States, the foreign person.

(B) CURRENT VISAS REVOKED.—

(i) IN GENERAL.—The issuing consular officer, the Secretary of State, or the Secretary of Homeland Security (or a designee of one of such Secretaries) shall revoke any visa or other entry documentation issued to the foreign person regardless of when issued.

(ii) EFFECT OF REVOCATION.—A revocation under clause (i) shall take effect immediately and shall automatically cancel any other valid visa or entry documentation that is in the possession of the foreign person.

(c) WAIVER.—Subject to section 216, the President may waive the application of sanctions under subsection (b) with respect to a person if the President determines that such a waiver is in the national security interest of the United States.

(d) DEFINITIONS.—In this section:

(1) FINANCIAL, MATERIAL, OR TECHNOLOGICAL SUPPORT.—The term "financial, material, or technological support" has the meaning given such term in section 542.304 of title 31, Code of Federal Regulations (or any corresponding similar regulation or ruling).

(2) FOREIGN PERSON.—The term "foreign person" has the meaning given such term in section 594.304 of title 31, Code of Federal Regulations (or any corresponding similar regulation or ruling).

(3) SYRIA.—The term "Syria" has the meaning given such term in section 542.316 of title 31, Code of Federal Regulations (or any corresponding similar regulation or ruling).

SEC. 235. SANCTIONS DESCRIBED.

(a) SANCTIONS DESCRIBED.—The sanctions to be imposed with respect to a person under section 224(a)(2), 231(b), 232(a), or 233(a) are the following:

(1) EXPORT-IMPORT BANK ASSISTANCE FOR EXPORTS TO SANCTIONED PERSONS.—The President may direct the Export-Import Bank of the United States not to give approval to the issuance of any guarantee, insurance, extension of credit, or participation in the extension of credit in connection with the export of any goods or services to the sanctioned person.

(2) EXPORT SANCTION.—The President may order the United States Government not to issue any specific license and not to grant any other specific permission or authority
to export any goods or technology to the sanctioned person under—
(B) the Arms Export Control Act (22 U.S.C. 2751 et seq.);
(C) the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.); or
(D) any other statute that requires the prior review and approval of the United States Government as a condition for the export or reexport of goods or services.
(3) LOANS FROM UNITED STATES FINANCIAL INSTITUTIONS.—The President may prohibit any United States financial institution from making loans or providing credits to the sanctioned person totaling more than $10,000,000 in any 12-month period unless the person is engaged in activities to relieve human suffering and the loans or credits are provided for such activities.
(4) LOANS FROM INTERNATIONAL FINANCIAL INSTITUTIONS.—The President may direct the United States executive director to each international financial institution to use the voice and vote of the United States to oppose any loan from the international financial institution that would benefit the sanctioned person.
(5) PROHIBITIONS ON FINANCIAL INSTITUTIONS.—The following prohibitions may be imposed against the sanctioned person if that person is a financial institution:
(A) PROHIBITION ON DESIGNATION AS PRIMARY DEALER.—Neither the Board of Governors of the Federal Reserve System nor the Federal Reserve Bank of New York may designate, or permit the continuation of any prior designation of, the financial institution as a primary dealer in United States Government debt instruments.
(B) PROHIBITION ON SERVICE AS A REPOSITORY OF GOVERNMENT FUNDS.—The financial institution may not serve as agent of the United States Government or serve as repository for United States Government funds.
The imposition of either sanction under subparagraph (A) or (B) shall be treated as one sanction for purposes of subsection (b), and the imposition of both such sanctions shall be treated as two sanctions for purposes of subsection (b).
(6) PROCUREMENT SANCTION.—The United States Government may not procure, or enter into any contract for the procurement of, any goods or services from the sanctioned person.
(7) FOREIGN EXCHANGE.—The President may, pursuant to such regulations as the President may prescribe, prohibit any transactions in foreign exchange that are subject to the jurisdiction of the United States and in which the sanctioned person has any interest.
(8) BANKING TRANSACTIONS.—The President may, pursuant to such regulations as the President may prescribe, prohibit any transfers of credit or payments between financial institutions or by, through, or to any financial institution, to the
extent that such transfers or payments are subject to the jurisdiction of the United States and involve any interest of the sanctioned person.

(9) Property Transactions.—The President may, pursuant to such regulations as the President may prescribe, prohibit any person from—

(A) acquiring, holding, withholding, using, transferring, withdrawing, transporting, importing, or exporting any property that is subject to the jurisdiction of the United States and with respect to which the sanctioned person has any interest;

(B) dealing in or exercising any right, power, or privilege with respect to such property; or

(C) conducting any transaction involving such property.

(10) Ban on Investment in Equity or Debt of Sanctioned Person.—The President may, pursuant to such regulations or guidelines as the President may prescribe, prohibit any United States person from investing in or purchasing significant amounts of equity or debt instruments of the sanctioned person.

(11) Exclusion of Corporate Officers.—The President may direct the Secretary of State to deny a visa to, and the Secretary of Homeland Security to exclude from the United States, any alien that the President determines is a corporate officer or principal of, or a shareholder with a controlling interest in, the sanctioned person.

(12) Sanctions on Principal Executive Officers.—The President may impose on the principal executive officer or officers of the sanctioned person, or on persons performing similar functions and with similar authorities as such officer or officers, any of the sanctions under this subsection.

"sanctioned person" means a person subject to sanctions under section 224(a)(2), 231(b), 232(a), or 233(a).

SEC. 236. Exceptions, Waiver, and Termination.

(a) Exceptions.—The provisions of this part and amendments made by this part shall not apply with respect to the following:

(1) Activities subject to the reporting requirements under title V of the National Security Act of 1947 (50 U.S.C. 3091 et seq.), or any authorized intelligence activities of the United States.

(2) The admission of an alien to the United States if such admission is necessary to comply with United States obligations under the Agreement between the United Nations and the United States of America regarding the Headquarters of the United Nations, signed at Lake Success June 26, 1947, and entered into force November 21, 1947, under the Convention on Consular Relations, done at Vienna April 24, 1963, and entered into force March 19, 1967, or under other international agreements.

(b) Waiver of Sanctions That Are Imposed.—Subject to section 216, if the President imposes sanctions with respect to a person under this part or the amendments made by this part, the President may waive the application of those sanctions if the President determines that such a waiver is in the national security interest of the United States.
(c) **Termination.**—Subject to section 216, the President may terminate the application of sanctions under section 224, 231, 232, 233, or 234 with respect to a person if the President submits to the appropriate congressional committees—

(1) a notice of and justification for the termination; and

(2) a notice that—

(A) the person is not engaging in the activity that was the basis for the sanctions or has taken significant verifiable steps toward stopping the activity; and

(B) the President has received reliable assurances that the person will not knowingly engage in activity subject to sanctions under this part in the future.

**SEC. 237. EXCEPTION RELATING TO ACTIVITIES OF THE NATIONAL AERONAUTICS AND SPACE ADMINISTRATION.**

(a) **In General.**—This Act and the amendments made by this Act shall not apply with respect to activities of the National Aeronautics and Space Administration.

(b) **Rule of Construction.**—Nothing in this Act or the amendments made by this Act shall be construed to authorize the imposition of any sanction or other condition, limitation, restriction, or prohibition, that directly or indirectly impedes the supply by any entity of the Russian Federation of any product or service, or the procurement of such product or service by any contractor or subcontractor of the United States or any other entity, relating to or in connection with any space launch conducted for—

(1) the National Aeronautics and Space Administration; or

(2) any other non-Department of Defense customer.

**SEC. 238. RULE OF CONSTRUCTION.**

Nothing in this part or the amendments made by this part shall be construed—


(2) to prohibit a contractor or subcontractor of the Department of Defense from acquiring components referred to in such section 1608.

**PART 3—REPORTS**

**SEC. 241. REPORT ON OLIGARCHS AND PARASTATAL ENTITIES OF THE RUSSIAN FEDERATION.**

(a) **In General.**—Not later than 180 days after the date of the enactment of this Act, the Secretary of the Treasury, in consultation with the Director of National Intelligence and the Secretary of State, shall submit to the appropriate congressional committees a detailed report on the following:

(1) Senior foreign political figures and oligarchs in the Russian Federation, including the following:
H. R. 3364—38

(A) An identification of the most significant senior foreign political figures and oligarchs in the Russian Federation, as determined by their closeness to the Russian regime and their net worth.

(B) An assessment of the relationship between individuals identified under subparagraph (A) and President Vladimir Putin or other members of the Russian ruling elite.

(C) An identification of any indices of corruption with respect to those individuals.

(D) The estimated net worth and known sources of income of those individuals and their family members (including spouses, children, parents, and siblings), including assets, investments, other business interests, and relevant beneficial ownership information.

(E) An identification of the non-Russian business affiliations of those individuals.

(2) Russian parastatal entities, including an assessment of the following:
   (A) The emergence of Russian parastatal entities and their role in the economy of the Russian Federation.
   (B) The leadership structures and beneficial ownership of those entities.
   (C) The scope of the non-Russian business affiliations of those entities.

(3) The exposure of key economic sectors of the United States to Russian politically exposed persons and parastatal entities, including, at a minimum, the banking, securities, insurance, and real estate sectors.

(4) The likely effects of imposing debt and equity restrictions on Russian parastatal entities, as well as the anticipated effects of adding Russian parastatal entities to the list of specially designated nationals and blocked persons maintained by the Office of Foreign Assets Control of the Department of the Treasury.

(5) The potential impacts of imposing secondary sanctions with respect to Russian oligarchs, Russian state-owned enterprises, and Russian parastatal entities, including impacts on the entities themselves and on the economy of the Russian Federation, as well as on the economies of the United States and allies of the United States.

(b) FORM OF REPORT.—The report required under subsection (a) shall be submitted in an unclassified form, but may contain a classified annex.

(c) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term “appropriate congressional committees” means—
   (A) the Committee on Banking, Housing, and Urban Affairs, the Committee on Foreign Relations, and the Committee on Finance of the Senate; and
   (B) the Committee on Foreign Affairs, the Committee on Financial Services, and the Committee on Ways and Means of the House of Representatives.

(2) SENIOR FOREIGN POLITICAL FIGURE.—The term “senior foreign political figure” has the meaning given that term in section 1010.605 of title 31, Code of Federal Regulations (or any corresponding similar regulation or ruling).
H. R. 3364—39

SEC. 242. REPORT ON EFFECTS OF EXPANDING SANCTIONS TO INCLUDE SOVEREIGN DEBT AND DERIVATIVE PRODUCTS.

(a) In General.—Not later than 180 days after the date of the enactment of this Act, the Secretary of the Treasury, in consultation with the Director of National Intelligence and the Secretary of State, shall submit to the appropriate congressional committees a report describing in detail the potential effects of expanding sanctions under Directive 1 (as amended), dated September 12, 2014, issued by the Office of Foreign Assets Control under Executive Order No. 13662 (79 Fed. Reg. 16169; relating to blocking property of additional persons contributing to the situation in Ukraine), or any successor directive, to include sovereign debt and the full range of derivative products.

(b) Form of Report.—The report required under subsection (a) shall be submitted in an unclassified form, but may contain a classified annex.

(c) Appropriate Congressional Committees Defined.—In this section, the term “appropriate congressional committees” means—

(1) the Committee on Banking, Housing, and Urban Affairs, the Committee on Foreign Relations, and the Committee on Finance of the Senate; and

(2) the Committee on Foreign Affairs, the Committee on Financial Services, and the Committee on Ways and Means of the House of Representatives.

SEC. 243. REPORT ON ILLICIT FINANCE RELATING TO THE RUSSIAN FEDERATION.

(a) In General.—Not later than 1 year after the date of the enactment of this Act, and not later than the end of each 1-year period thereafter until 2021, the Secretary of the Treasury shall submit to the appropriate congressional committees a report describing interagency efforts in the United States to combat illicit finance relating to the Russian Federation.

(b) Elements.—The report required by subsection (a) shall contain a summary of efforts by the United States to do the following:

(1) Identify, investigate, map, and disrupt illicit financial flows linked to the Russian Federation if such flows affect the United States financial system or those of major allies of the United States.

(2) Conduct outreach to the private sector, including information sharing efforts to strengthen compliance efforts by entities, including financial institutions, to prevent illicit financial flows described in paragraph (1).

(3) Engage and coordinate with allied international partners on illicit finance, especially in Europe, to coordinate efforts to uncover and prosecute the networks responsible for illicit financial flows described in paragraph (1), including examples of that engagement and coordination.

(4) Identify foreign sanctions evaders and loopholes within the sanctions regimes of foreign partners of the United States.

(5) Expand the number of real estate geographic targeting orders or other regulatory actions, as appropriate, to degrade illicit financial activity relating to the Russian Federation in relation to the financial system of the United States.
(6) Provide support to counter those involved in illicit finance relating to the Russian Federation across all appropriate law enforcement, intelligence, regulatory, and financial authorities of the Federal Government, including by imposing sanctions with respect to or prosecuting those involved.

(7) In the case of the Department of the Treasury and the Department of Justice, investigate or otherwise develop major cases, including a description of those cases.

(c) BRIEFING.—After submitting a report under this section, the Secretary of the Treasury shall provide briefings to the appropriate congressional committees with respect to that report.

(d) COORDINATION.—The Secretary of the Treasury shall coordinate with the Attorney General, the Director of National Intelligence, the Secretary of Homeland Security, and the Secretary of State in preparing each report under this section.

(e) FORM.—Each report submitted under this section shall be submitted in unclassified form, but may contain a classified annex.

(f) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term “appropriate congressional committees” means—

(A) the Committee on Banking, Housing, and Urban Affairs, the Committee on Foreign Relations, and the Committee on Finance of the Senate; and

(B) the Committee on Foreign Affairs, the Committee on Financial Services, and the Committee on Ways and Means of the House of Representatives.

(2) ILLICIT FINANCE.—The term “illicit finance” means the financing of terrorism, narcotics trafficking, or proliferation, money laundering, or other forms of illicit financing domestically or internationally, as defined by the President.

Subtitle B—Countering Russian Influence in Europe and Eurasia

SEC. 251. FINDINGS.

Congress makes the following findings:

(1) The Government of the Russian Federation has sought to exert influence throughout Europe and Eurasia, including in the former states of the Soviet Union, by providing resources to political parties, think tanks, and civil society groups that sow distrust in democratic institutions and actors, promote xenophobic and illiberal views, and otherwise undermine European unity. The Government of the Russian Federation has also engaged in well-documented corruption practices as a means toward undermining and buying influence in European and Eurasian countries.

(2) The Government of the Russian Federation has largely eliminated a once-vibrant Russian-language independent media sector and severely curtails free and independent media within the borders of the Russian Federation. Russian-language media organizations that are funded and controlled by the Government of the Russian Federation and disseminate information within and outside of the Russian Federation routinely traffic in anti-Western disinformation, while few independent, fact-based media sources provide objective reporting for Russian-speaking audiences inside or outside of the Russian Federation.
(3) The Government of the Russian Federation continues to violate its commitments under the Memorandum on Security Assurances in connection with Ukraine’s Accession to the Treaty on the Non-Proliferation of Nuclear Weapons, done at Budapest December 5, 1994, and the Conference on Security and Co-operation in Europe Final Act, concluded at Helsinki August 1, 1975 (commonly referred to as the “Helsinki Final Act”), which laid the groundwork for the establishment of the Organization for Security and Co-operation in Europe, of which the Russian Federation is a member, by its illegal annexation of Crimea in 2014, its illegal occupation of South Ossetia and Abkhazia in Georgia in 2008, and its ongoing destabilizing activities in eastern Ukraine.

(4) The Government of the Russian Federation continues to ignore the terms of the August 2008 ceasefire agreement relating to Georgia, which requires the withdrawal of Russian Federation troops, free access by humanitarian groups to the regions of South Ossetia and Abkhazia, and monitoring of the conflict areas by the European Union Monitoring Mission.

(5) The Government of the Russian Federation is failing to comply with the terms of the Minsk Agreement to address the ongoing conflict in eastern Ukraine, signed in Minsk, Belarus, on February 11, 2015, by the leaders of Ukraine, Russia, France, and Germany, as well as the Minsk Protocol, which was agreed to on September 5, 2014.

(6) The Government of the Russian Federation is—

(A) in violation of the Treaty between the United States of America and the Union of Soviet Socialist Republics on the Elimination of their Intermediate-Range and Shorter-Range Missiles, signed at Washington December 8, 1987, and entered into force June 1, 1988 (commonly known as the “INF Treaty”); and

(B) failing to meet its obligations under the Treaty on Open Skies, done at Helsinki March 24, 1992, and entered into force January 1, 2002 (commonly known as the “Open Skies Treaty”).

SEC. 252. SENSE OF CONGRESS.

It is the sense of Congress that—

(1) the Government of the Russian Federation bears responsibility for the continuing violence in Eastern Ukraine, including the death on April 24, 2017, of Joseph Stone, a citizen of the United States working as a monitor for the Organization for Security and Co-operation in Europe;

(2) the President should call on the Government of the Russian Federation—

(A) to withdraw all of its forces from the territories of Georgia, Ukraine, and Moldova;

(B) to return control of the borders of those territories to their respective governments; and

(C) to cease all efforts to undermine the popularly elected governments of those countries;

(3) the Government of the Russian Federation has applied, and continues to apply, to the countries and peoples of Georgia and Ukraine, traditional uses of force, intelligence operations, and influence campaigns, which represent clear and present threats to the countries of Europe and Eurasia;
(4) in response, the countries of Europe and Eurasia should redouble efforts to build resilience within their institutions, political systems, and civil societies;

(5) the United States supports the institutions that the Government of the Russian Federation seeks to undermine, including the North Atlantic Treaty Organization and the European Union;

(6) a strong North Atlantic Treaty Organization is critical to maintaining peace and security in Europe and Eurasia;

(7) the United States should continue to work with the European Union as a partner against aggression by the Government of the Russian Federation, coordinating aid programs, development assistance, and other counter-Russian efforts;

(8) the United States should encourage the establishment of a commission for media freedom within the Council of Europe, modeled on the Venice Commission regarding rule of law issues, that would be chartered to provide governments with expert recommendations on maintaining legal and regulatory regimes supportive of free and independent media and an informed citizenry able to distinguish between fact-based reporting, opinion, and disinformation;

(9) in addition to working to strengthen the North Atlantic Treaty Organization and the European Union, the United States should work with the individual countries of Europe and Eurasia—

(A) to identify vulnerabilities to aggression, disinformation, corruption, and so-called hybrid warfare by the Government of the Russian Federation;

(B) to establish strategic and technical plans for addressing those vulnerabilities;

(C) to ensure that the financial systems of those countries are not being used to shield illicit financial activity by officials of the Government of the Russian Federation or individuals in President Vladimir Putin’s inner circle who have been enriched through corruption;

(D) to investigate and prosecute cases of corruption by Russian actors; and

(E) to work toward full compliance with the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (commonly referred to as the “Anti-Bribery Convention”) of the Organization for Economic Co-operation and Development; and

(10) the President of the United States should use the authority of the President to impose sanctions under—

(A) the Sergei Magnitsky Rule of Law Accountability Act of 2012 (title IV of Public Law 112–208; 22 U.S.C. 5811 note); and

(B) the Global Magnitsky Human Rights Accountability Act (subtitle F of title XII of Public Law 114–328; 22 U.S.C. 2656 note).

SEC. 253. STATEMENT OF POLICY.

The United States, consistent with the principle of ex injuria jus non oritur, supports the policy known as the “Stimson Doctrine” and thus does not recognize territorial changes effected by force, including the illegal invasions and occupations of Abkhazia, South Ossetia, Crimea, Eastern Ukraine, and Transnistria.
SEC. 254. COORDINATING AID AND ASSISTANCE ACROSS EUROPE AND EURASIA.

(a) Authorization of Appropriations.—There are authorized to be appropriated for the Countering Russian Influence Fund $250,000,000 for fiscal years 2018 and 2019.

(b) Use of Funds.—Amounts in the Countering Russian Influence Fund shall be used to effectively implement, prioritized in the following order and subject to the availability of funds, the following goals:

(1) To assist in protecting critical infrastructure and electoral mechanisms from cyberattacks in the following countries:
   (A) Countries that are members of the North Atlantic Treaty Organization or the European Union that the Secretary of State determines—
      (i) are vulnerable to influence by the Russian Federation; and
      (ii) lack the economic capability to effectively respond to aggression by the Russian Federation without the support of the United States.
   (B) Countries that are participating in the enlargement process of the North Atlantic Treaty Organization or the European Union, including Albania, Bosnia and Herzegovina, Georgia, Macedonia, Moldova, Kosovo, Serbia, and Ukraine.

(2) To combat corruption, improve the rule of law, and otherwise strengthen independent judiciaries and prosecutors general offices in the countries described in paragraph (1).

(3) To respond to the humanitarian crises and instability caused or aggravated by the invasions and occupations of Georgia and Ukraine by the Russian Federation.

(4) To improve participatory legislative processes and legal education, political transparency and competition, and compliance with international obligations in the countries described in paragraph (1).

(5) To build the capacity of civil society, media, and other nongovernmental organizations countering the influence and propaganda of the Russian Federation to combat corruption, prioritize access to truthful information, and operate freely in all regions in the countries described in paragraph (1).

(6) To assist the Secretary of State in executing the functions specified in section 1287(b) of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 22 U.S.C. 2656 note) for the purposes of recognizing, understanding, exposing, and countering propaganda and disinformation efforts by foreign governments, in coordination with the relevant regional Assistant Secretary or Assistant Secretaries of the Department of State.

(c) Revision of Activities for Which Amounts May Be Used.—The Secretary of State may modify the goals described in subsection (b) if, not later than 15 days before revising such a goal, the Secretary notifies the appropriate congressional committees of the revision.

(d) Implementation.—

(1) In General.—The Secretary of State shall, acting through the Coordinator of United States Assistance to Europe and Eurasia (authorized pursuant to section 601 of the Support for East European Democracy (SEED) Act of 1989 (22 U.S.C. 2452 note))...
H. R. 3364—44

5461) and section 102 of the Freedom for Russia and Emerging Eurasian Democracies and Open Markets Support Act of 1992 (22 U.S.C. 5812)), and in consultation with the Administrator for the United States Agency for International Development, the Director of the Global Engagement Center of the Department of State, the Secretary of Defense, the Chairman of the Broadcasting Board of Governors, and the heads of other relevant Federal agencies, coordinate and carry out activities to achieve the goals described in subsection (b).

(2) Method.—Activities to achieve the goals described in subsection (b) shall be carried out through—

(A) initiatives of the United States Government;

(B) Federal grant programs such as the Information Access Fund; or

(C) nongovernmental or international organizations, such as the Organization for Security and Co-operation in Europe, the National Endowment for Democracy, the Black Sea Trust, the Balkan Trust for Democracy, the Prague Civil Society Centre, the North Atlantic Treaty Organization Strategic Communications Centre of Excellence, the European Endowment for Democracy, and related organizations.

(3) Report on Implementation.—

(A) In general.—Not later than April 1 of each year, the Secretary of State, acting through the Coordinator of United States Assistance to Europe and Eurasia, shall submit to the appropriate congressional committees a report on the programs and activities carried out to achieve the goals described in subsection (b) during the preceding fiscal year.

(B) Elements.—Each report required by subparagraph (A) shall include, with respect to each program or activity described in that subparagraph—

(i) the amount of funding for the program or activity;

(ii) the goal described in subsection (b) to which the program or activity relates; and

(iii) an assessment of whether or not the goal was met.

(e) Coordination with Global Partners.—

(1) In General.—In order to maximize cost efficiency, eliminate duplication, and speed the achievement of the goals described in subsection (b), the Secretary of State shall ensure coordination with—

(A) the European Union and its institutions;

(B) the governments of countries that are members of the North Atlantic Treaty Organization or the European Union; and

(C) international organizations and quasi-governmental funding entities that carry out programs and activities that seek to accomplish the goals described in subsection (b).

(2) Report by Secretary of State.—Not later than April 1 of each year, the Secretary of State shall submit to the appropriate congressional committees a report that includes—

(A) the amount of funding provided to each country referred to in subsection (b) by—
(i) the European Union or its institutions;  
(ii) the government of each country that is a member of the European Union or the North Atlantic  
Treaty Organization; and  
(iii) international organizations and quasi-governmental funding entities that carry out programs and  
activities that seek to accomplish the goals described in subsection (b); and  
(B) an assessment of whether the funding described in subparagraph (A) is commensurate with funding pro-  
vided by the United States for those goals.  

(f) RULE OF CONSTRUCTION.—Nothing in this section shall be  
construed to apply to or limit United States foreign assistance not provided using amounts available in the Countering Russian Influence Fund.  

(g) ENSURING ADEQUATE STAFFING FOR GOVERNANCE ACTIVI-  
ties.—In order to ensure that the United States Government is properly focused on combating corruption, improving rule of law, and building the capacity of civil society, media, and other non-governmental organizations in countries described in subsection (b)(1), the Secretary of State shall establish a pilot program for Foreign Service officer positions focused on governance and anticorruption activities in such countries.

SEC. 255. REPORT ON MEDIA ORGANIZATIONS CONTROLLED AND FUNDED BY THE GOVERNMENT OF THE RUSSIAN FEDERA-  
TION.

(a) IN GENERAL.—Not later than 90 days after the date of  
the enactment of this Act, and annually thereafter, the President shall submit to the appropriate congressional committees a report that includes a description of media organizations that are con-  
trolled and funded by the Government of the Russian Federation, and any affiliated entities, whether operating within or outside the Russian Federation, including broadcast and satellite-based television, radio, Internet, and print media organizations.

(b) FORM OF REPORT.—The report required by subsection (a)  
shall be submitted in unclassified form but may include a classified annex.

SEC. 256. REPORT ON RUSSIAN FEDERATION INFLUENCE ON ELEC-  
TIONS IN EUROPE AND EURASIA.

(a) IN GENERAL.—Not later than 90 days after the date of  
the enactment of this Act, and annually thereafter, the President shall submit to the appropriate congressional committees and leadership a report on funds provided by, or funds the use of which was directed by, the Government of the Russian Federation or any Russian person with the intention of influencing the outcome of any election or campaign in any country in Europe or Eurasia during the preceding year, including through direct support to any political party, candidate, lobbying campaign, nongovernmental organization, or civic organization.

(b) FORM OF REPORT.—Each report required by subsection (a)  
shall be submitted in unclassified form but may include a classified annex.

(c) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES AND LEADER-  
SHIP.—The term “appropriate congressional committees and leadership” means—
H. R. 3364—46

(A) the Committee on Foreign Relations, the Committee on Banking, Housing, and Urban Affairs, the Committee on Armed Services, the Committee on Homeland Security and Governmental Affairs, the Committee on Appropriations, the Select Committee on Intelligence, and the majority and minority leaders of the Senate; and

(B) the Committee on Foreign Affairs, the Committee on Financial Services, the Committee on Armed Services, the Committee on Homeland Security, the Committee on Appropriations, the Permanent Select Committee on Intelligence, and the Speaker, the majority leader, and the minority leader of the House of Representatives.

(2) RUSSIAN PERSON.—The term “Russian person” means—

(A) an individual who is a citizen or national of the Russian Federation; or

(B) an entity organized under the laws of the Russian Federation or otherwise subject to the jurisdiction of the Government of the Russian Federation.

SEC. 257. UKRAINIAN ENERGY SECURITY.

(a) STATEMENT OF POLICY.—It is the policy of the United States—

(1) to support the Government of Ukraine in restoring its sovereign and territorial integrity;

(2) to condemn and oppose all of the destabilizing efforts by the Government of the Russian Federation in Ukraine in violation of its obligations and international commitments;

(3) to never recognize the illegal annexation of Crimea by the Government of the Russian Federation or the separation of any portion of Ukrainian territory through the use of military force;

(4) to deter the Government of the Russian Federation from further destabilizing and invading Ukraine and other independent countries in Central and Eastern Europe and the Caucasus;

(5) to assist in promoting reform in regulatory oversight and operations in Ukraine’s energy sector, including the establishment and empowerment of an independent regulatory organization;

(6) to encourage and support fair competition, market liberalization, and reliability in Ukraine’s energy sector;

(7) to help Ukraine and United States allies and partners in Europe reduce their dependence on Russian energy resources, especially natural gas, which the Government of the Russian Federation uses as a weapon to coerce, intimidate, and influence other countries;

(8) to work with European Union member states and European Union institutions to promote energy security through developing diversified and liberalized energy markets that provide diversified sources, suppliers, and routes;

(9) to continue to oppose the NordStream 2 pipeline given its detrimental impacts on the European Union’s energy security, gas market development in Central and Eastern Europe, and energy reforms in Ukraine; and

(10) that the United States Government should prioritize the export of United States energy resources in order to create...
American jobs, help United States allies and partners, and strengthen United States foreign policy.

(b) PLAN TO PROMOTE ENERGY SECURITY IN UKRAINE.—

(1) IN GENERAL.—The Secretary of State, in coordination with the Administrator of the United States Agency for International Development and the Secretary of Energy, shall work with the Government of Ukraine to develop a plan to increase energy security in Ukraine, increase the amount of energy produced in Ukraine, and reduce Ukraine’s reliance on energy imports from the Russian Federation.

(2) ELEMENTS.—The plan developed under paragraph (1) shall include strategies for market liberalization, effective regulation and oversight, supply diversification, energy reliability, and energy efficiency, such as through supporting—

(A) the promotion of advanced technology and modern operating practices in Ukraine’s oil and gas sector;

(B) modern geophysical and meteorological survey work as needed followed by international tenders to help attract qualified investment into exploration and development of areas with untapped resources in Ukraine;

(C) a broadening of Ukraine’s electric power transmission interconnection with Europe;

(D) the strengthening of Ukraine’s capability to maintain electric power grid stability and reliability;

(E) independent regulatory oversight and operations of Ukraine’s gas market and electricity sector;

(F) the implementation of primary gas law including pricing, tariff structure, and legal regulatory implementation;

(G) privatization of government owned energy companies through credible legal frameworks and a transparent process compliant with international best practices;

(H) procurement and transport of emergency fuel supplies, including reverse pipeline flows from Europe;

(I) provision of technical assistance for crisis planning, crisis response, and public outreach;

(J) repair of infrastructure to enable the transport of fuel supplies;

(K) repair of power generating or power transmission equipment or facilities; and

(L) improved building energy efficiency and other measures designed to reduce energy demand in Ukraine.

(3) REPORTS.—

(A) IMPLEMENTATION OF UKRAINE FREEDOM SUPPORT ACT OF 2014 PROVISIONS.—Not later than 180 days after the date of the enactment of this Act, the Secretary of State shall submit to the appropriate congressional committees a report detailing the status of implementing the provisions required under section 7(c) of the Ukraine Freedom Support Act of 2014 (22 U.S.C. 8926(c)), including detailing the plans required under that section, the level of funding that has been allocated to and expended for the strategies set forth under that section, and progress that has been made in implementing the strategies developed pursuant to that section.

(B) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and every 180 days
thereafter, the Secretary of State shall submit to the appropriate congressional committees a report detailing the plan developed under paragraph (1), the level of funding that has been allocated to and expended for the strategies set forth in paragraph (2), and progress that has been made in implementing the strategies.

(C) BRIEINGS.—The Secretary of State, or a designee of the Secretary, shall brief the appropriate congressional committees not later than 30 days after the submission of each report under subparagraph (B). In addition, the Department of State shall make relevant officials available upon request to brief the appropriate congressional committees on all available information that relates directly or indirectly to Ukraine or energy security in Eastern Europe.

(D) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this paragraph, the term "appropriate congressional committees" means—

(i) the Committee on Foreign Relations and the Committee on Appropriations of the Senate; and

(ii) the Committee on Foreign Affairs and the Committee on Appropriations of the House of Representatives.

(c) SUPPORTING EFFORTS OF COUNTRIES IN EUROPE AND EURASIA TO DECREASE THEIR DEPENDENCE ON RUSSIAN SOURCES OF ENERGY.—

(1) FINDINGS.—Congress makes the following findings:

(A) The Government of the Russian Federation uses its strong position in the energy sector as leverage to manipulate the internal politics and foreign relations of the countries of Europe and Eurasia.

(B) This influence is based not only on the Russian Federation’s oil and natural gas resources, but also on its state-owned nuclear power and electricity companies.

(2) SENSE OF CONGRESS.—It is the sense of Congress that—

(A) the United States should assist the efforts of the countries of Europe and Eurasia to enhance their energy security through diversification of energy supplies in order to lessen dependencies on Russian Federation energy resources and state-owned entities; and

(B) the Export-Import Bank of the United States and the Overseas Private Investment Corporation should play key roles in supporting critical energy projects that contribute to that goal.

(3) USE OF COUNTERING RUSSIAN INFLUENCE FUND TO PROVIDE TECHNICAL ASSISTANCE.—Amounts in the Countering Russian Influence Fund pursuant to section 254 shall be used to provide technical advice to countries described in subsection (b)(1) of such section designed to enhance energy security and lessen dependence on energy from Russian Federation sources.

(d) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated for the Department of State a total of $30,000,000 for fiscal years 2018 and 2019 to carry out the strategies set forth in subsection (b)(2) and other activities under this section related to the promotion of energy security in Ukraine.

(e) RULE OF CONSTRUCTION.—Nothing in this section shall be construed as affecting the responsibilities required and authorities

SEC. 258. TERMINATION.

The provisions of this subtitle shall terminate on the date that is 5 years after the date of the enactment of this Act.

SEC. 259. APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.

Except as otherwise provided, in this subtitle, the term “appropriate congressional committees” means—

(1) the Committee on Foreign Relations, the Committee on Banking, Housing, and Urban Affairs, the Committee on Armed Services, the Committee on Homeland Security and Governmental Affairs, the Committee on Appropriations, and the Select Committee on Intelligence of the Senate; and

(2) the Committee on Foreign Affairs, the Committee on Financial Services, the Committee on Armed Services, the Committee on Homeland Security, the Committee on Appropriations, and the Permanent Select Committee on Intelligence of the House of Representatives.

Subtitle C—Combating Terrorism and Illicit Financing

PART 1—NATIONAL STRATEGY FOR COMBATING TERRORIST AND OTHER ILICT FINANCING

SEC. 261. DEVELOPMENT OF NATIONAL STRATEGY.

(a) In General.—The President, acting through the Secretary, shall, in consultation with the Attorney General, the Secretary of State, the Secretary of Homeland Security, the Director of National Intelligence, the Director of the Office of Management and Budget, and the appropriate Federal banking agencies and Federal functional regulators, develop a national strategy for combating the financing of terrorism and related forms of illicit finance.

(b) TRANSMITTAL TO CONGRESS.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the President shall submit to the appropriate congressional committees a comprehensive national strategy developed in accordance with subsection (a).

(2) UPDATES.—Not later than January 31, 2020, and January 31, 2022, the President shall submit to the appropriate congressional committees updated versions of the national strategy submitted under paragraph (1).

(c) SEPARATE PRESENTATION OF CLASSIFIED MATERIAL.—Any part of the national strategy that involves information that is properly classified under criteria established by the President shall be submitted to Congress separately in a classified annex and, if requested by the chairman or ranking member of one of the appropriate congressional committees, as a briefing at an appropriate level of security.

SEC. 262. CONTENTS OF NATIONAL STRATEGY.

The strategy described in section 261 shall contain the following:
(1) EVALUATION OF EXISTING EFFORTS.—An assessment of the effectiveness of and ways in which the United States is currently addressing the highest levels of risk of various forms of illicit finance, including those identified in the documents entitled "2015 National Money Laundering Risk Assessment" and "2015 National Terrorist Financing Risk Assessment", published by the Department of the Treasury and a description of how the strategy is integrated into, and supports, the broader counter terrorism strategy of the United States.

(2) GOALS, OBJECTIVES, AND PRIORITIES.—A comprehensive, research-based, long-range, quantifiable discussion of goals, objectives, and priorities for disrupting and preventing illicit finance activities within and transiting the financial system of the United States that outlines priorities to reduce the incidence, dollar value, and effects of illicit finance.

(3) THREATS.—An identification of the most significant illicit finance threats to the financial system of the United States.

(4) REVIEWS AND PROPOSED CHANGES.—Reviews of enforcement efforts, relevant regulations and relevant provisions of law and, if appropriate, discussions of proposed changes determined to be appropriate to ensure that the United States pursues coordinated and effective efforts at all levels of government, and with international partners of the United States, in the fight against illicit finance.

(5) DETECTION AND PROSECUTION INITIATIVES.—A description of efforts to improve, as necessary, detection and prosecution of illicit finance, including efforts to ensure that—

(A) subject to legal restrictions, all appropriate data collected by the Federal Government that is relevant to the efforts described in this section be available in a timely fashion to—

(i) all appropriate Federal departments and agencies; and

(ii) as appropriate and consistent with section 314 of the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001 (31 U.S.C. 5311 note), to financial institutions to assist the financial institutions in efforts to comply with laws aimed at curbing illicit finance; and

(B) appropriate efforts are undertaken to ensure that Federal departments and agencies charged with reducing and preventing illicit finance make thorough use of publicly available data in furtherance of this effort.

(6) THE ROLE OF THE PRIVATE FINANCIAL SECTOR IN PREVENTION OF ILICIT FINANCE.—A discussion of ways to enhance partnerships between the private financial sector and Federal departments and agencies with regard to the prevention and detection of illicit finance, including—

(A) efforts to facilitate compliance with laws aimed at stopping such illicit finance while maintaining the effectiveness of such efforts; and

(B) providing guidance to strengthen internal controls and to adopt on an industry-wide basis more effective policies.
(7) **Enhancement of Intergovernmental Cooperation.**—A discussion of ways to combat illicit finance by enhancing—

(A) cooperative efforts between and among Federal, State, and local officials, including State regulators, State and local prosecutors, and other law enforcement officials; and

(B) cooperative efforts with and between governments of countries and with and between multinational institutions with expertise in fighting illicit finance, including the Financial Action Task Force and the Egmont Group of Financial Intelligence Units.

(8) **Trend Analysis of Emerging Illicit Finance Threats.**—A discussion of and data regarding trends in illicit finance, including evolving forms of value transfer such as so-called cryptocurrencies, other methods that are computer, telecommunications, or Internet-based, cyber crime, or any other threats that the Secretary may choose to identify.

(9) **Budget Priorities.**—A multiyear budget plan that identifies sufficient resources needed to successfully execute the full range of missions called for in this section.

(10) **Technology Enhancements.**—An analysis of current and developing ways to leverage technology to improve the effectiveness of efforts to stop the financing of terrorism and other forms of illicit finance, including better integration of open-source data.

**PART 2—ENHANCING ANTITERRORISM TOOLS OF THE DEPARTMENT OF THE TREASURY**

**SEC. 271. IMPROVING ANTITERROR FINANCE MONITORING OF FUNDS TRANSFERS.**

(a) **Study.**—

(1) **In General.**—To improve the ability of the Department of the Treasury to better track cross-border fund transfers and identify potential financing of terrorist or other forms of illicit finance, the Secretary shall carry out a study to assess—

(A) the potential efficacy of requiring banking regulators to establish a pilot program to provide technical assistance to depository institutions and credit unions that wish to provide account services to money services businesses serving individuals in Somalia;

(B) whether such a pilot program could be a model for improving the ability of United States persons to make legitimate funds transfers through transparent and easily monitored channels while preserving strict compliance with the Bank Secrecy Act (Public Law 91–508; 84 Stat. 1114) and related controls aimed at stopping money laundering and the financing of terrorism; and

(C) consistent with current legal requirements regarding confidential supervisory information, the potential impact of allowing money services businesses to share certain State examination information with depository institutions and credit unions, or whether another appropriate mechanism could be identified to allow a similar exchange of information to give the depository institutions
and credit unions a better understanding of whether an individual money services business is adequately meeting its anti-money laundering and counter-terror financing obligations to combat money laundering, the financing of terror, or related illicit finance.

(2) PUBLIC INPUT.—The Secretary should solicit and consider public input as appropriate in developing the study required under subsection (a).

(b) REPORT.—Not later than 270 days after the date of the enactment of this Act, the Secretary shall submit to the Committee on Banking, Housing, and Urban Affairs and the Committee on Foreign Relations of the Senate and the Committee on Financial Services and the Committee on Foreign Affairs of the House of Representatives a report that contains all findings and determinations made in carrying out the study required under subsection (a).

SEC. 272. SENSE OF CONGRESS ON INTERNATIONAL COOPERATION REGARDING TERRORIST FINANCING INTELLIGENCE.

It is the sense of Congress that the Secretary, acting through the Under Secretary for Terrorism and Financial Crimes, should intensify work with foreign partners to help the foreign partners develop intelligence analytic capacities, in a financial intelligence unit, finance ministry, or other appropriate agency, that are—

(1) commensurate to the threats faced by the foreign partner; and

(2) designed to better integrate intelligence efforts with the anti-money laundering and counter-terrorist financing regimes of the foreign partner.


Not later than 180 days after the date of the enactment of this Act, the Secretary shall submit to the Committee on Banking, Housing, and Urban Affairs and the Committee on Foreign Relations of the Senate and the Committee on Financial Services and the Committee on Foreign Affairs of the House of Representatives a report that contains—

(1) a list of the United States embassies in which a full-time Department of the Treasury financial attache is stationed and a description of how the interests of the Department of the Treasury relating to terrorist financing and money laundering are addressed (via regional attaches or otherwise) at United States embassies where no such attaches are present;

(2) a list of the United States embassies at which the Department of the Treasury has assigned a technical assistance advisor from the Office of Technical Assistance of the Department of the Treasury;

(3) an overview of how Department of the Treasury financial attaches and technical assistance advisors assist in efforts to counter illicit finance, to include money laundering, terrorist financing, and proliferation financing; and

(4) an overview of patterns, trends, or other issues identified by the Department of the Treasury and whether resources are sufficient to address these issues.
SEC. 274. INCLUSION OF SECRETARY OF THE TREASURY ON THE NATIONAL SECURITY COUNCIL.

(a) In General.—Section 101(c)(1) of the National Security Act of 1947 (50 U.S.C. 3021(c)(1)) is amended by inserting "the Secretary of the Treasury," before "and such other officers".

(b) Rule of Construction.—The amendment made by subsection (a) may not be construed to authorize the National Security Council to have a professional staff level that exceeds the limitation set forth under section 101(e)(3) of the National Security Act of 1947 (50 U.S.C. 3021(e)(3)).

SEC. 275. INCLUSION OF ALL FUNDS.

(a) In General.—Section 5326 of title 31, United States Code, is amended—

(1) in the heading of such section, by striking "coin and currency";

(2) in subsection (a)—

(A) by striking "subtitle and" and inserting "subtitle or to"; and

(B) in paragraph (1)(A), by striking "United States coins or currency (or such other monetary instruments as the Secretary may describe in such order)" and inserting "funds (as the Secretary may describe in such order)";

and

(3) in subsection (b)—

(A) in paragraph (1)(A), by striking "coins or currency (or monetary instruments)" and inserting "funds"; and

(B) in paragraph (2), by striking "coins or currency (or such other monetary instruments as the Secretary may describe in the regulation or order)" and inserting "funds (as the Secretary may describe in the regulation or order)".

(b) Clerical Amendment.—The table of contents for chapter 53 of title 31, United States Code, is amended in the item relating to section 5326 by striking "coin and currency".

PART 3—DEFINITIONS

SEC. 281. DEFINITIONS.

In this subtitle—

(1) the term "appropriate congressional committees" means—

(A) the Committee on Banking, Housing, and Urban Affairs, the Committee on Foreign Relations, Committee on Armed Services, Committee on the Judiciary, Committee on Homeland Security and Governmental Affairs, and the Select Committee on Intelligence of the Senate; and

(B) the Committee on Financial Services, the Committee on Foreign Affairs, the Committee on Armed Services, the Committee on the Judiciary, Committee on Homeland Security, and the Permanent Select Committee on Intelligence of the House of Representatives;

(2) the term "appropriate Federal banking agencies" has the meaning given the term in section 3 of the Federal Deposit Insurance Act (12 U.S.C. 1813);

(3) the term "Bank Secrecy Act" means—

(A) section 21 of the Federal Deposit Insurance Act (12 U.S.C. 1829b);

(4) the term "Board of Governors of the Federal Reserve System" means—

(A) the Board of Governors of the Federal Reserve System; and

(B) the Director of the Federal Reserve Bank of New York;
the term "Federal functional regulator" has the meaning given that term in section 509 of the
Gramm-Leach-Bliley Act (15 U.S.C. 6809);
(5) the term "illicit finance" means the financing of terror-
ism, narcotics trafficking, or proliferation, money laundering,
or other forms of illicit financing domestically or internationally,
as defined by the President;
(6) the term "money services business" has the meaning
given the term under section 1010.100 of title 31, Code of
Federal Regulations;
(7) the term "Secretary" means the Secretary of the
Treasury; and
(8) the term "State" means each of the several States,
the District of Columbia, and each territory or possession of
the United States.

Subtitle D—Rule of Construction

SEC. 291. RULE OF CONSTRUCTION.

Nothing in this title or the amendments made by this title
(other than sections 216 and 236(b)) shall be construed to limit
the authority of the President under the International Emergency

SEC. 292. SENSE OF CONGRESS ON THE STRATEGIC IMPORTANCE OF
ARTICLE 5 OF THE NORTH ATLANTIC TREATY.

(a) FINDINGS.—Congress makes the following findings:
(1) The principle of collective defense of the North Atlantic
Treaty Organization (NATO) is immortalized in Article 5 of
the North Atlantic Treaty in which members pledge that "an
armed attack against one or more of them in Europe or North
America shall be considered an attack against them all".
(2) For almost 7 decades, the principle of collective defense
has effectively served as a strategic deterrent for the member
nations of the North Atlantic Treaty Organization and provided
stability throughout the world, strengthening the security of
the United States and all 28 other member nations.
(3) Following the September 11, 2001, terrorist attacks
in New York, Washington, and Pennsylvania, the Alliance
agreed to invoke Article 5 for the first time, affirming its
commitment to collective defense.
(4) Countries that are members of the North Atlantic
Treaty Organization have made historic contributions and sac-
crifices while combating terrorism in Afghanistan through the
International Security Assistance Force and the Resolute Sup-
port Mission.
(5) The recent attacks in the United Kingdom underscore
the importance of an international alliance to combat hostile
nation states and terrorist groups.
(6) At the 2014 NATO summit in Wales, the member
countries of the North Atlantic Treaty Organization decided
that all countries that are members of NATO would spend
an amount equal to 2 percent of their gross domestic product on defense by 2024.

(7) Collective defense unites the 29 members of the North Atlantic Treaty Organization, each committing to protecting and supporting one another from external adversaries, which bolsters the North Atlantic Alliance.

(b) SENSE OF CONGRESS.—It is the sense of Congress—

(1) to express the vital importance of Article 5 of the North Atlantic Treaty, the charter of the North Atlantic Treaty Organization, as it continues to serve as a critical deterrent to potential hostile nations and terrorist organizations;

(2) to remember the first and only invocation of Article 5 by the North Atlantic Treaty Organization in support of the United States after the terrorist attacks of September 11, 2001;

(3) to affirm that the United States remains fully committed to the North Atlantic Treaty Organization and will honor its obligations enshrined in Article 5; and

(4) to condemn any threat to the sovereignty, territorial integrity, freedom, or democracy of any country that is a member of the North Atlantic Treaty Organization.

TITLE III—SANCTIONS WITH RESPECT TO NORTH KOREA

SEC. 301. SHORT TITLE.

This title may be cited as the “Korean Interdiction and Modernization of Sanctions Act”.

SEC. 302. DEFINITIONS.

(a) AMENDMENTS TO DEFINITIONS IN THE NORTH KOREA SANCTIONS AND POLICY ENHANCEMENT ACT OF 2016.—

(1) APPLICABLE EXECUTIVE ORDER.—Section 3(1)(A) of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9202(1)(A)) is amended—

(A) by striking “or Executive Order 13694” and inserting “Executive Order No. 13694”;

(B) by inserting “or Executive Order No. 13722 (50 U.S.C. 1701 note; relating to blocking the property of the Government of North Korea and the Workers’ Party of Korea, and Prohibiting Certain Transactions With Respect to North Korea),” before “to the extent”.


(3) FOREIGN PERSON.—Section 3 of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9202) is amended—

(A) by redesignating paragraphs (5) through (14) as paragraphs (6) through (15), respectively; and

(B) by inserting after paragraph (4) the following new paragraph:

“(5) FOREIGN PERSON.—The term ‘foreign person’ means—
“(A) an individual who is not a United States citizen or an alien lawfully admitted for permanent residence to the United States; or

“(B) an entity that is not a United States person.”.

(4) LUXURY GOODS.—Paragraph (9) of section 3 of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9202), as redesignated by paragraph (3) of this subsection, is amended—

(A) in subparagraph (A), by striking “and” at the end; and

(B) in subparagraph (B), by striking the period at the end and inserting “; and”;

and—

(C) by adding at the end the following new subparagraph:

“(C) also includes any items so designated under an applicable United Nations Security Council resolution.”.

(5) NORTH KOREAN PERSON.—Section 3 of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9202), as amended by paragraph (3) of this subsection, is further amended—

(A) by redesignating paragraphs (13) through (15) as paragraphs (14) through (16), respectively; and

(B) by inserting after paragraph (12) the following new paragraph:

“(13) NORTH KOREAN PERSON.—The term ‘North Korean person’ means—

“(A) a North Korean citizen or national; or

“(B) an entity owned or controlled by the Government of North Korea or by a North Korean citizen or national.”.

(b) DEFINITIONS FOR PURPOSES OF THIS ACT.—In this title:

(1) APPLICABLE UNITED NATIONS SECURITY COUNCIL RESOLUTION; LUXURY GOODS.—The terms “applicable United Nations Security Council resolution” and “luxury goods” have the meanings given those terms, respectively, in section 3 of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9202), as amended by subsection (a).

(2) APPROPRIATE CONGRESSIONAL COMMITTEES; GOVERNMENT OF NORTH KOREA; UNITED STATES PERSON.—The terms “appropriate congressional committees”, “Government of North Korea”, and “United States person” have the meanings given those terms, respectively, in section 3 of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9202).

(3) FOREIGN PERSON; NORTH KOREAN PERSON.—The terms “foreign person” and “North Korean person” have the meanings given those terms, respectively, in paragraph (5) and paragraph (13) of section 3 of the North Korea Sanctions and Policy Enforcement Act of 2016 (22 U.S.C. 9202(5) and 9202(13)), as added by subsection (a).

(4) PROHIBITED WEAPONS PROGRAM.—The term “prohibited weapons program” means—

(A) any program related to the development of nuclear, chemical, or biological weapons, and their means of delivery, including ballistic missiles; and

(B) any program to develop related materials with respect to a program described in subparagraph (A).
Subtitle A—Sanctions to Enforce and Implement United Nations Security Council Sanctions Against North Korea

SEC. 311. MODIFICATION AND EXPANSION OF REQUIREMENTS FOR THE DESIGNATION OF PERSONS.

(a) EXPANSION OF MANDATORY DESIGNATIONS.—Section 104(a) of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9214(a)) is amended—

(1) in paragraph (9), by striking “; or” and inserting “or any defense article or defense service (as such terms are defined in section 47 of the Arms Export Control Act (22 U.S.C. 2794));”;

(2) by redesignating paragraph (10) as paragraph (15);

(3) by inserting after paragraph (9) the following new paragraphs:

"(10) knowingly, directly or indirectly, purchases or otherwise acquires from North Korea any significant amounts of gold, titanium ore, vanadium ore, copper, silver, nickel, zinc, or rare earth minerals;

"(11) knowingly, directly or indirectly, sells or transfers to North Korea any significant amounts of rocket, aviation, or jet fuel (except for use by a civilian passenger aircraft outside North Korea, exclusively for consumption during its flight to North Korea or its return flight);

"(12) knowingly, directly or indirectly, provides significant amounts of fuel or supplies, provides bunkering services, or facilitates a significant transaction or transactions to operate or maintain, a vessel or aircraft that is designated under an applicable Executive order or an applicable United Nations Security Council resolution, or that is owned or controlled by a person designated under an applicable Executive order or applicable United Nations Security Council resolution;

"(13) knowingly, directly or indirectly, insures, registers, facilitates the registration of, or maintains insurance or a registration for, a vessel owned or controlled by the Government of North Korea, except as specifically approved by the United Nations Security Council;

"(14) knowingly, directly or indirectly, maintains a correspondent account (as defined in section 201Ad(x1)) with any North Korean financial institution, except as specifically approved by the United Nations Security Council; or; and

(4) in paragraph (15), as so redesignated, by striking “(9)” and inserting “(14)".

(b) EXPANSION OF ADDITIONAL DISCRETIONARY DESIGNATIONS.—

(1) IN GENERAL.—Section 104(b)(1) of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9214(b)(1)) is amended—

(A) in subparagraph (A), by striking “pursuant to an applicable United Nations Security Council resolution;” and inserting the following: “pursuant to—

"(i) an applicable United Nations Security Council resolution;

"(ii) any regulation promulgated under section 404; or

"(iii) any applicable Executive order;";
(B) in subparagraph (B)(iii), by striking "or" at the end;
(C) in subparagraph (C), by striking the period at the end and inserting a semicolon; and
(D) by adding at the end the following new subparagraphs:

"(D) knowingly, directly or indirectly, purchased or otherwise acquired from the Government of North Korea significant quantities of coal, iron, or iron ore, in excess of the limitations provided in applicable United Nations Security Council resolutions;

"(E) knowingly, directly or indirectly, purchased or otherwise acquired significant types or amounts of textiles from the Government of North Korea;

"(F) knowingly facilitated a significant transfer of funds or property of the Government of North Korea that materially contributes to any violation of an applicable United National Security Council resolution;

"(G) knowingly, directly or indirectly, facilitated a significant transfer to or from the Government of North Korea of bulk cash, precious metals, gemstones, or other stores of value not described under subsection (a)(10);

"(H) knowingly, directly or indirectly, sold, transferred, or otherwise provided significant amounts of crude oil, condensates, refined petroleum, other types of petroleum or petroleum byproducts, liquified natural gas, or other natural gas resources to the Government of North Korea (except for heavy fuel oil, gasoline, or diesel fuel for humanitarian use or as excepted under subsection (a)(11));

"(I) knowingly, directly or indirectly, engaged in, facilitated, or was responsible for the online commercial activities of the Government of North Korea, including online gambling;

"(J) knowingly, directly or indirectly, purchased or otherwise acquired fishing rights from the Government of North Korea;

"(K) knowingly, directly or indirectly, purchased or otherwise acquired significant types or amounts of food or agricultural products from the Government of North Korea;

"(L) knowingly, directly or indirectly, engaged in, facilitated, or was responsible for the exportation of workers from North Korea in a manner intended to generate significant revenue, directly or indirectly, for use by the Government of North Korea or by the Workers' Party of Korea;

"(M) knowingly conducted a significant transaction or transactions in North Korea's transportation, mining, energy, or financial services industries; or

"(N) except as specifically approved by the United Nations Security Council, and other than through a correspondent account as described in subsection (a)(14), knowingly facilitated the operation of any branch, subsidiary, or office of a North Korean financial institution.".

(2) EFFECTIVE DATE.—The amendments made by paragraph (1) take effect on the date of the enactment of this Act and apply with respect to conduct described in subparagraphs (D) through (N) of section 104(b)(1) of the North Korea Sanctions
H. R. 3364—59

and Policy Enhancement Act of 2016, as added by paragraph (1), engaged in on or after such date of enactment.

(c) MANDATORY AND DISCRETIONARY ASSET BLOCKING.—Section 104(c) of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9214(c)) is amended—

(1) by striking “of a designated person” and inserting “of a person designated under subsection (a)”;

(2) by striking “The President” and inserting the following: “(1) MANDATORY ASSET BLOCKING.—The President”; and

(3) by adding at the end the following new paragraph: “(2) DISCRETIONARY ASSET BLOCKING.—The President may also exercise such powers, in the same manner and to the same extent described in paragraph (1), with respect to a person designated under subsection (b).”

(d) DESIGNATION OF ADDITIONAL PERSONS.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the President shall submit to the appropriate congressional committees a report including a determination as to whether reasonable grounds exist, and an explanation of the reasons for any determination that such grounds do not exist, to designate, pursuant to section 104 of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9214), as amended by this section, each of the following:

(A) The Korea Shipowners' Protection and Indemnity Association, a North Korean insurance company, with respect to facilitating imports, exports, and reexports of arms and related materiel to and from North Korea, or for other activities prohibited by such section 104.

(B) Chinpo Shipping Company (Private) Limited, a Singapore corporation, with respect to facilitating imports, exports, and reexports of arms and related materiel to and from North Korea.

(C) The Central Bank of the Democratic People's Republic of Korea, with respect to the sale of gold to, the receipt of gold from, or the import or export of gold by the Government of North Korea.

(D) Kumgang Economic Development Corporation (KKG), with respect to being an entity controlled by Bureau 39 of the Workers' Party of the Government of North Korea.

(E) Sam Pa, also known as Xu Jinghua, Xu Songhua, Sa Muxu, Samo, Sampa, or Sam King, and any entities owned or controlled by such individual, with respect to transactions with KKG.

(F) The Chamber of Commerce of the Democratic People's Republic of Korea, with respect to the exportation of workers in violation of section 104(a)(5) or of section 104(b)(1)(M) of such Act, as amended by subsection (b) of this section.

(2) FORM.—The report submitted under paragraph (1) may contain a classified annex.

SEC. 312. PROHIBITION ON INDIRECT CORRESPONDENT ACCOUNTS.

(a) IN GENERAL.—Title II of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9221 et seq.) is amended by inserting after section 201 the following new section:
SEC. 201A. PROHIBITION ON INDIRECT CORRESPONDENT ACCOUNTS.

(a) In General.—Except as provided in subsection (b), if a United States financial institution has or obtains knowledge that a correspondent account established, maintained, administered, or managed by that institution for a foreign financial institution is being used by the foreign financial institution to provide significant financial services indirectly to any person, foreign government, or financial institution designated under section 104, the United States financial institution shall ensure that such correspondent account is no longer used to provide such services.

(b) Exception.—A United States financial institution is authorized to process transfers of funds to or from North Korea, or for the direct or indirect benefit of any person, foreign government, or financial institution that is designated under section 104, only if the transfer—

(1) arises from, and is ordinarily incident and necessary to give effect to, an underlying transaction that has been authorized by a specific or general license issued by the Secretary of the Treasury; and

(2) does not involve debiting or crediting a North Korean account.

(c) Definitions.—In this section:

(1) CORRESPONDENT ACCOUNT.—The term 'correspondent account' has the meaning given that term in section 5318A of title 31, United States Code.

(2) UNITED STATES FINANCIAL INSTITUTION.—The term 'United States financial institution' means has the meaning given that term in section 510.310 of title 31, Code of Federal Regulations, as in effect on the date of the enactment of this section.

(3) FOREIGN FINANCIAL INSTITUTION.—The term 'foreign financial institution' has the meaning given that term in section 1010.605 of title 31, Code of Federal Regulations, as in effect on the date of the enactment of this section.

SEC. 313. LIMITATIONS ON FOREIGN ASSISTANCE TO NONCOMPLIANT GOVERNMENTS.

Section 203 of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9223) is amended—

(1) in subsection (b)—

(A) in the heading, by striking "TRANSACTIONS IN LETHAL MILITARY EQUIPMENT" and inserting "TRANSACTIONS IN DEFENSE ARTICLES OR DEFENSE SERVICES";

(B) in paragraph (1), by striking "that provides lethal military equipment to the Government of North Korea" and inserting "that provides to or receives from the Government of North Korea a defense article or defense service, as such terms are defined in section 47 of the Arms Export Control Act (22 U.S.C. 2794), if the President determines that a significant type or amount of such article or service has been so provided or received"; and
(C) in paragraph (2), by striking “1 year” and inserting “2 years”; 
(2) in subsection (d), by striking “or emergency” and inserting “maternal and child health, disease prevention and response, or”; and 
(3) by adding at the end the following new subsection: 
“(e) REPORT ON ARMS TRAFFICKING INVOLVING NORTH KOREA.—
“(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this subsection, and annually thereafter for 5 years, the Secretary of State shall submit to the appropriate congressional committees a report that specifically describes the compliance of foreign countries and other foreign jurisdictions with the requirement to curtail the trade described in subsection (b)(1).
“(2) FORM.—The report required under paragraph (1) shall be submitted in unclassified form but may contain a classified annex.”

SEC. 314. AMENDMENTS TO ENHANCE INSPECTION AUTHORITIES.

Title II of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9221 et seq.), as amended by section 102 of this Act, is further amended by striking section 205 and inserting the following:

“SEC. 205. ENHANCED INSPECTION AUTHORITIES.

“(a) REPORT REQUIRED.—
“(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this section, and annually thereafter for 5 years, the President shall submit to the appropriate congressional committees a report—
“(A) identifying the operators of foreign sea ports and airports that knowingly—
“(i) significantly fail to implement or enforce regulations to inspect ships, aircraft, cargo, or conveyances in transit to or from North Korea, as required by applicable United Nations Security Council resolutions;
“(ii) facilitate the transfer, transshipment, or conveyance of significant types or quantities of cargo, vessels, or aircraft owned or controlled by persons designated under applicable United Nations Security Council resolutions; or
“(iii) facilitate any of the activities described in section 104(a);
“(B) describing the extent to which the requirements of applicable United Nations Security Council resolutions to de-register any vessel owned, controlled, or operated by or on behalf of the Government of North Korea have been implemented by other foreign countries;
“(C) describing the compliance of the Islamic Republic of Iran with the sanctions mandated in applicable United Nations Security Council resolutions;
“(D) identifying vessels, aircraft, and conveyances owned or controlled by the Reconnaissance General Bureau of the Workers’ Party of Korea; and
“(E) describing the diplomatic and enforcement efforts by the President to secure the full implementation of the applicable United Nations Security Council resolutions, as described in subparagraphs (A) through (C).
"(2) FORM.—The report required under paragraph (1) shall be submitted in unclassified form but may contain a classified annex.

(b) SPECIFIC FINDINGS.—Each report required under subsection (a) shall include specific findings with respect to the following ports and airports:

(1) The ports of Dandong, Dalian, and any other port in the People’s Republic of China that the President deems appropriate.


(3) The ports of Nakhodka, Vanino, and Vladivostok, in the Russian Federation.

(4) The ports of Latakia, Banias, and Tartous, and Damascus International Airport, in the Syrian Arab Republic.

(c) ENHANCED SECURITY TARGETING REQUIREMENTS.—

(1) IN GENERAL.—Except as provided in paragraph (2), the Secretary of Homeland Security may, using a layered approach, require enhanced screening procedures to determine whether physical inspections are warranted of any cargo bound for or landed in the United States that—

(A) has been transported through a sea port or airport the operator of which has been identified by the President in accordance with subsection (a)(1) as having repeatedly failed to comply with applicable United Nations Security Council resolutions;

(B) is aboard a vessel or aircraft, or within a conveyance that has, within the last 365 days, entered the territory or waters of North Korea, or landed in any of the sea ports or airports of North Korea; or

(C) is registered by a country or jurisdiction whose compliance has been identified by the President as deficient pursuant to subsection (a)(2).

(2) EXCEPTION FOR FOOD, MEDICINE, AND HUMANITARIAN SHIPMENTS.—Paragraph (1) shall not apply to any vessel, aircraft, or conveyance that has entered the territory or waters of North Korea, or landed in any of the sea ports or airports of North Korea, exclusively for the purposes described in section 208(b)(3)(B), or to import food, medicine, or supplies into North Korea to meet the humanitarian needs of the North Korean people.

(d) SEIZURE AND FORFEITURE.—A vessel, aircraft, or conveyance used to facilitate any of the activities described in section 104(a) under the jurisdiction of the United States may be seized and forfeited, or subject to forfeiture, under—

(1) chapter 46 of title 18, United States Code; or

(2) part V of title IV of the Tariff Act of 1930 (19 U.S.C. 1581 et seq.)."

SEC. 315. ENFORCING COMPLIANCE WITH UNITED NATIONS SHIPPING SANCTIONS AGAINST NORTH KOREA.

(a) IN GENERAL.—The Ports and Waterways Safety Act (33 U.S.C. 1221 et seq.) is amended by adding at the end the following new section:
SEC. 16. PROHIBITION ON ENTRY AND OPERATION.

(a) Prohibition.—

(1) In general.—Except as otherwise provided in this section, no vessel described in subsection (b) may enter or operate in the navigable waters of the United States or transfer cargo in any port or place under the jurisdiction of the United States.

(2) Limitations on application.—

(A) In general.—The prohibition under paragraph (1) shall not apply with respect to—

(i) a vessel described in subsection (b)(1), if the Secretary of State determines that—

(I) the vessel is owned or operated by or on behalf of a country the government of which the Secretary of State determines is closely cooperating with the United States with respect to implementing the applicable United Nations Security Council resolutions (as such term is defined in section 3 of the North Korea Sanctions and Policy Enhancement Act of 2016); or

(II) it is in the national security interest not to apply the prohibition to such vessel; or

(ii) a vessel described in subsection (b)(2), if the Secretary of State determines that the vessel is no longer registered as described in that subsection.

(B) Notice.—Not later than 15 days after making a determination under subparagraph (A), the Secretary of State shall submit to the Committee on Foreign Affairs and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Foreign Relations and the Committee on Commerce, Science, and Transportation of the Senate written notice of the determination and the basis upon which the determination was made.

(C) Publication.—The Secretary of State shall publish a notice in the Federal Register of each determination made under subparagraph (A).

(b) Vessels described.—A vessel referred to in subsection (a) is a foreign vessel for which a notice of arrival is required to be filed under section 4(a)(5), and that—

(1) is on the most recent list of vessels published in Federal Register under subsection (c)(2); or

(2) more than 180 days after the publication of such list, is knowingly registered, pursuant to the 1958 Convention on the High Seas entered into force on September 30, 1962, by a government the agents or instrumentalities of which are maintaining a registration of a vessel that is included on such list.

(c) Information and publication.—The Secretary of the department in which the Coast Guard is operating, with the concurrence of the Secretary of State, shall—

(1) maintain timely information on the registrations of all foreign vessels over 300 gross tons that are known to be—

(A) owned or operated by or on behalf of the Government of North Korea or a North Korean person;

(B) owned or operated by or on behalf of any country in which a sea port is located, the operator of which the
President has identified in the most recent report submitted under section 205(a)(1)(A) of the North Korea Sanctions and Policy Enhancement Act of 2016; or

"(C) owned or operated by or on behalf of any country identified by the President as a country that has not complied with the applicable United Nations Security Council resolutions (as such term is defined in section 3 of such Act); and

"(2) not later than 180 days after the date of the enactment of this section, and periodically thereafter, publish in the Federal Register a list of the vessels described in paragraph (1).

"(d) NOTIFICATION OF GOVERNMENTS.—

"(1) IN GENERAL.—The Secretary of State shall notify each government, the agents or instrumentalities of which are maintaining a registration of a foreign vessel that is included on a list published under subsection (c)(2), not later than 30 days after such publication, that all vessels registered under such government’s authority are subject to subsection (a).

"(2) ADDITIONAL NOTIFICATION.—In the case of a government that continues to maintain a registration for a vessel that is included on such list after receiving an initial notification under paragraph (1), the Secretary shall issue an additional notification to such government not later than 120 days after the publication of a list under subsection (c)(2).

"(e) NOTIFICATION OF VESSELS.—Upon receiving a notice of arrival under section 4(a)(5) from a vessel described in subsection (b), the Secretary of the department in which the Coast Guard is operating shall notify the master of such vessel that the vessel may not enter or operate in the navigable waters of the United States or transfer cargo in any port or place under the jurisdiction of the United States, unless—

"(1) the Secretary of State has made a determination under subsection (a)(2); or

"(2) the Secretary of the department in which the Coast Guard is operating allows provisional entry of the vessel, or transfer of cargo from the vessel, under subsection (f).

"(f) PROVISIONAL ENTRY OR CARGO TRANSFER.—Notwithstanding any other provision of this section, the Secretary of the department in which the Coast Guard is operating may allow provisional entry of, or transfer of cargo from, a vessel, if such entry or transfer is necessary for the safety of the vessel or persons aboard.

"(g) RIGHT OF INNOCENT PASSAGE AND RIGHT OF TRANSIT PASSAGE.—This section shall not be construed as authority to restrict the right of innocent passage or the right of transit passage as recognized under international law.

"(h) FOREIGN VESSEL DEFINED.—In this section, the term ‘foreign vessel’ has the meaning given that term in section 110 of title 46, United States Code.”.

(b) CONFORMING AMENDMENTS.—

(1) SPECIAL POWERS.—Section 4(b)(2) of the Ports and Waterways Safety Act (33 U.S.C. 1223(b)(2)) is amended by inserting “or 16” after “section 9”.

(2) DENIAL OF ENTRY.—Section 13(e) of the Ports and Waterways Safety Act (33 U.S.C. 1232(e)) is amended by striking “section 9” and inserting “section 9 or 16.”
H. R. 3364—65

SEC. 316. REPORT ON COOPERATION BETWEEN NORTH KOREA AND IRAN.

(a) In general.—Not later than 180 days after the date of the enactment of this Act, and annually thereafter for 5 years, the President shall submit to the appropriate congressional committees and leadership a report that includes—

1. an assessment of the extent of cooperation (including through the transfer of goods, services, technology, or intellectual property) between North Korea and Iran relating to their respective nuclear, ballistic missile development, chemical or biological weapons development, or conventional weapons programs;

2. the names of any Iranian or North Korean persons that have knowingly engaged in or directed—

(A) the provision of material support to such programs; or

(B) the exchange of information between North Korea and Iran with respect to such programs;

3. the names of any other foreign persons that have facilitated the activities described in paragraph (1); and

4. a determination whether any of the activities described in paragraphs (1) and (2) violate United Nations Security Council Resolution 2231 (2015).

(b) Form.—The report required under subsection (a) shall be submitted in unclassified form but may contain a classified annex.

(c) Appropriate congressional committees and leadership defined.—In this section, the term “appropriate congressional committees and leadership” means—

1. the Committee on Foreign Relations, the Committee on Banking, Housing, and Urban Affairs, and the majority and minority leaders of the Senate; and

2. the Committee on Foreign Affairs, the Committee on Financial Services, the Committee on Ways and Means, and the Speaker, the majority leader, and the minority leader of the House of Representatives.

SEC. 317. REPORT ON IMPLEMENTATION OF UNITED NATIONS SECURITY COUNCIL RESOLUTIONS BY OTHER GOVERNMENTS.

(a) In general.—Not later than 180 days after the date of the enactment of this Act, and annually thereafter for 5 years, the President shall submit to the appropriate congressional committees and leadership a report that evaluates the degree to which the governments of other countries have knowingly failed to—

1. close the representative offices of persons designated under applicable United Nations Security Council resolutions;

2. expel any North Korean nationals, including diplomats, working on behalf of such persons;

3. prohibit the opening of new branches, subsidiaries, or representative offices of North Korean financial institutions within the jurisdictions of such governments; or

4. expel any representatives of North Korean financial institutions.

(b) Form.—The report required under subsection (a) shall be submitted in unclassified form but may contain a classified annex.

(c) Appropriate congressional committees and leadership defined.—In this section, the term “appropriate congressional committees and leadership” means—
(1) the Committee on Foreign Relations, the Committee on Banking, Housing, and Urban Affairs, and the majority and minority leaders of the Senate; and
(2) the Committee on Foreign Affairs, the Committee on Financial Services, the Committee on Ways and Means, and the Speaker, the majority leader, and the minority leader of the House of Representatives.

SEC. 318. BRIEFING ON MEASURES TO DENY SPECIALIZED FINANCIAL MESSAGING SERVICES TO DESIGNATED NORTH KOREAN FINANCIAL INSTITUTIONS.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and every 180 days thereafter for 5 years, the President shall provide to the appropriate congressional committees a briefing that includes the following information:

(1) A list of each person or foreign government the President has identified that directly provides specialized financial messaging services to, or enables or facilitates direct or indirect access to such messaging services for—

(A) any North Korean financial institution (as such term is defined in section 3 of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9202)) designated under an applicable United Nations Security Council resolution; or

(B) any other North Korean person, on behalf of such a North Korean financial institution.

(2) A detailed assessment of the status of efforts by the Secretary of the Treasury to work with the relevant authorities in the home jurisdictions of such specialized financial messaging providers to end such provision or access.

(b) FORM.—The briefing required under subsection (a) may be classified.

Subtitle B—Sanctions With Respect to Human Rights Abuses by the Government of North Korea

SEC. 321. SANCTIONS FOR FORCED LABOR AND SLAVERY OVERSEAS OF NORTH KOREANS.

(a) SANCTIONS FOR TRAFFICKING IN PERSONS.—

(1) IN GENERAL.—Section 302(b) of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9241(b)) is amended—

(A) in paragraph (1), by striking “and” at the end; 

(B) in paragraph (2), by striking the period at the end and inserting “; and”; and 

(C) by adding at the end the following new paragraph:

“(3) a list of foreign persons that knowingly employ North Korean laborers, as described in section 104(b)(1)(M).”.

(2) ADDITIONAL DETERMINATIONS; REPORTS.—With respect to any country identified in section 302(b)(2) of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9241(b)(2), as amended by paragraph (1), the report required under section 302(a) of such Act shall—
A) include a determination whether each person identified in section 302(b)(3) of such Act (as amended by paragraph (1)) who is a national or a citizen of such identified country meets the criteria for sanctions under—

(i) section 111 of the Trafficking Victims Protection Act of 2000 (22 U.S.C. 7108) (relating to the prevention of trafficking in persons); or

(ii) section 104(a) or 104(b)(1) of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9214(a)), as amended by section 101 of this Act;

(B) be included in the report required under section 110(b) of the Trafficking Victims Protection Act of 2000 (22 U.S.C. 7107(b)) (relating to the annual report on trafficking in persons); and

(C) be considered in any determination that the government of such country has made serious and sustained efforts to eliminate severe forms of trafficking in persons, as such term is defined for purposes of the Trafficking Victims Protection Act of 2000.

(b) SANCTIONS ON FOREIGN PERSONS THAT EMPLOY NORTH KOREAN LABOR.—

(1) IN GENERAL.—Title III of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9241 et seq.) is amended by inserting after section 302 the following new sections:

"SEC. 302A. REBUTTABLE PRESUMPTION APPLICABLE TO GOODS MADE WITH NORTH KOREAN LABOR.

"(a) IN GENERAL.—Except as provided in subsection (b), any significant goods, wares, articles, and merchandise mined, produced, or manufactured wholly or in part by the labor of North Korean nationals or citizens shall be deemed to be prohibited under section 307 of the Tariff Act of 1930 (19 U.S.C. 1307) and shall not be entitled to entry at any of the ports of the United States.

"(b) EXCEPTION.—The prohibition described in subsection (a) shall not apply if the Commissioner of U.S. Customs and Border Protection finds, by clear and convincing evidence, that the goods, wares, articles, or merchandise described in such paragraph were not produced with convict labor, forced labor, or indentured labor under penal sanctions.

"SEC. 302B. SANCTIONS ON FOREIGN PERSONS EMPLOYING NORTH KOREAN LABOR.

"(a) IN GENERAL.—Except as provided in subsection (c), the President shall designate any person identified under section 302(b)(3) for the imposition of sanctions under subsection (b).

"(b) IMPOSITION OF SANCTIONS.—

"(1) IN GENERAL.—The President shall impose the sanctions described in paragraph (2) with respect to any person designated under subsection (a).

"(2) SANCTIONS DESCRIBED.—The sanctions described in this paragraph are sanctions pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) to block and prohibit all transactions in property and interests in property of a person designated under subsection (a), if such property and interests in property are in the United States, come
within the United States, or are or come within the possession or control of a United States person.

"(c) EXCEPTION.—

"(1) IN GENERAL.—A person may not be designated under subsection (a) if the President certifies to the appropriate congressional committees that the President has received reliable assurances from such person that—

"(A) the employment of North Korean laborers does not result in the direct or indirect transfer of convertible currency, luxury goods, or other stores of value to the Government of North Korea;

"(B) all wages and benefits are provided directly to the laborers, and are held, as applicable, in accounts within the jurisdiction in which they reside in locally denominated currency; and

"(C) the laborers are subject to working conditions consistent with international standards.

"(2) RECERTIFICATION.—Not later than 180 days after the date on which the President transmits to the appropriate congressional committees an initial certification under paragraph (1), and every 180 days thereafter, the President shall—

"(A) transmit a recertification stating that the conditions described in such paragraph continue to be met; or

"(B) if such recertification cannot be transmitted, impose the sanctions described in subsection (b) beginning on the date on which the President determines that such recertification cannot be transmitted.

(2) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the North Korea Sanctions and Policy Enhancement Act of 2016 is amended by inserting after the item relating to section 302 the following new items:

"Sec. 302A. Rebuttable presumption applicable to goods made with North Korean labor.

"Sec. 302B. Sanctions on foreign persons employing North Korean labor.

SEC. 322. MODIFICATIONS TO SANCTIONS SUSPENSION AND WAIVER AUTHORITIES.

(a) EXEMPTIONS.—Section 208(a) of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9228(a)) is amended in the matter preceding paragraph (1)—

(1) by inserting "201A," after "104,;" and

(2) by inserting "302A, 302B," after "209,.

(b) HUMANITARIAN WAIVER.—Section 208(b) of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9228(b)) is amended—

(1) by inserting "201A," after "104," in each place it appears; and

(2) by inserting "302A, 302B," after "209(b)," in each place it appears.

(c) WAIVER.—Section 208(c) of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9228(c)) is amended in the matter preceding paragraph (1)—

(1) by inserting "201A," after "104,"; and

(2) by inserting "302A, 302B," after "209(b),."
SEC. 323. REWARD FOR INFORMANTS.

Section 36(b) of the State Department Basic Authorities Act of 1956 (22 U.S.C. 2708(b)), is amended—
(1) in paragraph (9), by striking “or” at the end;
(2) in paragraph (10), by striking the period at the end and inserting a semicolon; and
(3) by adding at the end the following new paragraphs:
“(11) the identification or location of any person who, while acting at the direction of or under the control of a foreign government, aids or abets a violation of section 1030 of title 18, United States Code; or
“(12) the disruption of financial mechanisms of any person who has engaged in the conduct described in sections 104(a) or 104(b)(1) of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 2914(a) or (b)(1)).”.

SEC. 324. DETERMINATION ON DESIGNATION OF NORTH KOREA AS A STATE SPONSOR OF TERRORISM.

(a) Determination.—
(1) In general.—Not later than 90 days after the date of the enactment of this Act, the Secretary of State shall submit to the appropriate congressional committees a determination whether North Korea meets the criteria for designation as a state sponsor of terrorism.
(2) Form.—The determination required by paragraph (1) shall be submitted in unclassified form but may include a classified annex, if appropriate.

(b) State Sponsor of Terrorism Defined.—For purposes of this section, the term “state sponsor of terrorism” means a country the government of which the Secretary of State has determined, for purposes of section 6(j) of the Export Administration Act of 1979 (46 U.S.C. 4605(j)) (as in effect pursuant to the International Emergency Economic Powers Act), section 620A of the Foreign Assistance Act of 1961 (22 U.S.C. 2371), section 40 of the Arms Export Control Act (22 U.S.C. 2780), or any other provision of law, is a government that has repeatedly provided support for acts of international terrorism.

Subtitle C—General Authorities

SEC. 331. AUTHORITY TO CONSOLIDATE REPORTS.

Any reports required to be submitted to the appropriate congressional committees under this title or any amendment made by this title that are subject to deadlines for submission consisting of similar units of time may be consolidated into a single report that is submitted to appropriate congressional committees pursuant to the earlier of such deadlines. The consolidated reports must contain all information required under this title or any amendment made by this title, in addition to all other elements mandated by previous law.

SEC. 332. RULE OF CONSTRUCTION.

Nothing in this title shall be construed to limit—
(1) the authority or obligation of the President to apply the sanctions described in section 104 of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 2914), as amended by section 311 of this Act, with regard
to persons who meet the criteria for designation under such section, or in any other provision of law; or
(2) the authorities of the President pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.).

SEC. 333. REGULATORY AUTHORITY.
(a) IN GENERAL.—The President shall, not later than 180 days after the date of the enactment of this Act, promulgate regulations as necessary for the implementation of this title and the amendments made by this title.
(b) NOTIFICATION TO CONGRESS.—Not fewer than 10 days before the promulgation of a regulation under subsection (a), the President shall notify and provide to the appropriate congressional committees the proposed regulation, specifying the provisions of this title or the amendments made by this title that the regulation is implementing.

SEC. 334. LIMITATION ON FUNDS.
No additional funds are authorized to carry out the requirements of this title or of the amendments made by this title. Such requirements shall be carried out using amounts otherwise authorized.

Speaker of the House of Representatives.

Vice President of the United States and President of the Senate.
LAWFARE AND U.S. NATIONAL SECURITY

Professor Orde F. Kittrie*

The increasing legalization of international relations has made law an increasingly powerful alternative to traditional military means to achieve operational objectives. Terrorist groups and their state sponsors have made explicit use of such “lawfare” to achieve their operational objectives. The U.S. government’s response to law’s potential as a tool for advancing national security objectives has thus far been predominantly defensive. The United States should not only fight back hard against terrorists’ use of lawfare but also more vigorously look for ways to itself so use law. Lawfare is less deadly than traditional warfare. Also, the U.S.’s advantage in sophisticated legal weapons is surely even greater than its advantage in sophisticated lethal weapons. The article suggests how the United States could more effectively deploy some types of lawfare as a tool for promoting its national security objectives. It takes as a case study the uses and potential uses of lawfare against Iran.

I. LAWFARE AND ITS USE BY TERRORISTS AND THEIR STATE SPONSORS.................................................................395
   A. Battlefield Tactics Designed to Gain Advantage from the Other Side’s Greater Allegiance to International Law .................395
   B. Use—Or Misuse—of Legal Forums to Achieve Operational Objectives Traditionally Achieved by Military Means........397

II. THE U.S. EXECUTIVE BRANCH’S DEFENSIVE RESPONSE TO LAWFARE .............................................................398

III. HOW THE U.S. GOVERNMENT CAN BETTER USE LAWFARE AS A TOOL FOR PROMOTING NATIONAL SECURITY .........................401
   A. The Iranian Threat to International Peace and Security ............402
   B. Overview of U.S. and International Responses to Iran ................403
      1. State and local actions including pension divestment ..........407
      2. Pressure on foreign banks doing business with Iran ..........408

* Orde Félix Kittrie is a Professor of Law at the Sandra Day O’Connor College of Law at Arizona State University. Prior to joining the ASU law faculty, the author served for eleven years at the United States Department of State, including as the lead attorney for nuclear nonproliferation, the lead attorney for arms and dual use trade controls, and special assistant to the Under Secretary of State for Economic and Business Affairs. The views expressed herein are the author’s own.
3. Legal pressure on foreign energy companies supplying refined petroleum to Iran.................................................................411
4. Litigation strategies.........................................................................................................................................................416

IV. CONCLUSION.................................................................................................................................................................419

The increasing legalization of international relations has made law an increasingly powerful alternative to traditional military means to achieve operational objectives. Major General Charles Dunlap, Jr., has famously coined the term “lawfare” to describe the strategy of so using—or misusing—law. Terrorist groups and their state sponsors have made explicit and sometimes effective use of lawfare to achieve their operational objectives.

Under the Obama Administration, and especially the Bush Administration, the U.S. executive branch’s response to law’s potential as a tool for advancing military objectives has thus far been predominantly defensive. This is unfortunate. If there are ways of accomplishing traditional military objectives using law, the United States should not only fight back hard against terrorists’ use of them but also vigorously look for ways to itself so use law. First, lawfare is less deadly than traditional warfare. Second, if some portion of the battle can take place in the courts rather than the battlefield, that should be to the U.S.’s great advantage. While the United States does have more sophisticated lethal weapons than those of its adversaries, its advantage in sophisticated legal weapons is surely even greater. However, the U.S.’s advantage in sophisticated legal weapons has thus far been underutilized.

Part I of this article analyzes lawfare and its use by terrorists and their state sponsors. Part II examines the U.S. executive branch’s defensive response to lawfare. Part III employs as a case study the uses thus far and potential future uses of lawfare against Iran, which is both the leading state sponsor of terrorism and the leading threat to the nuclear nonproliferation regime. The remarkable impact of the limited deployment of lawfare against Iran to date indicates that some types of lawfare, deployed systematically and effectively, may be able to save U.S. and foreign lives by significantly advancing U.S. national security objectives that would otherwise require kinetic warfare. Part IV notes that the successes of lawfare-style sanctions vis-à-vis Iran call into question the accuracy of the dominant paradigm in the scholarly literature regarding sanctions, which derides sanctions as ineffective in a globalized economy. Part IV concludes by considering lessons

learned and how the United States could more effectively use some types of lawfare as a tool for promoting its national security.

I. LAWFARE AND ITS USE BY TERRORISTS AND THEIR STATE SPONSORS

In his series of influential articles on “lawfare,” Major General Charles Dunlap, Jr., used the term lawfare to describe the “strategy of using—or misusing—law as a substitute for traditional military means to achieve an operational objective.”2 The concept of lawfare is extremely useful both for describing a particular set of distinct activities undertaken by enemies of the United States (and its allies), principally terrorists and their state sponsors, and for describing a particular set of distinct activities that could be undertaken by the United States to accomplish its national security objectives vis à vis its enemies.

Lawfare, as practiced by enemies of the U.S., has thus far predominantly taken two interrelated forms: (1) battlefield tactics designed to gain advantage from the greater allegiance of the United States and its allies to international law—especially the international law of armed conflict—and its processes; and (2) the use—or misuse—of legal forums to achieve operational objectives traditionally achieved by military means.

A. Battlefield Tactics Designed to Gain Advantage from the Other Side’s Greater Allegiance to International Law

In his first major article on lawfare, published in 2001, Dunlap focused primarily on battlefield tactics designed to gain advantage from the U.S.’ greater allegiance to international law and its processes, and especially the international law of armed conflict.3 He suggested that these tactics are

2 Charles Dunlap, Lawfare Today: A Perspective, 3 YALE J. INT’L AFF. 146, 146 (2008). Other commentators have offered various narrower definitions. See, e.g., David B. Rivkin, Jr. and Lee Casey, Lawfare, WALL ST. J., Feb. 23, 2007, at A11 (“The term ‘lawfare’ describes the growing use of international law claims, usually factually or legally meritless, as a tool of war.”); Kenneth Anderson, ‘Lawfare’ as Illegal Behavioral Counters to Superior Military Forces, and the Limits of Technological Responses to It, KENNETH ANDERSON’S LAW AND JUST WAR THEORY Blog (May 5, 2008, 10:09 AM), http://kennethandersonlawofwar.blogspot.com/2008/05/as-illegal-behavioral-counters-to.html (“One way to define ‘lawfare,’ in fact, is systematic behavioral violations of the rules of war, violations of law undertaken and planned through advance study of the laws of war in order to predict how law-abiding military forces will behave and exploit their compliance; and where such violations are intended as a behavioral counter to superior military forces, including superior, yet law-compliant, technology and weapons systems.”).

designed to accomplish two main goals: (1) the tactical goal of causing U.S. armed forces to fight with one hand tied behind their back and (2) the strategic goal of destroying the American public’s will to fight by making it appear that the United States is waging war in violation of the law of armed conflict. The same enemy act can accomplish both goals. Dunlap gave as an example Taliban placement of military assets in or around “noncombatant facilities such as religious structures and NGO [non-governmental organization] compounds in the hopes of either deterring attacks or, if attacks do take place, producing collateral damage media events that serve their cause.” Similar tactics have been adopted by other armed forces, including Saddam Hussein’s Iraqi military and Hamas, which, as Laurie Blank notes, has fired from schools and residential areas “in the hope that nearby civilians would deter Israel from responding.”

It has been said by some at this conference that insurgent activities such as firing from amongst civilians are simply a violation of the law of war, and do not merit their own attention, separate from that, as examples of one type of lawfare—the deliberate attempt to gain advantage from the other side’s greater allegiance to international law and its processes. I disagree. I find particularly cynical, troubling, corrosive of international law, and worthy of separate study, efforts to deliberately try to gain advantage from one side’s greater allegiance to international law and its processes. This is a type of lawfare that the United States should strongly oppose and definitely not seek to replicate.

---

4 Id. at 11–13.
5 Id. at 13.
6 See Jefferson D. Reynolds, Collateral Damage on the 21st Century Battlefield, Enemy Exploitation of the Law of Armed Conflict, and the Struggle for a Moral High Ground, 56 A.F. L. Rev. 1, 43–51 (2005); Human Rights Watch, Off Target: The Conduct of the War and Civilian Casualties in Iraq 74-76 (2003); Senior Def. Official, U.S. Dep’t of Def., Briefing on Use of Human Shields in Iraq (Feb. 26, 2003), available at http://www.globalsecurity.org/wmd/library/news/iraq/2003/iraq-030226-dod01.htm (“The Iraqis have regularly placed air defense missile systems and associated equipment in and around civilian areas, including parks, mosques, hospitals, hotels, crowded shopping districts, and even in cemeteries. They have positioned rocket launchers next to soccer stadiums that are in active use, and they’ve parked operational surface-to-air missile systems in civilian industrial areas. This is a well-organized, centrally managed effort, and its objectives are patently clear: preserve Iraq’s military capabilities at any price, even though it means placing innocent civilians and Iraq’s cultural and religious heritage at risk, all in violation of the fundamental principle that civilians and civilian objects must be protected in wartime.”).
2010] U.S. NATIONAL SECURITY 397

B. Use—Or Misuse—of Legal Forums to Achieve Operational Objectives Traditionally Achieved by Military Means

Briefly in Dunlap’s seminal 2001 article, and especially since, the concept of lawfare has also been used, in particular by other commentators, to describe efforts to use—or misuse—legal forums to advance operational objectives traditionally achieved by military means. This latter type of lawfare was famously referred to in the Pentagon’s March 2005 National Defense Strategy for the United States of America, which stated: “Our strength as a nation will continue to be challenged by those who employ a strategy of the weak, focusing on international fora, judicial processes, and terrorism.”

Dunlap provides several examples of such efforts to manipulate legal forums to advance operational objectives traditionally achieved by military means. For instance, in Colombia, the FARC rebels discovered that one way of getting rid of a particularly effective government military commander is to accuse that commander of human rights violations. This is effective because under Colombian law, the commander must then be relieved of command and is not eligible for military defense counsel, thus requiring him to spend personal funds to hire defense counsel.

The manipulation of legal forums to advance military objectives is also an explicit tactic of Hezbollah and Hamas. Hezbollah Secretary General Sayyed Nasrallah has spoken as follows of manipulating legal forums to advance his military objective of defeating Israel: “We have to sue the Israeli leaders anywhere possible in the world. Suing Israel for its crimes will render Israeli leaders beleaguered and perplexed.”

Similarly, a Hamas leader recently discussed the group’s “policy” of seeking to have senior Israeli leaders arrested whenever they visit European countries. The Times of London reported that “Hamas says that it initiated” a British arrest warrant issued against Tzipi Livni, who served as

8 Dunlap, Law and Military Interventions, supra note 3, at 36.
11 Dunlap, Law and Military Interventions, supra note 3, at 36.
14 James Hider, Hamas Using English Law to Demand Arrest of Israeli Leaders for War Crimes, TIMES OF LONDON (Dec. 21, 2009).
Foreign Minister of Israel during the 2008 war in Gaza.\textsuperscript{15} According to the \textit{Times}, in the United Kingdom “the campaign by Hamas takes advantage of an aspect of law in England and Wales that allows anyone to apply for an arrest warrant for alleged war crimes without the need for a prosecuting lawyer.”\textsuperscript{16} As a result of the warrant, Livni, who had been scheduled to address a meeting in London, was forced to cancel her visit.\textsuperscript{17}

Similar warrant efforts have led other Israeli leaders to cancel other visits to the U.K.\textsuperscript{18} Such efforts to manipulate legal forums to transform Israel into a pariah state seem designed to contribute to the Hezbollah and Hamas objectives of destroying Israel, including by distracting Israel’s leaders from their duties; contributing to Israel’s delegitimization and demoralization; and reducing Israel’s ability to conduct diplomatic relations and communicate effectively with foreign audiences.

II. THE U.S. EXECUTIVE BRANCH’S DEFENSIVE RESPONSE TO LAWFARE

Under the Obama Administration, and especially the Bush Administration, the U.S. executive branch’s response to law’s potential as a tool for advancing military objectives has thus far been predominantly defensive. Donald Rumsfeld, Secretary of Defense during the George W. Bush Administration, saw lawfare in “personal terms,” expecting to be “at the top of the target list,” according to Jack Goldsmith, who served during that administration as Special Counsel at the Department of Defense and then Assistant Attorney General for the Office of Legal Counsel.\textsuperscript{19}

Rumsfeld’s concern increased after a group of Iraqis brought universal jurisdiction criminal complaints against him and General Tommy Franks in a Belgian court in the spring of 2003.\textsuperscript{20} The complaints centered on war crimes alleged to have been committed during the invasion of Iraq.\textsuperscript{21} After Rumsfeld threatened to move NATO headquarters out of Belgium, Belgium changed its universal jurisdiction law and blocked the prosecutions of Rumsfeld and Franks.\textsuperscript{22} However, Rumsfeld worried about both the universal jurisdiction laws that remained on the books elsewhere in Europe and international tribunals.\textsuperscript{23} Rumsfeld’s concern about the latter was heigh-
tened by a narrowly averted move by the International Criminal Tribunal for the former Yugoslavia to prosecute NATO officials for bombing a Serbian television station and other alleged war crimes during the 1999 Kosovo campaign. 24

As was discussed in detail at the Lawfare! symposium, some associated with the Bush Administration used the term “lawfare” to derogatorily describe legal work by a human rights non-governmental organization (NGO) and several American attorneys defending Guantanamo detainees and other defendants in the war on terror. 25 The unsubstantiated implication was that the NGO and attorneys were trying to use law to advance a traditional military objective; for example, the defeat of the United States and its allies. 26

The Bush Administration placed considerable weight in its legal policy decisions on defending the United States from lawfare. For example, the Administration opposed U.S. participation in the International Criminal Court (ICC) out of fear that those hostile to the United States might bring about ICC trials of American leaders or soldiers. 27 The Administration also argued for its Guantánamo military tribunals in part on the grounds that standard criminal trials of al-Qaeda operatives could be manipulated by defense counsel to put prosecutors to a choice between revealing sensitive U.S. intelligence sources and methods or letting terrorists go free. 28 As of January 2011, nearly two years into the Obama Administration, the United States still has not joined the ICC, and the Obama Administration has itself decided to use military commissions in certain circumstances. 29

24 Id.
26 It is worth noting that the implication may not be as far off the mark in the specific case of American attorney Lynne Stewart, who was convicted in 2005 by a U.S. federal district court of “assisting terrorism by smuggling information from an imprisoned client to violent followers in Egypt.” John Eligon, Heftier Term for Lawyer in Terrorism Case, N.Y. TIMES, July 16, 2010, at A22.
29 Charlie Savage, Judge Delays Resumption of Guantanamo Trial, N.Y. TIMES, Oct. 15, 2010, http://www.nytimes.com/2010/10/15/us/15gitmo.html# (“Mr. Obama had been a critic during the presidential campaign of Mr. Bush’s use of military commissions. But his administration eventually decided that the tribunals were necessary if certain detainees were to receive trials, because they offered greater flexibility than civilian courts in the admission of certain kinds of evidence, like hearsay and materials gathered under battlefield conditions.”)(emphasis added).
In addition, the U.S. military has, at least in part in response to lawfare, greatly restricted its targeting (on occasion restricting itself beyond the requirements of international law) in order to avoid accusations of disproportionate collateral damage to civilians.\(^{30}\) Dunlap provides an example of how reports about NATO airstrikes allegedly causing civilian casualties were responded to by the International Security Assistance Force (ISAF) in Afghanistan.\(^{31}\) ISAF responded to reports of such deaths by proclaiming that NATO “would not fire on positions if it knew there were civilians nearby.”\(^{32}\) A NATO spokesman emphasized that “if there is the likelihood of even one civilian casualty, [NATO] will not strike, not even if we think Osama bin Laden is down there.”\(^{33}\) This goes beyond the requirements of international law and also encourages enemy forces to surround themselves with innocents so as to immunize themselves from attack.\(^{34}\) As Dunlap so eloquently puts it, NATO’s creation of restrictions beyond what is required by the law of armed conflict creates for its adversary a substitute for conventional military weaponry. . . . for the Taliban to survive it is not necessary for them to build conventional air defenses; rather, just by operating amidst civilians they enjoy a legal sanctuary . . . that is as secure as any fortress bristling with anti-aircraft guns.\(^{35}\)

So the U.S. executive branch’s response to lawfare—law as a tool for advancing operational objectives traditionally achieved by military means—has been predominantly defensive, a response adopted originally by the Bush Administration but which still strongly influences the U.S. ap-

---

30 Charles J. Dunlap, Jr., Visiting Professor, Duke University School of Law and Associate Director, Center on Law, Ethics, and National Security, Presented at Case Western University School of Law Frederick K. Cox International Law Center War Crimes Research Symposium, Does Lawfare Need an Apologia? (Sept. 10, 2010), available at http://www.au.af.mil/au/aunews/archive/2010/0520/0520Articles/Dunlap0520.pdf (“By creating restrictions beyond what the law of armed conflict would require, NATO’s pronouncements encourage the Taliban to shield themselves from air attack by violating the law of armed conflict by embedding themselves among civilians.”).

31 See id. (discussing comments from Maj. John Thomas, spokesman for NATO’s International Security Assistance Force).

32 Id.

33 Id.

34 Id.; Charles J. Dunlap, Jr., Op-Ed., Lawfare Amid Warfare, WASH. TIMES, Aug. 3, 2007, at A17, available at http://www.washingtontimes.com/news/2007/aug/03/lawfare-amid-warfare/?page=1 (“Establishing a paradigm of “zero tolerance” for casualties may well come back to haunt us in yet another way. Specifically, it encourages the enemy to do exactly what we do not want them to do: surround themselves with innocent civilians so as to virtually immunize themselves from attack. It creates a sanctuary that the bad guys are not entitled to enjoy, and sends them exactly the wrong message.”).

35 Dunlap, supra note 30.
proach to the ICC and other issues. This is unfortunate, as the U.S. government could more effectively advance its national security objectives by making more proactive use of lawfare.

III. HOW THE U.S. GOVERNMENT CAN BETTER USE LAWFARE AS A TOOL FOR PROMOTING NATIONAL SECURITY

The U.S. government’s response to lawfare should not simply be a defensive crouch. If there are ways of accomplishing traditionally military objectives using law, the United States should not only fight back hard against others’ use of them but also vigorously look for ways to itself so use law. As Phillip Carter so eloquently put it: “[W]e have every reason to embrace lawfare, for it is vastly preferable to the bloody, expensive, and destructive forms of warfare that ravaged the world in the 20th century.”

First, lawfare has the clear advantage of being less deadly to both combatants and bystanders than is conventional warfare. As Carter wryly puts it, he “would far prefer to have motions and discovery requests fired at [him] than incoming mortar or rocket-propelled grenade fire.” Second, if some part of the fight is to take place not in the battlefields but rather the courts, that should be to U.S. society’s great advantage. While the United States does have more sophisticated lethal weapons than its adversaries, its advantage in sophisticated legal weapons is surely even greater. Thus far, the U.S. advantage in sophisticated legal weapons has been underutilized in the war on terror. The U.S. government, and perhaps even concerned U.S. attorneys in the private sector, could be doing far more to use law—both existing law and potential changes to law—as part of the fight against al-Qaeda, the Taliban, the Iranian regime, and others who seek to engage in terrorist acts against the United States and/or acquire weapons of mass destruction.

In order to concretely analyze how the United States could more effectively use lawfare as a tool for promoting its national security, the remaining sections of this article employ as a case study the uses thus far and potential future uses of lawfare against Iran, which is both the leading state sponsor of terrorism and the leading threat to the nuclear nonproliferation regime. The article will analyze, and draw more broadly applicable lessons from, four existing examples of where law is already being used deliberate-

37 Id. (“[L]awfare rarely generates the collateral damage of conventional warfare. In recent war zones such as Bosnia, Chechnya, and Iraq, the cumulative civilian death toll stretches into the hundreds of thousands.”).
38 Id.
ly, systematically, and creatively to achieve operational objectives against Iran.

A. The Iranian Threat to International Peace and Security

Iran’s nuclear weapons program, state sponsorship of terrorism, and human rights abuses make it a preeminent threat to international peace and security. In pursuing its dangerous agenda, the Iranian government egregiously violates international law. For example, Iran continues to violate U.N. Security Council resolutions ordering Iran to suspend its nuclear enrichment, reprocessing, and heavy water related activities. In a series of periodic reports, most recently on November 23, 2010, the Director General of the International Atomic Energy Agency has determined again and again that “contrary to the relevant resolutions of the Board of Governors and the Security Council, Iran has not suspended its enrichment related activities” and has “continued” with “heavy water related activities.”

At the same time, Iran has chosen to violate numerous other international legal obligations. Iran’s brutal response to postelection protests contravened its human rights obligations under international law, including the International Covenant on Civil and Political Rights. Iran has also continued its destabilizing support for terrorist groups across the Middle East, including by providing them with arms in violation of U.N. Security Council Resolutions 1701 and 1747.

---


43 For example, an Iranian ship carrying weapons from Iran to Yemeni rebels, which was seized by the Yemeni government on October 26, 2009, violated UN Security Council Resolution 1747, which orders that “Iran shall not supply, sell or transfer directly or indirectly from its territory or by its nationals or using its flag vessels or aircraft any arms or related materiel.” S.C. Res. 1747, supra note 41, ¶ 5. A second ship, carrying 500 tons of weapons from Iran to Hezbollah in Lebanon, which was seized by the Israeli navy on November 3,
B. Overview of U.S. and International Responses to Iran

What is the range of responses available to the United States and to the international community? A U.S. President’s five key tools for altering the behavior of a foreign country can be alliteratively characterized as: (1) speaking (statements and negotiations); (2) sweeteners (incentives); (3) sanctions (economic and diplomatic restrictions); (4) sabotage and (5) soldiers (military action). In the case of Iran, speaking and sweeteners have been tried and failed, and soldiers are a very problematic option.

The United States and its allies are reportedly focusing their efforts against Iran’s nuclear program on sanctions and covert sabotage (including, for example, the Stuxnet computer virus). The combination of sanctions and sabotage seems, as of early January 2011, to be succeeding in significantly slowing Iran’s nuclear program. On January 10, 2011, Secretary of State Hillary Clinton stated: “The most recent analysis is that the sanctions have been working. They have made it much more difficult for Iran to pur-
sue its nuclear ambitions." As Washington Post Associate Editor David Ignatius wrote about U.S. policy towards Iran in a column in early January 2011, "What’s increasingly clear is that low-key weapons—covert sabotage and economic sanctions—are accomplishing many of the benefits of military action, without the costs."

While Stuxnet and other efforts to sabotage Iran’s nuclear program are clearly having a significant impact, and undoubtedly raise important questions in the cyberlaw and other relevant legal arenas, they are not examples of using law as a tool to achieve an operational objective. In contrast, sanctions are a form of lawfare, as Paul Williams noted at the Lawfare! symposium, and as Gen. Charles Dunlap discusses in the section titled ‘Lawfare as an American Weapon’ of his article for this symposium. Gen. Dunlap provides several examples of when ‘actions that could be characterized as lawfare have been carried out by the United States—and properly so.’ In doing so, he offers the following outstanding example of the potential power of the sanctions type of lawfare:

Legal ‘weaponry’ can have effects utterly indistinguishable from those produced by their kinetic analogs. During the 2003 invasion, for example, the Iraqi air force found itself hobbled by a legal device—sanctions—as effectively as by any outcome from traditional aerial combat. By preventing the acquisition of new aircraft, as well as spare parts for the existing fleet, Iraqi airpower was so debilitated that not a single aircraft rose in opposition to the coalition air armada.

The sanctions imposed on Iran in recent years—through U.N. Security Council resolutions binding under international law and through changes to the domestic laws of the U.S., European Union, and others—have been a particularly salient, deliberate, and, in many cases, creative form of lawfare. The sanctions use law as a substitute for traditional military means to advance an operational objective—in this case, halting Iran’s illicit nuclear program.

---

48 Ignatius, supra note 45, at A17.
49 Dunlap, supra note 30.
50 Id.
51 Id.
52 See, e.g., S.C. Res. 1737, supra note 40 (the Security Council, in the resolution’s preamble, notes that the resolution is motivated in part by a determination “to constrain Iran’s development of sensitive technologies in support of its nuclear and missile programmes”); Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010, Pub. L. No. 111-195, § 2 (10) (2010) (finding that “economic sanctions to prevent Iran from
What are the principal means by which sanctions—economic and other restrictions imposed through changes to international and domestic law—can advance their operational objective? Sanctions can have any or all of several useful impacts on the target, including especially (1) coercing the target (in this case Iran) into halting its illegal behavior, if the costs of the behavior (in this case proceeding with the nuclear program or supporting terrorism) are increased sufficiently to outweigh the benefits to the regime of proceeding with the behavior; and (2) constraining the target from engaging in illegal behavior, if the sanctions materially reduce the target’s supply of assets necessary to engage in the behavior. The U.S. government’s current sanctions on Iran are designed to both coerce and constrain Iran.

Recent history shows that strong sanctions, effectively implemented, can help stop illegal nuclear weapons programs and terrorism. For example, robust sanctions helped induce Libya to forsake terrorism and verifiably relinquish its nuclear, chemical, and biological weapons programs. In exchange for the lifting of sanctions imposed by the United Nations and United States, Libya halted its support for terrorism, paid $2.7 billion to the families of the Pan Am flight 103 bombing victims, and allowed a team of British and U.S. government experts to enter Libya and dismantle its weapons of mass destruction infrastructure.

Developing nuclear weapons, are necessary to protect the essential security interests of the United States.

---

53 Readers interested in a more detailed discussion of the goals potentially served by the imposition of sanctions in the international arena may wish to refer to Orde F. Kittrie, Averting Catastrophe: Why the Nuclear Nonproliferation Treaty is Losing its Deterrence Capacity and How to Restore It, 28 MICH. J. INT’L L. 337, 354–61 (2007).

54 Press Release, U.S. Dep’t of the Treasury, Remarks at the Center for Strategic and International Studies by Treasury Under Secretary for Terrorism and Financial Intelligence Stuart Levey (Sept. 20, 2010) [hereinafter Levey remarks], available at http://www.ustreas.gov/press/releases/tg862.htm (Levey emphasizes two desired impacts of the Obama Administration’s tightening sanctions on Iran. One is “to sharpen the choice for Iran’s leaders between integration with the international community, predicated on fulfilling their international obligations, and the hardship of further isolation.” Levey explains that “[b]y dramatically isolating Iran financially and commercially and by capitalizing on Iran’s existing vulnerabilities, we can impact Iran’s calculations” so as to “create crucial leverage for our diplomacy.” Another desired impact is to “make it harder for Iran to pursue international procurement for its nuclear and military programs.”).

55 GARY CLYDE HUFBAUER, JEFFREY J. SCHOTT, KIMBERLY ANN ELLIOTT & BARBARA OEGG, ECONOMIC SANCTIONS RECONSIDERED 12–13 (3d ed. 2007) (“[T]he surprise decision by Libyan President Muammar Gadhafi in 2003 to renounce weapons of mass destruction was partly influenced by his desire to end the decade-old U.S. sanctions and to gain access to American oil field technology and know-how.”).

56 The sanctions on Libya both contained Qaddafi’s ability to develop weapons of mass destruction and ultimately coerced him, including by grinding down Libya’s oil industry and causing economic problems so severe they threatened his grip on Libya. See Kittrie, supra note 53, at 406–14.
Unfortunately, the U.N. Security Council—thanks to Russian and Chinese obstructionism—has thus far imposed relatively weak sanctions on Iran for its proliferant activities.\textsuperscript{57} For example, the sanctions thus far imposed by the Security Council on Iran are significantly weaker than the sanctions imposed by the Council in response to many lesser threats to international peace and security—including on Liberia during its 2003 civil war, Sierra Leone in response to its 1997 military coup, Yugoslavia during the Bosnia crisis, Haiti in response to its 1991 military coup, Libya in response to its support for terrorism, and Iraq in response to its invasion of Kuwait and weapons of mass destruction programs.\textsuperscript{58}

Due to its ideology, the value to the Iranian regime of engaging in nuclear proliferation is particularly high.\textsuperscript{59} However, the price the international community has exacted from the Iranian regime for its violations has thus far been remarkably low. Security Council Resolutions 1737, 1747, 1803, and 1929 are, by themselves, too weak to coerce Iran into compliance, halt Iran’s ability to advance its nuclear weapons program, or deter other states from following Iran’s lead and developing their own nuclear weapons program. This is unfortunate because Iran’s heavy dependence on foreign trade leaves it highly vulnerable to strong economic sanctions.\textsuperscript{60}

Concerned that U.N. Security Council sanctions on Iran are insufficiently impactful, and faced with the drawbacks of a U.S. military option, American opponents of Iran’s nuclear weapons program are creatively using law in four key ways to step up the pressure on Iran to comply with international law and cease its enrichment and other sensitive nuclear activities: (1) state and local actions including pension divestment; (2) legal pressure on foreign banks doing business with Iran; (3) legal pressure on foreign energy companies supplying refined petroleum to Iran; and (4) litigation strategies.

\textsuperscript{57} See id. at 383–84, 389 (discussing Russian and Chinese blocking of strong Security Council sanctions on Iran).


\textsuperscript{59} See id. at 543–44 (“Iranian leadership is . . . motivated by a religious conviction that exalts martyrdom and suffering. In comparison with a purely economic calculation, the Iranian regime’s ideology causes it to ascribe greater cost to complying with the sender’s demand to shut down the nuclear weapons program and lesser cost to any suffering that may be imposed by sanctions.”).

\textsuperscript{60} See Kittrie, \textit{supra} note 58, at 536–537 (“Iran’s heavy dependence on oil export revenue and other foreign trade leaves it highly vulnerable to economic sanctions.”); see also Kittrie, \textit{Using Stronger Sanctions to Increase Negotiating Leverage with Iran}, \textsc{Arms Control Today} (Dec. 2009), at 18–21, http://www.armscontrol.org/print/3982.
1. State and local actions including pension divestment

As of 2004, U.S. state and local pension funds reportedly had some $188 billion invested in foreign companies doing business with state sponsors of terrorism, including Iran. As and local pension fund divestment from such companies was seen by its proponents as having the potential to contribute significantly to discouraging these and other foreign companies from investing in, or otherwise doing business with, these state sponsors of terrorism. In addition, the threatened withdrawal from such companies of state and local pension fund investment was seen as providing these companies with a strong incentive to withdraw from business they were already doing with the state sponsors of terrorism. At least twenty-seven states and the District of Columbia have divested pension funds from companies doing business with Sudan, as have at least twenty-two cities. In addition, at least nineteen states and the District of Columbia have divested pension funds from companies investing in Iran’s energy sector. In order to facilitate such divestment relating to Sudan, Congress passed, and President Bush signed into law in 2007, the Sudan Accountability and Divestment Act, which clarifies that certain types of state and local divestment from companies doing business with Sudan are not preempted. Similarly, on July 1, 2010, President Obama signed into law the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010, which clarifies that certain types of state and local divestment from companies doing business with Iran are not preempted.

Iran’s opponents in the United States have also used state and local law in other ways to put pressure on Iran. For example, in 2007, when Minnesota Governor Tim Pawlenty discovered that an Indian company, Essar, was seeking to both invest some $1.6 billion in Minnesota and invest over

---

61 See Ctr. for Sec. Policy, The Terrorism Investments of the 50 States, DivestTERROR.ORG, 2 (Aug. 12, 2004), http://merln.ndu.edu/merln/mipal/reports/DivestTerror_Report.pdf (“The total estimated value of the stock of some 400 companies doing business in terrorist sponsoring states held by America’s leading public pension systems is approximately $188 billion.”).
62 See id.
63 See id.
$5 billion in building a refinery in Iran, he put Essar to a choice.\textsuperscript{68} Pawlenty threatened to block state infrastructure subsidies and perhaps even construction permits for the Minnesota purchase unless Essar withdrew from the Iranian investment.\textsuperscript{69} Essar promptly withdrew from the Iranian investment.\textsuperscript{70}

In 2009, activists in Los Angeles, California put pressure on Siemens, which sold communications monitoring and other equipment to the Iranian government, by opposing Siemens’ efforts to supply rail cars to the Los Angeles Metropolitan Transportation Authority.\textsuperscript{71} In January 2010, Siemens announced that it would forgo new business with Iran.\textsuperscript{72} Although the Siemens decision to forgo new business with Iran was not as clearly tied to U.S. state or local pressures as was Essar’s decision, the rail car contract incident provides another interesting example of how lawfare can be used at the state or local level.

2. Pressure on foreign banks doing business with Iran\textsuperscript{73}

The U.S. Department of the Treasury has convinced more than eighty banks around the world, including most of the world’s top financial institutions,\textsuperscript{74} to cease some or all of their business with Iran.\textsuperscript{75} The tactics Treasury is using were designed and first implemented under the George W.

\textsuperscript{68} See Larry Oakes, Essar Drops Plan with Iran: Steel Mill on Range is a Go, STARTRIBUNE.COM (Oct. 31, 2007, 8:12 PM), http://www.startribune.com/business/11245206.html (discussing Minnesota Governor Tim Pawlenty’s statement that Essar’s plans with Iran, if carried out, would jeopardize Essar’s subsidies to operate in Minnesota).

\textsuperscript{69} See id. (stating that Minnesota Governor Tim Pawlenty had threatened to pull construction permits if Essar followed through with its plans to build an oil refinery in Iran).

\textsuperscript{70} See Tim Pugmire, Pawlenty Says Essar Concerns are Resolved, MPR NEWS (Oct. 31, 2007, 5:16 PM), http://minnesota.priprod.publicradio.org/display/web/2007/10/31/essargoesforward/.

\textsuperscript{71} See Eli Lake, Siemens Risks Losses Due to Iran Ties, WASH. TIMES (July 17, 2009, 4:45 AM), http://www.washingtontimes.com/news/2009/jul/17/siemens-risks-losses-due-to-iran-ties/print/ (“One of the world’s largest engineering firms, Siemens, could lose hundreds of millions of dollars in sales to the Los Angeles Metropolitan Transportation Authority (MTA) because it sold Iran equipment used to spy on dissidents.”).


\textsuperscript{73} Readers interested in a more detailed discussion of the U.S. Treasury Department’s innovative campaign to persuade banks to curtail their business with Iran may wish to refer to Orde F. Kittrie, New Sanctions for a New Century: Treasury’s Innovative use of Financial Sanctions, 30 U. PA. J. INT’L L. 789, 789–822 (2009), from which this discussion is adapted.

\textsuperscript{74} See id. at 815 (“More than 80 banks around the world, including ‘most of the world’s top financial institutions,’ have curtailed business with Iran.”).

\textsuperscript{75} See Robin Wright, Stuart Levy’s War, N.Y. TIMES MAG., Nov. 2, 2008, at 31.
Bush administration. However, the Obama Administration cast a strong vote of confidence in them, including by taking the extraordinary decision to retain in place Stuart Levey, the Bush-appointed Under Secretary of the Treasury, who is principally known as the leading architect of these financial sanctions.

What is Treasury’s rationale for pressuring foreign banks to curtail their business dealings with Iran? Iran utilizes the international financial system to advance both its nuclear program and its state sponsorship of terrorism. In order to avoid suspicion and minimize the risk of detection, Iran’s state-owned banks and other entities use an array of deceptive practices when using their global financial ties to advance Iran’s nuclear program and sponsorship of terrorism. For example, Iran uses front companies and intermediaries to surreptitiously obtain technology and materials for its nuclear and missile programs from countries that would prohibit such exports to Iran. In addition, Iranian banks ask other financial institutions to remove the Iranian banks’ names when processing their transactions through the international financial system. The goal is to allow Iranian banks to remain undetected as they move money through the international financial system to pay for the Iranian government’s nuclear and missile related purchases and to fund terrorism.

What accounts for Treasury’s considerable success in persuading foreign banks to stop doing business with Iran? Treasury’s principal innovation can be described as follows: Rather than asking, e.g., the Swiss government to order its banks to stop doing business with Iran, the Treasury has gone directly to the Swiss banks. Treasury has found that its unprecedented direct outreach to a country’s key private financial institutions can yield results much more quickly than does outreach to that same country’s government, which can lack political will or the necessary authority, or may face cumbersome bureaucratic procedures for exercising whatever relevant

76 See, e.g., id., Kittrie supra note 73, at 815.
77 Paul Richter, Obama Administration Keeps Bush Official Involved with Iran Sanctions, L.A. TIMES (Feb. 3, 2009), http://articles.latimes.com/2009/feb/03/world/fg-usiran3 (“The Obama administration has decided to retain the official who led the Bush administration’s effort to squeeze Iran with economic sanctions, providing an important clue on how it intends to approach the Islamic Republic.”).
79 Id.
80 Id.
authorities it does have.\textsuperscript{81} Once some foreign private financial institutions decide to halt business with entities or individuals of concern, the reputational risk for others not to follow is increased, and those who have halted business with Iran often cooperate with the United States in putting pressure on those who have not yet done so.\textsuperscript{82} Other banks within the jurisdiction soon follow.\textsuperscript{83} Such private sector decisions can in turn make it more politically feasible for foreign governments to impose restrictions because some or all of the major relevant companies in their jurisdiction have already foregone the business.\textsuperscript{84} 

What does the Treasury Department say to the foreign banks to get them to stop doing business with Iran? Treasury officials remind the foreign banks of the risks of doing even prima facie legal business with Iran.\textsuperscript{85} The banks with which the Treasury Department communicates are already aware of the prosecutions the Treasury has brought against other banks. For example, in May 2004, the Federal Reserve fined UBS, Switzerland’s largest bank, $100 million for sending U.S. dollars to Cuba, Iran, Libya, and Yugoslavia, and intentionally hiding the transactions by submitting false monthly reports to the Federal Reserve.\textsuperscript{86} In December 2005, ABN Amro Bank NV, a Dutch firm, was fined $80 million by U.S. federal and state financial regulators for actions including modification by its branch in Dubai of payment instructions on wire transfers, letters of credit, and checks issued by Iran’s Bank Melli and a Libyan bank in order to hide their involvement in the transactions and enable access to the U.S. banking system.\textsuperscript{87} As one former Treasury official put it in 2008, the Treasury Department’s success in persuading foreign banks to curtail transactions with Iran

\textsuperscript{81} \textsc{Press Release}, U.S. Dep’t of Treasury, Remarks by Treasury Secretary Paulson on Targeted Financial Measures to Protect Our National Security (June 14, 2007) [hereinafter Paulson Remarks].

\textsuperscript{82} See id.

\textsuperscript{83} See id.

\textsuperscript{84} Glaser statement, supra note 78, at 35.

\textsuperscript{85} Id.

\textsuperscript{86} See UBS Fined $100 Million Over Trading of Dollars, N.Y. Times, May 11, 2004, at C17.

\textsuperscript{87} Paul Blustein, Dutch Bank Fined for Iran, Libya Transactions: $80 Million Levied for Foreign Dealings, Money Laundering, Wash. Post (Dec. 20, 2005, 5:09 PM), http://www.washingtonpost.com/wp-dyn/content/article/2005/12/19/AR2005121901804.html. Between December 2001 and April 2004, ABN AMRO’s overseas branches removed or revised references to entities in which the governments of Libya and Iran had an interest before forwarding wire transfers, letters of credit and U.S. dollar checks to ABN AMRO branches in New York, NY and Chicago, IL. Office of Foreign Assets Control, Dep’t of Treasury, Enforcement Information (Jan. 3, 2006).
was due in part to those banks’ eagerness “to avoid being the ‘next ABN AMRO.’”\textsuperscript{88}

Such prosecutions have continued under the Obama Administration. In January 2009, Lloyds TSB Bank had to pay the U.S. government $350 million in fines and forfeiture as a result of a scheme in which Lloyds altered or “stripped” wire-transfer information to hide the identities of Iranian and Sudanese clients in order to deceive American financial institutions and enable the clients to access the U.S. banking system.\textsuperscript{89} The stripping of wire-transfer information “made it appear that the transactions originated at Lloyds TSB Bank” in the U.K. rather than in the sanctioned countries.\textsuperscript{90} Most recently, in August 2010, Barclays PLC agreed to a $298 million settlement with U.S. prosecutors in connection with allegations that it violated U.S. financial sanctions against countries including Iran.\textsuperscript{91}

What has been the impact on Iran of the pressure on foreign banks doing business with Iran? With most leading foreign banks curtailing their business with Iran, Iranian companies and their business partners are finding it difficult to arrange letters of credit, a central requirement for conducting trade.\textsuperscript{92} Many companies doing business in or with Iran have been forced to use smaller banks or go through intermediaries to arrange new letters of credit, adding twenty to thirty percent to their costs.\textsuperscript{93}

3. Legal pressure on foreign energy companies supplying refined petroleum to Iran

Although Iranian oil wells produce far more petroleum (crude oil) than Iran needs, Iran has relatively little capacity to refine that petroleum (turn it into gasoline and diesel fuel).\textsuperscript{94} Remarkably for a country that is investing so much in its nuclear programs, Iran has developed insufficient

\textsuperscript{88} Michael Jacobson, Sanctions Against Iran: A Promising Struggle, 31 WASH. Q. 69, 73 (2008).
\textsuperscript{89} Chad Bray, Lloyds TSB Settles with U.S. Officials, WALL ST. J., Jan 10, 2009, at B8.
\textsuperscript{90} Id.
\textsuperscript{91} Barclays Deal with U.S. Over Trade Sanctions is Approved, N.Y. TIMES, Aug. 19, 2010, at B9.
\textsuperscript{92} See, e.g., Mark Trevelyan, More Companies Suspend Business with Iran, INT’L HERALD TRIB., Jan. 17, 2008, at 15 (quoting a senior German banking and finance consultant as stating that “[i]t is today impossible more or less in Europe, with a couple of exceptions, to get a letter of credit” for trade with Iran); No Letters of Credit, No Steel for Iranian Importers, say Traders, METAL BULLETIN WEEKLY, Sept. 13, 2010, http://www.metalbulletin.co.uk/Article/2675316/No-letters-of-credit-no-steel-for-Iranian-importers-say-traders.html.
\textsuperscript{94} U.S. ENERGY & INFO. ADMIN., COUNTRY ANALYSIS, IRAN, http://www.eia.doe.gov/cabs/Iran/Oil.html.
capacity to refine the petroleum it pumps out of its own soil. As a result, in 2009, Iran imported some forty percent of the gasoline it was consuming. In 2008, nonproliferation law experts and members of Congress began looking into how they might use law as a tool to pressure those companies to stop doing business with Iran. Newsweek put it as follows:

An Arizona State University law professor and former State Department nuclear-nonproliferation official, Orde Kittrie, discovered that Reliance had benefited from two U.S. Export-Import Bank loan guarantees totaling $900 million. Members of Congress—led by Democratic Rep. Brad Sherman of California and Republican Mark Kirk of Illinois—demanded that the Ex-Im Bank cut off U.S. taxpayer assistance. After consulting with its high-priced Washington lobbying firm, BGR, Reliance quietly passed the word to members of Congress: it was halting all sales to Iran and would insist that its trading partners do the same.

The idea of squeezing Iran’s gasoline supplies came to the attention of Presidential candidate Barack Obama. In a June 2008 speech, then-Senator Obama said: “We should work with Europe, Japan and the Gulf states to find every avenue outside the United Nations to isolate the Iranian regime—from cutting off loan guarantees and expanding financial sanctions, to banning the export of refined petroleum to Iran.” Obama repeated this sentiment during the presidential candidates’ debate on Oct. 7, 2008: “Iran right now imports gasoline . . . if we can prevent them from importing the gasoline that they need . . . that starts changing their cost-benefit analysis. That starts putting the squeeze on them.”

After Iran’s leadership rebuffed the Obama Administration’s initial attempts to engage Iran, Congress stepped up its efforts to place legal pressure on foreign energy companies supplying gasoline to Iran. In October 2009, both houses of Congress passed, and President Obama signed into law, a prohibition on foreign companies selling to the U.S. government’s

---

Strategic Petroleum Reserve if they are significantly involved in providing refined petroleum to Iran.100

Then, on July 1, 2010, President Obama signed the Comprehensive Iran Sanctions, Accountability, and Divestment Act (CISADA).101 CISADA principally mandates that the President impose sanctions (up to and including being barred from doing business in the U.S.) on any foreign company that does various types of business with Iran’s energy sector, including being involved with providing gasoline to Iran.102 CISADA notably also:

- Requires each prospective contractor submitting a federal government bid to certify that the contractor or a person owned or controlled by the contractor does not conduct any activity sanctionable under a key provision of CISADA103
- Prohibits most remaining trade between Iran and the United States104
- Requires the Secretary of the Treasury to restrict the opening or maintaining in the United States of a correspondent or payable-through account by a foreign financial institution if that institution knowingly engages in various types of transactions with proscribed Iranian entities105
- Directs the Secretary of the Treasury to prohibit any person owned or controlled by a domestic financial institution from knowingly engaging in a transaction with or benefitting the Iranian Revolutionary Guard Corps or its designated affiliates.106
- Prohibits U.S. executive agencies from entering into procurement contracts with entities that have exported to Iran sensitive communications technology intended to be used to monitor or disrupt the free flow of communications to, or restrict the speech of, the people of Iran107
- Increases criminal penalties for violations of various sanctions provisions108
- Clarifies that certain types of state and local divestment from companies doing business with Iran are not preempted109


102 Id.

103 Id. at § 102.

104 Id. at § 103(b).

105 Id. at § 104(c).

106 Id. at § 104(d).

107 Id. at § 106.

108 Id. at § 107.
CISADA had a significant impact on gasoline exports to Iran even before it was signed into law. Different companies stopped their varied forms of involvement in providing gasoline to Iran at different stages in the legislative process. For example, several companies stopped such business once the bill passed both houses of Congress, another company stopped once the conferenced legislation had been passed by both house of Congress, and another stopped conducting such business with Iran a few days after President Obama signed the bill into law.\textsuperscript{110}

Since CISADA’s enactment in July 2010, the Obama Administration has, with foreign companies doing business with Iran’s energy sector, taken an analogous approach to the Treasury Department’s unprecedented direct outreach to key foreign private financial institutions. William Burns, the Under Secretary of State for Political Affairs, put it as follows in his December 1, 2010 statement to the House Committee on Foreign Affairs:

[W]e have used the powerful instrument provided by CISADA’s “special rule” to persuade major European and Asian firms, including Shell, Statoil, ENI, Total and INPEX, to terminate or take significant verifiable steps toward stopping potentially sanctionable activities in Iran and provide clear assurances that they would not undertake any sanctionable activities in Iran’s energy sector in the future. According to reliable estimates, Iran may be losing as much as $50-60 billion overall in potential energy investments, along with the critical technology and know-how that comes with them. More specifically, major international oil companies such as Shell, Statoil, ENI, Total and INPEX have decided not to undertake any new activities in Iran. In addition, major fuel suppliers such as Vitol, Shell, Reliance, IPG, Glencore, and Trafigura have announced that

\textsuperscript{109} \textit{Id.} at § 202.

they will no longer sell refined petroleum products to Iran. Investment in Iran’s upstream oil and gas sector has dropped dramatically, forcing Iran to abandon liquefied natural gas projects for lack of foreign investment and technical expertise.\footnote{Hearing on Iran Sanctions, H. Comm. On Foreign Affairs, 111th Cong. (Dec. 1, 2010) (written statement of William Burns, Under Secretary of State for Political Affairs), http://foreignaffairs.house.gov/111/bur120110.pdf.}

The “special rule” contained in Section 102(g) of CISADA allows the President to on a case-by-case basis terminate, or not initiate, an investigation of certain sanctionable activities under the Act if the President certifies that the sanctionable entity has stopped the sanctionable activity or has “taken significant verifiable steps toward stopping the activity” and the President has “received reliable assurances” that the sanctionable entity “will not knowingly engage in [such activities] in the future.”\footnote{Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010, Pub. L. No. 111-195, § 102 (g) (2010).}

As discussed in section B.2 of this article, the Treasury Department has in recent years persuaded foreign banks to stop doing business with Iran by directly reaching out to those foreign banks and reminding them of the risks of doing business with Iran, a risk exemplified by the steep fines levied against banks caught conducting illicit trade with Iran. In much the same way, the State Department has in recent months persuaded foreign energy companies to stop doing business with Iran by directly reaching out to those foreign energy companies and advising them of the risks of doing business with Iran, a risk exemplified by the CISADA sanctions (on companies doing business with Iran’s energy sector), imposition of which can be halted if the President receives reliable assurances that the company is stopping such business with Iran’s energy sector.\footnote{See, e.g., U.S. DEP’T OF STATE, SPECIAL BRIEFING BY DEPUTY SECRETARY OF STATE JAMES B. STEINBERG ON IRAN SANCTIONS IMPLEMENTATION (Sept. 30, 2010), http://www.state.gov/s/d/2010/148479.htm (“[F]our major international oil companies . . . have pledged to end their investments in Iran’s energy sector . . . . These companies have provided assurances to us that they have stopped or are taking significant verifiable steps to stop their activity in Iran and have provided assurances not to undertake new energy-related activity in Iran that may be sanctionable . . . . as a result, the Secretary has decided to use the Special Rule to avoid making a determination of sanctionability for these companies.”).} In both cases, an implied or explicit threat of legal action pursuant to U.S. law, delivered to the foreign company directly by U.S. officials, persuades the foreign company to stop doing business with Iran, even though such business is not prohibited by the government of the country in which the foreign company is headquartered.

As a result of this creative new form of lawfare, by October 2010, each of the companies that had, two years before, been one of the top five
suppliers of gasoline to Iran, had dropped out of supplying gasoline to Iran. The volume of gasoline imported by Iran in September 2010 was reportedly as much as ninety percent less than what Iran imported in months prior to the July 1, 2010 enactment of CISADA. Meanwhile, Iran’s remaining gasoline suppliers have demanded higher premiums from Iran for their willingness to risk U.S. penalties. By using lawfare, the United States and its allies have managed to drastically reduce Iran’s gasoline supplies without intercepting a single tanker or firing a single shot.

4. Litigation strategies

The small cadre of private sector American attorneys who sue terrorist groups and the national governments which support them are an exceptional example of the use of lawfare in the war against terrorism. These lawsuits have been extremely effective at times, including by bringing attention to the harm done by terrorists to Americans, using the American judicial system to find facts and make determinations as to the connections between countries such as Iran and terrorist attacks by groups such as Hezbollah, and putting financial pressure on terrorist-supporting states such as Libya and Iran. For example, the lawsuit against Libya by the American victims of Libya’s bombing of Pan Am 103 was a vehicle by which Libya, in August 2003, formally accepted responsibility for the bombing and paid $2.7 billion in compensation to the victims’ families.

---


Iran is already a major target of these litigators as a result of terrorist acts including the 1983 Marine barracks bombing in Beirut, Lebanon.\(^{118}\) On October 23, 1983, a truck bomb struck a barracks housing U.S. Marine participants in the multinational peacekeeping force in Beirut, killing 241 Marines.\(^{119}\) In July 1987, Iran’s then-Minister of Revolutionary Guards, Mohsen Rafiqdoost, admitted that, “both the TNT and the ideology which in one blast sent to hell 400 officers, NCOs, and soldiers at the Marines headquarters were provided by Iran.”\(^{120}\) There is a broad consensus among Western experts that the planning of the attacks was supervised by Iran’s ambassador to Syria.\(^{121}\)

In May 2003, in a case brought by relatives of some of the U.S. Marines who were killed, U.S. District Court Judge Royce C. Lamberth ruled that the Islamic Republic of Iran was responsible for the Marine barracks attack.\(^{122}\) Lamberth based his conclusion on testimony by expert witnesses, including a Hezbollah member who participated in the group that planned the attack, and a declassified National Security Agency intercept of a September 1983 message sent from Iranian intelligence headquarters in Tehran instructing the leader of Hezbollah (then known as Islamic Amal) to “take a spectacular action against the United States Marines.”\(^{123}\) In 2007, Lamberth ordered Iran to pay $2.7 billion in compensation to the victims’ families.\(^{124}\) In 2008, Lamberth’s ruling served as the basis for the U.S. District Court for the Southern District of New York freezing $2 billion in Iranian assets, held in a Citibank account in New York City, at the behest of an attorney for the victims’ families.\(^{125}\)

U.S. nonproliferation officials, these private sector attorneys, and others are now considering how to use these civil litigation tactics, and the

---

\(^{118}\) Readers interested in a more detailed discussion of Iran’s long state sponsorship of terrorism and the international community’s response may wish to refer to Orde F. Kittrie, *Emboldened by Impunity: The History and Consequences of Failure to Enforce Iranian Violations of International Law*, 57 SYRACUSE L. REV. 519 (2007), from which this discussion is adapted.


\(^{120}\) Rafiqdoost’s comments were published in the Tehran daily *Resalat* on July 20, 1987.

\(^{121}\) **Pollack, supra note 119, at 203.**


\(^{123}\) Id. at 54.


legal precedents they have set, to go after proliferators and their suppliers. Civil litigation options being considered include:

- Lawsuits against foreign suppliers of dual-use items to Iran, for example for aiding and abetting Iran’s violations of international nonproliferation law. One key question raised by this option is who, including prospective victims of an illicit Weapons of Mass Destruction program, could get standing to sue.

- Lawsuits based on the apparent personal involvement of senior Iranian leaders in Hezbollah terrorist attacks. In 2008, the European Union designated the current Iranian defense minister, Ahmed Vahidi, as “a person linked to Iran’s proliferation-sensitive nuclear activities or Iran’s development of nuclear weapon delivery systems.” Separately, an Argentinian judge has issued an arrest warrant for Vahidi, who is accused by Argentina of having masterminded Hezbollah’s 1994 bombing of a Jewish cultural center in Argentina, which killed eighty-five people. Despite assistance from Interpol, Argentina has not yet succeeded in bringing Vahidi to justice. Perhaps civil litigation could be more effective in reaching Vahidi and his assets.

- Legal actions for intellectual property theft based on the fact that Iran’s nuclear program uses designs originally stolen from a European company, Urenco, by A.Q. Khan, the father of the Pakistani nuclear bomb.

127 Id.
128 Id.
130 Id.
131 Id.
It may also be possible to promote U.S. and allied national security objectives vis-à-vis Iran through action before international tribunals. For example:

- It may be possible to bring an action before the International Criminal Court (ICC) against Iranian Defense Minister Vahidi for his involvement in the AMIA bombing.\textsuperscript{133} Alan Baker, former legal adviser to the Foreign Ministry of Israel, has stated that Vahidi “carried out a crime which could probably be defined as a crime against humanity,” noting that “this has all the components of being a crime that is within the framework of the ICC.”\textsuperscript{134}

- Various international experts have called for pursuing legal action against Iranian President Ahmadinejad on the basis that his calls for the destruction of Israel are tantamount to incitement to genocide,\textsuperscript{135} which is prohibited by Article III (a) of the United Nations Convention on the Prevention and Punishment of the Crime of Genocide.\textsuperscript{136}

IV. CONCLUSION

The increasing legalization of international relations has made lawfare an increasingly powerful alternative to traditional military means to achieve operational objectives. Terrorist groups and their state sponsors are seizing on this development by making explicit and sometimes effective use of lawfare to achieve their operational objectives.

In contrast, the U.S. executive branch’s response to law’s potential as a tool for advancing military objectives has thus far been predominantly defensive. The U.S.’s advantage in sophisticated legal weapons has thus far been underutilized.

The remarkable impact of the limited deployment of lawfare against Iran to date indicates that lawfare, deployed systematically and effectively, may in some circumstances be able to save U.S. and foreign lives by signif-

\textsuperscript{133} Yaakov Lappin, Interpol: No warrant out for Iranian defense minister. Ahmad Vahidi wanted by Argentina for allegedly masterminding the 1994 Buenos Aires Jewish center bombing, Jerusalem Post, Sept. 8, 2009, at 5.

\textsuperscript{134} Id.


icantly advancing U.S. national security objectives that would otherwise require traditional warfare. These successes call into question the dominant paradigm in the scholarly literature regarding sanctions, which derides multilateral sanctions as predominantly ineffective and unilateral sanctions as almost always ineffective in a globalized economy.137 Perhaps the innovative types of lawfare-style sanctions described in this article represent a new breed of more effective sanctions than those derided in the scholarly literature.

In light of lawfare’s advantages over kinetic warfare, and the remarkable impact of the limited deployment of lawfare against Iran to date, strong consideration should be given to broadening lawfare’s application by the United States and its allies. Each of the types of lawfare identified by this article as being deployed against Iran in limited fashion could be replicated in additional sectors and applied to additional security challenges.

There is clearly room for much more vigorous deployment of state and local lawfare measures. For example, the fact that twenty-seven states have divested pension funds from companies doing business with Sudan and nineteen states have divested pension funds from companies doing business with Iran means there are twenty-three more states that still could divest from Sudan and thirty-three additional states that still could divest from Iran. In addition, Governor Pawlenty’s effectiveness in putting Essar to a choice between investing in Minnesota and building a refinery in Iran means that there may be merit in putting together a comprehensive list of where else in the United States Iran’s key business partners are seeking to invest and requesting subsidies and permits. Consideration could also be given to applying state and local lawfare measures to a broader set of target countries.

In light of the success of the Treasury Department’s unprecedented direct outreach to foreign banks and the success of the State Department’s subsequent similar direct outreach to foreign energy companies doing business with Iran, the Obama Administration, or a future administration, may decide to try to replicate in other sectors the willingness to use economic

137 See, e.g., DANIEL DREZNER, THE SANCTIONS PARADOX: ECONOMIC STATECRAFT AND INTERNATIONAL RELATIONS 10 (1999) (providing numerous quotes in which “pundits and policymakers have disparaged the use of sanctions in foreign policy” and noting that “this disdain mirrors the scholarly community’s consensus about sanctions”); DAVID BALDWIN, ECONOMIC STATECRAFT 51 (1985) (describing “the literature on economic statecraft” as characterized by “the nearly universal tendency to denigrate the utility of such tools of foreign policy.”) See also, e.g., Richard N. Haass, SANCTIONING MADNESS, Foreign Affairs, Nov/Dec. 1997, at 75 (“the problem with economic sanctions is that they frequently contribute little to American foreign policy goals while being costly and even counterproductive”); id. at 77 (“In a global economy, unilateral sanctions impose higher costs on American firms than on the target country”); Robert A. Pape, WHY ECONOMIC SANCTIONS DO NOT WORK, 22 Int’l Security 90–136 (1997).
and regulatory muscle to pursue national security objectives and the novel tactic of direct outreach to individual foreign private institutions. If so, foreign companies in exceptionally globalized, strategic, regulated and information-rich sectors such as mobile telecommunications, the internet, and transportation could be next in line. Before the U.S. government takes such steps, it should analyze and weigh very carefully both the risk posed by such measures to U.S. economic and regulatory preeminence in those sectors and the risk that such steps might set problematic precedents that could be used against the United States by current or future adversaries. Moves into additional sectors should be designed with an eye to minimizing those risks.

Finally, the creative use of civil litigation and international tribunals to achieve U.S. national security objectives is still at an early juncture. For example, the application against proliferators of the types of civil litigation tactics and precedents deployed against state sponsors of terrorism is still mostly at the conceptual stage, and the efforts to bring Iranian President Ahmadinejad before an international tribunal for incitement to genocide have yet to succeed. The potential for the United States to more effectively use civil litigation and international tribunals to achieve national security objectives traditionally achieved by military means merits further study by scholars, private practitioners, and government officials.

Lawfare’s success in its limited deployment against Iran demonstrates lawfare’s considerable potential as a tool for advancing U.S. national security objectives with far less bloodshed than traditional warfare. The U.S.’s advantage in sophisticated legal weapons should not remain underutilized.

---

138 For example, the United States depends heavily on Chinese purchases of American debt, a dependence which provides China with significant leverage over the United States. See, e.g., Keith Bradsher, China Losing Taste for Debt from the U.S., N.Y. TIMES, Jan. 8, 2009, at A1.
Resolution 2371 (2017)

Adopted by the Security Council at its 8019th meeting, on 5 August 2017

The Security Council,

Recalling its previous relevant resolutions, including resolution 825 (1993), resolution 1540 (2004), resolution 1695 (2006), resolution 1718 (2006), resolution 1874 (2009), resolution 1887 (2009), resolution 2087 (2013), resolution 2094 (2013), resolution 2270 (2016), resolution 2321 (2016), and resolution 2356 (2017), as well as the statements of its President of 6 October 2006 (S/PRST/2006/41), 13 April 2009 (S/PRST/2009/7) and 16 April 2012 (S/PRST/2012/13),

Reaffirming that proliferation of nuclear, chemical and biological weapons, as well as their means of delivery, constitutes a threat to international peace and security,

Expressing its gravest concern at the July 3 and July 28 of 2017 ballistic missile tests by the Democratic People’s Republic of Korea (“the DPRK”), which the DPRK has stated were tests of intercontinental ballistic missiles, in violation of resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), and 2356 (2017), and at the challenge such tests constitute to the Treaty on Non-Proliferation of Nuclear Weapons (“the NPT”) and to international efforts aimed at strengthening the global regime of non-proliferation of nuclear weapons, and the danger they pose to peace and stability in the region and beyond,

Underlining once again the importance that the DPRK respond to other security and humanitarian concerns of the international community,

Underlining also that measures imposed by this resolution are not intended to have adverse humanitarian consequences for the civilian population of the DPRK,

Expressing serious concern that the DPRK has continued to violate relevant Security Council resolutions through repeated launches and attempted launches of ballistic missiles, and noting that all such ballistic missile activities contribute to the DPRK’s development of nuclear weapons delivery systems and increase tension in the region and beyond,

Expressing continued concern that the DPRK is abusing the privileges and immunities accorded under the Vienna Conventions on Diplomatic and Consular Relations,
Expressing great concern that the DPRK’s prohibited arms sales have generated revenues that are diverted to the pursuit of nuclear weapons and ballistic missiles while DPRK citizens have unmet needs,

Expressing its gravest concern that the DPRK’s ongoing nuclear- and ballistic missile-related activities have further generated increased tension in the region and beyond, and determining that there continues to exist a clear threat to international peace and security,

Acting under Chapter VII of the Charter of the United Nations, and taking measures under its Article 41,

1. Condemns in the strongest terms the ballistic missile launches conducted by the DPRK on 3 July and 28 July of 2017, which the DPRK has stated were launches of intercontinental ballistic missiles, and which used ballistic missile technology in violation and flagrant disregard of the Security Council’s resolutions;

2. Reaffirms its decisions that the DPRK shall not conduct any further launches that use ballistic missile technology, nuclear tests, or any other provocation; shall suspend all activities related to its ballistic missile program and in this context re-establish its pre-existing commitments to a moratorium on missile launches; shall abandon all nuclear weapons and existing nuclear programs in a complete, verifiable and irreversible manner, and immediately cease all related activities; and shall abandon any other existing weapons of mass destruction and ballistic missile programs in a complete, verifiable and irreversible manner;

Designations

3. Decides that the measures specified in paragraph 8 (d) of resolution 1718 (2006) shall apply also to the individuals and entities listed in Annex I and II of this resolution and to any individuals or entities acting on their behalf or at their direction, and to entities owned or controlled by them, including through illicit means, and decides further that the measures specified in paragraph 8 (e) of resolution 1718 (2006) shall also apply to the individuals listed in Annex I of this resolution and to individuals acting on their behalf or at their direction;

4. Decides to adjust the measures imposed by paragraph 8 of resolution 1718 (2006) and this resolution through the designation of additional goods, directs the Committee to undertake its tasks to this effect and to report to the Security Council within fifteen days of adoption of this resolution, and further decides that, if the Committee has not acted, then the Security Council will complete action to adjust the measures within seven days of receiving that report;

5. Decides to adjust the measures imposed by paragraph 7 of resolution 2321 (2016) through the designation of additional conventional arms-related items, materials, equipment, goods, and technology, directs the Committee to undertake its tasks to this effect and to report to the Security Council within thirty days of adoption of this resolution, further decides that, if the Committee has not acted, then the Security Council will complete action to adjust the measures within seven days of receiving that report, and directs the Committee to update this list every 12 months;

Transportation

6. Decides that the Committee may designate vessels for which it has information indicating they are, or have been, related to activities prohibited by resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), or this resolution and all Member States shall prohibit the entry into their ports of such designated vessels, unless entry is required in the case of emergency or in the case of return to its port of origination, or unless the Committee
determines in advance that such entry is required for humanitarian purposes or any other purposes consistent with the objectives of resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), or this resolution;

7. Clarifies that the measures set forth in paragraph 20 of resolution 2270 (2016) and paragraph 9 of resolution 2321 (2016), requiring States to prohibit their nationals, persons subject to their jurisdiction and entities incorporated in their territory or subject to their jurisdiction from owning, leasing, operating any vessel flagged by the DPRK, without exception, unless the Committee approves on a case-by-case basis in advance, apply to chartering vessels flagged by the DPRK;

Sectoral

8. Decides that paragraph 26 of resolution 2321 (2016) shall be replaced by the following:

“Decides that the DPRK shall not supply, sell or transfer, directly or indirectly, from its territory or by its nationals or using its flag vessels or aircraft, coal, iron, and iron ore, and that all States shall prohibit the procurement of such material from the DPRK by their nationals, or using their flag vessels or aircraft, and whether or not originating in the territory of the DPRK, decides that for sales and transactions of iron and iron ore for which written contracts have been finalized prior to the adoption of this resolution, all States may allow those shipments to be imported into their territories up to 30 days from the date of adoption of this resolution with notification provided to the Committee containing details on those imports by no later than 45 days after the date of adoption of this resolution, and decides further that this provision shall not apply with respect to coal that the exporting State confirms on the basis of credible information has originated outside the DPRK and was transported through the DPRK solely for export from the Port of Rajin (Rason), provided that the exporting State notifies the Committee in advance and such transactions involving coal originating outside of the DPRK are unrelated to generating revenue for the DPRK’s nuclear or ballistic missile programs or other activities prohibited by resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), or this resolution;”

9. Decides that the DPRK shall not supply, sell or transfer, directly or indirectly, from its territory or by its nationals or using its flag vessels or aircraft, seafood (including fish, crustaceans, mollusks, and other aquatic invertebrates in all forms), and that all States shall prohibit the procurement of such items from the DPRK by their nationals, or using their flag vessels or aircraft, whether or not originating in the territory of the DPRK, and further decides that for sales and transactions of seafood (including fish, crustaceans, mollusks, and other aquatic invertebrates in all forms) for which written contracts have been finalized prior to the adoption of this resolution, all States may allow those shipments to be imported into their territories up to 30 days from the date of adoption of this resolution with notification provided to the Committee containing details on those imports by no later than 45 days after the date of adoption of this resolution;

10. Decides that the DPRK shall not supply, sell or transfer, directly or indirectly, from its territory or by its nationals or using its flag vessels or aircraft, lead and lead ore, and that all States shall prohibit the procurement of such items from the DPRK by their nationals, or using their flag vessels or aircraft, whether or not originating in the territory of the DPRK, and further decides that for sales and transactions of lead and lead ore for which written contracts have been finalized prior to the adoption of this resolution, all States may allow those shipments to be imported into their territories up to 30 days from the date of adoption of this resolution with
notification provided to the Committee containing details on those imports by no later than 45 days after the date of adoption of this resolution;

11. **Expresses concern** that DPRK nationals frequently work in other States for the purpose of generating foreign export earnings that the DPRK uses to support its prohibited nuclear and ballistic missile programs, **decides** that all Member States shall not exceed on any date after the date of adoption of this resolution the total number of work authorizations for DPRK nationals provided in their jurisdictions at the time of the adoption of this resolution unless the Committee approves on a case-by-case basis in advance that employment of additional DPRK nationals beyond the number of work authorizations provided in a member state’s jurisdiction at the time of the adoption of this resolution is required for the delivery of humanitarian assistance, denuclearization or any other purpose consistent with the objectives of resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), or this resolution;

**Financial**

12. **Decides** that States shall prohibit, by their nationals or in their territories, the opening of new joint ventures or cooperative entities with DPRK entities or individuals, or the expansion of existing joint ventures through additional investments, whether or not acting for or on behalf of the government of the DPRK, unless such joint ventures or cooperative entities have been approved by the Committee in advance on a case-by-case basis;

13. **Clarifies** that the prohibitions contained in paragraph 11 of resolution 2094 (2013) apply to clearing of funds through all Member States’ territories;

14. **Clarifies** that companies performing financial services commensurate with those provided by banks are considered financial institutions for the purposes of implementing paragraph 11 of resolution 2094 (2013), paragraphs 33 and 34 of resolution 2270 (2016), and paragraph 33 of resolution 2321 (2016);

**Chemical Weapons**

15. **Recalls** paragraph 24 of resolution 2270 (2016), **decides** that the DPRK shall not deploy or use chemical weapons, and **urgently calls upon** the DPRK to accede to the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and Their Destruction, and then to immediately comply with its provisions;

**Vienna Convention**

16. **Demands** that the DPRK fully comply with its obligations under the Vienna Convention on Diplomatic Relations and the Vienna Convention on Consular Relations;

**Impact on the People of the DPRK**

17. **Regrets** the DPRK’s massive diversion of its scarce resources toward its development of nuclear weapons and a number of expensive ballistic missile programs, **notes** the findings of the United Nations Office for the Coordination of Humanitarian Assistance that well over half of the people in the DPRK suffer from major insecurities in food and medical care, including a very large number of pregnant and lactating women and under-five children who are at risk of malnutrition and nearly a quarter of its total population suffering from chronic malnutrition, and, in this context, **expresses** deep concern at the grave hardship to which the people in the DPRK are subjected;
Sanctions Implementation

18. Decides that Member States shall report to the Security Council within ninety days of the adoption of this resolution, and thereafter upon request by the Committee, on concrete measures they have taken in order to implement effectively the provisions of this resolution, requests the Panel of Experts, in cooperation with other United Nations sanctions monitoring groups, to continue its efforts to assist Member States in preparing and submitting such reports in a timely manner;

19. Calls upon all Member States to redouble efforts to implement in full the measures in resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), and 2356 (2017), and to cooperate with each other in doing so, particularly with respect to inspecting, detecting and seizing items the transfer of which is prohibited by these resolutions;

20. Decides that the mandate of the Committee, as set out in paragraph 12 of resolution 1718 (2006), shall apply with respect to the measures imposed in this resolution and further decides that the mandate of the Panel of Experts, as specified in paragraph 26 of resolution 1874 (2009) and modified in paragraph 1 of resolution 2345 (2017), shall also apply with respect to the measures imposed in this resolution;

21. Decides to authorize all Member States to, and that all Member States shall, seize and dispose (such as through destruction, rendering inoperable or unusable, storage, or transferring to a State other than the originating or destination States for disposal) of items the supply, sale, transfer, or export of which is prohibited by resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), or this resolution that are identified in inspections, in a manner that is not inconsistent with their obligations under applicable Security Council resolutions, including resolution 1540 (2004), as well as any obligations of parties to the NPT, the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Development of 29 April 1997, and the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction of 10 April 1972;

22. Emphasizes the importance of all States, including the DPRK, taking the necessary measures to ensure that no claim shall lie at the instance of the DPRK, or of any person or entity in the DPRK, or of persons or entities designated for measures set forth in resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), or this resolution, or any person claiming through or for the benefit of any such person or entity, in connection with any contract or other transaction where its performance was prevented by reason of the measures imposed by this resolution or previous resolutions;

23. Requests that Interpol issue Special Notices with respect to designated individuals, and directs the Committee to work with Interpol to develop the appropriate arrangements to do so;

24. Requests the Secretary-General to provide additional analytical resources needed to the Panel of Experts established pursuant to resolution 1874 (2009) to strengthen its ability to analyze the DPRK’s sanctions violation and evasion activities;

Political

25. Reiterates its deep concern at the grave hardship that the people in the DPRK are subjected to, condemns the DPRK for pursuing nuclear weapons and ballistic missiles instead of the welfare of its people while people in the DPRK have
great unmet needs, and **emphasizes** the necessity of the DPRK respecting and ensuring the welfare and inherent dignity of people in the DPRK;

26. **Reaffirms** that the measures imposed by resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), and this resolution are not intended to have adverse humanitarian consequences for the civilian population of the DPRK or to affect negatively or restrict those activities, including economic activities and cooperation, food aid and humanitarian assistance, that are not prohibited by resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017) and this resolution, and the work of international and non-governmental organizations carrying out assistance and relief activities in the DPRK for the benefit of the civilian population of the DPRK and **decides** that the Committee may, on a case-by-case basis, exempt any activity from the measures imposed by these resolutions if the committee determines that such an exemption is necessary to facilitate the work of such organizations in the DPRK or for any other purpose consistent with the objectives of these resolutions, and **further decides** that the measures specified in paragraph 8 (d) of resolution 1718 (2006) shall not apply with respect to financial transactions with the DPRK Foreign Trade Bank or the Korea National Insurance Corporation if such transactions are solely for the operation of diplomatic or consular missions in the DPRK or humanitarian assistance activities that are undertaken by, or in coordination with, the United Nations;

27. **Reaffirms** its support for the Six Party Talks, **calls** for their resumption, and **reiterates** its support for the commitments set forth in the Joint Statement of 19 September 2005 issued by China, the DPRK, Japan, the Republic of Korea, the Russian Federation, and the United States, including that the goal of the Six-Party Talks is the verifiable denuclearization of the Korean Peninsula in a peaceful manner, that the United States and the DPRK undertook to respect each other’s sovereignty and exist peacefully together, that the Six Parties undertook to promote economic cooperation, and all other relevant commitments;

28. **Reiterates** the importance of maintaining peace and stability on the Korean Peninsula and in north-east Asia at large, and **expresses** its commitment to a peaceful, diplomatic, and political solution to the situation and welcomes efforts by the Council members as well as other States to facilitate a peaceful and comprehensive solution through dialogue and stresses the importance of working to reduce tensions in the Korean Peninsula and beyond;

29. **Affirms** that it shall keep the DPRK’s actions under continuous review and is prepared to strengthen, modify, suspend or lift the measures as may be needed in light of the DPRK’s compliance, and, in this regard, **expresses its determination** to take further significant measures in the event of a further DPRK nuclear test or launch;

30. **Decides** to remain seized of the matter.
Annex I

Travel Ban/Asset Freeze (Individuals)

1. CHOE CHUN YONG
   a. Description: Representative for Ilsim International Bank, which is affiliated with the DPRK military and has a close relationship with the Korea Kwangson Banking Corporation. Ilsim International Bank has attempted to evade United Nations sanctions.
   b. A.K.A.: Ch’oe Ch’un-yo’ng
   c. Identifiers: Nationality: DPRK; Passport no.: 654410078; Gender: male

2. HAN JANG SU
   a. Description: Chief Representative of the Foreign Trade Bank.
   b. A.K.A.: Chang-Su Han
   c. Identifiers: DOB: November 08, 1969; POB: Pyongyang, DPRK; Nationality: DPRK; Passport no.: 745420176, expires on October 19, 2020; Gender: male

3. JANG SONG CHOL
   a. Description: Jang Song Chol is a Korea Mining Development Corporation (KOMID) representative overseas.
   b. A.K.A.: n/a
   c. Identifiers: DOB: 12 March 1967; Nationality: DPRK

4. JANG SUNG NAM
   a. Description: Chief of an overseas Tangun Trading Corporation branch, which is primarily responsible for the procurement of commodities and technologies to support the DPRK’s defense research and development programs.
   b. A.K.A.: n/a
   c. Identifiers: DOB: July 14, 1970; Nationality: DPRK; Passport no.: 563120368, issued on March 22, 2013; Passport expiration date: March 22, 2018; Gender: male

5. JO CHOL SONG
   a. Description: Deputy Representative for the Korea Kwangson Banking Corporation, which provides financial services in support to Tanchon Commercial Bank and Korea Hyoksin Trading, a subordinate entity of Korea Ryongbong General Corporation.
   b. A.K.A.: Cho Ch’o’l-so’ng
   c. Identifiers: DOB: September 25, 1984; Nationality: DPRK; Passport no.: 654320502, expires on September 16, 2019; Gender: male

6. KANG CHOL SU
   a. Description: Official for Korea Ryongbong General Corporation, which specializes in acquisition for the DPRK’s defense industries and support for the DPRK’s military-related overseas sales. Its procurements also likely support the DPRK’s chemical weapons program.
b.  
  A.K.A.: n/a

c.  
  **Identifiers:** DOB: February 13, 1969; Nationality: DPRK; Passport no.: 472234895

7. KIM MUN CHOL

a.  
  **Description:** Representative for Korea United Development Bank.

b.  
  A.K.A.: Kim Mun-ch’o’l

c.  
  **Identifiers:** DOB: March 25, 1957; Nationality: DPRK

8. KIM NAM UNG

a.  
  **Description:** Representative for Ilsim International Bank, which is affiliated with the DPRK military and has a close relationship with the Korea Kwangson Banking Corporation. Ilsim International Bank has attempted to evade United Nations sanctions.

b.  
  A.K.A.: n/a

c.  
  **Identifiers:** Nationality: DPRK; Passport no.: 654110043

9. PAK IL KYU

a.  
  **Description:** Official for Korea Ryonbong General Corporation, which specializes in acquisition for DPRK’s defense industries and support to Pyongyang’s military-related sales. Its procurements also likely support the DPRK’s chemical weapons program.

b.  
  A.K.A.: Pak Il-Gyu

c.  
  **Identifiers:** Nationality: DPRK; Passport no.: 563120235; Gender: male

**List Update for Aliases:**

- JANG BOM SU (KPi.016) — *New AKA:* Jang Hyon U with date of birth 22 February 1958 and diplomatic passport number 836110034, which expires on 1 January 2020.

- JON MYONG GUK (KPi.018) — *New AKA:* Jon Yong Sang with date of birth 25 August 1976 and diplomatic passport number 836110035, which expires on 1 January 2020.
Annex II

Asset Freeze (Entities)

1. FOREIGN TRADE BANK (FTB)
   a. *Description*: Foreign Trade Bank is a state-owned bank and acts as the DPRK’s primary foreign exchange bank and has provided key financial support to the Korea Kwangson Banking Corporation.
   b. *AKA*: n/a
   c. *Location*: FTB Building, Jungsong-dong, Central District, Pyongyang, DPRK

2. KOREAN NATIONAL INSURANCE COMPANY (KNIC)
   a. *Description*: The Korean National Insurance Company is a DPRK financial and insurance company and is affiliated with Office 39.
   b. *AKA*: Korea Foreign Insurance Company
   c. *Location*: Central District, Pyongyang, DPRK

3. KORYO CREDIT DEVELOPMENT BANK
   a. *Description*: Koryo Credit Development Bank operates in the financial services industry in the DPRK’s economy.
   b. *AKA*: Daesong Credit Development Bank; Koryo Global Credit Bank; Koryo Global Trust Bank
   c. *Location*: Pyongyang, DPRK

4. MANSUDAЕ OVERSEAS PROJECT GROUP OF COMPANIES
   a. *Description*: Mansudae Overseas Project Group of Companies engaged in, facilitated, or was responsible for the exportation of workers from the DPRK to other nations for construction-related activities including for statues and monuments to generate revenue for the Government of the DPRK or the Workers’ Party of Korea. The Mansudae Overseas Project Group of Companies has been reported to conduct business in countries in Africa and Southeast Asia including Algeria, Angola, Botswana, Benin, Cambodia, Chad, the Democratic Republic of the Congo, Equatorial Guinea, Malaysia, Mozambique, Madagascar, Namibia, Syria, Togo, and Zimbabwe.
   b. *AKA*: Mansudae Art Studio
   c. *Location*: Pyongyang, DPRK
Resolution 2375 (2017)

Adopted by the Security Council at its 8042nd meeting, on 11 September 2017

The Security Council,


Reaffirming that proliferation of nuclear, chemical and biological weapons, as well as their means of delivery, constitutes a threat to international peace and security,

Expressing its gravest concern at the nuclear test by the Democratic People's Republic of Korea (“the DPRK”) on September 2, 2017 in violation of resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), and 2371 (2017) and at the challenge such a test constitutes to the Treaty on Non-Proliferation of Nuclear Weapons (“the NPT”) and to international efforts aimed at strengthening the global regime of non-proliferation of nuclear weapons, and the danger it poses to peace and stability in the region and beyond,

Underlining once again the importance that the DPRK respond to other security and humanitarian concerns of the international community and expressing great concern that the DPRK continues to develop nuclear weapons and ballistic missiles by diverting critically needed resources away from the people in the DPRK who have great unmet needs,

Expressing its gravest concern that the DPRK’s ongoing nuclear- and ballistic missile-related activities have destabilized the region and beyond, and determining that there continues to exist a clear threat to international peace and security,

Underscoring its concern that developments on the Korean Peninsula could have dangerous, large-scale regional security implications,

Underscoring its commitment to the sovereignty, territorial integrity, and political independence of all States in accordance with the Charter, and recalling the purposes and principles of the Charter of the United Nations,
Expressing also its desire for a peaceful and diplomatic solution to the situation, and reiterating its welcoming of efforts by Council members as well as other Member States to facilitate a peaceful and comprehensive solution through dialogue,

Underlining the need to ensure international peace and security, and ensure lasting stability in north-east Asia at large and to resolve the situation through peaceful, diplomatic and political means,

Acting under Chapter VII of the Charter of the United Nations, and taking measures under its Article 41,

1. Condemns in the strongest terms the nuclear test conducted by the DPRK on September 2 of 2017 in violation and flagrant disregard of the Security Council’s resolutions;

2. Reaffirms its decisions that the DPRK shall not conduct any further launches that use ballistic missile technology, nuclear tests, or any other provocation; shall immediately suspend all activities related to its ballistic missile program and in this context re-establish its pre-existing commitments to a moratorium on all missile launches; shall immediately abandon all nuclear weapons and existing nuclear programs in a complete, verifiable and irreversible manner, and immediately cease all related activities; and shall abandon any other existing weapons of mass destruction and ballistic missile programs in a complete, verifiable and irreversible manner;

Designations

3. Decides that the measures specified in paragraph 8 (d) of resolution 1718 (2006) shall apply also to the individual and entities listed in Annex I and II of this resolution and to any individuals or entities acting on their behalf or at their direction, and to entities owned or controlled by them, including through illicit means, and decides further that the measures specified in paragraph 8 (e) of resolution 1718 (2006) shall also apply to the individual listed in Annex I of this resolution and to individuals acting on their behalf or at their direction;

4. Decides to adjust the measures imposed by paragraph 8 of resolution 1718 (2006) through the designation of additional WMD-related dual-use items, materials, equipment, goods, and technology, directs the Committee to undertake its tasks to this effect and to report to the Security Council within fifteen days of adoption of this resolution, and further decides that, if the Committee has not acted, then the Security Council will complete action to adjust the measures within seven days of receiving that report, and directs the Committee to regularly update this list every twelve months;

5. Decides to adjust the measures imposed by paragraph 8 (a), 8 (b) and 8 (c) of resolution 1718 (2006) through the designation of additional conventional arms-related items, materials, equipment, goods, and technology, directs the Committee to undertake its tasks to this effect and to report to the Security Council within fifteen days of adoption of this resolution, and further decides that, if the Committee has not acted, then the Security Council will complete action to adjust the measures within seven days of receiving that report, and directs the Committee to regularly update this list every twelve months;

6. Decides to apply the measures imposed by paragraph 6 of resolution 2371 (2016) on vessels transporting prohibited items from the DPRK, directs the Committee to designate these vessels and to report to the Security Council within fifteen days of adoption of this resolution, further decides that, if the Committee has not acted, then the Security Council will complete action to adjust the measures within
seven days of receiving that report, and directs the Committee to regularly update this list when it is informed of additional violations;

**Maritime Interdiction of Cargo Vessels**

7. Calls upon all Member States to inspect vessels with the consent of the flag State, on the high seas, if they have information that provides reasonable grounds to believe that the cargo of such vessels contains items the supply, sale, transfer or export of which is prohibited by resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), 2371 (2017) or this resolution, for the purpose of ensuring strict implementation of those provisions;

8. Calls upon all States to cooperate with inspections pursuant to paragraph 7 above, and, if the flag State does not consent to inspection on the high seas, decides that the flag State shall direct the vessel to proceed to an appropriate and convenient port for the required inspection by the local authorities pursuant to paragraph 18 of resolution 2270 (2016), and decides further that, if a flag State neither consents to inspection on the high seas nor directs the vessel to proceed to an appropriate and convenient port for the required inspection, or if the vessel refuses to comply with flag State direction to permit inspection on the high seas or to proceed to such a port, then the Committee shall consider designating the vessel for the measures imposed in paragraph 8 (d) of resolution 1718 (2006) and paragraph 12 of resolution 2321 (2016) and the flag State shall immediately deregister that vessel provided that such designation has been made by the Committee;

9. Requires any Member State, when it does not receive the cooperation of a flag State of a vessel pursuant to paragraph 8 above, to submit promptly to the Committee a report containing relevant details regarding the incident, the vessel and the flag State, and requests the Committee to release on a regular basis information regarding these vessels and flag States involved;

10. Affirms that paragraph 7 contemplates only inspections carried out by warships and other ships or aircraft clearly marked and identifiable as being on government service and authorized to that effect, and underscores that it does not apply with respect to inspection of vessels entitled to sovereign immunity under international law;

11. Decides that all Member States shall prohibit their nationals, persons subject to their jurisdiction, entities incorporated in their territory or subject to their jurisdiction, and vessels flying their flag, from facilitating or engaging in ship-to-ship transfers to or from DPRK-flagged vessels of any goods or items that are being supplied, sold, or transferred to or from the DPRK;

12. Affirms that paragraphs 7, 8 and 9 apply only with respect to the situation in the DPRK and shall not affect the rights, obligations, or responsibilities of Member States under international law, including any rights or obligations under the United Nations Convention on the Law of the Sea of 10 December 1982, with respect to any other situation and underscores in particular that this resolution shall not be considered as establishing customary international law;

**Sectoral**

13. Decides that all Member States shall prohibit the direct or indirect supply, sale or transfer to the DPRK, through their territories or by their nationals, or using their flag vessels or aircraft, and whether or not originating in their territories, of all condensates and natural gas liquids, and decides that the DPRK shall not procure such materials;
14. Decides that all Member States shall prohibit the direct or indirect supply, sale or transfer to the DPRK, through their territories or by their nationals, or using their flag vessels or aircraft, and whether or not originating in their territories, of all refined petroleum products, decides that the DPRK shall not procure such products, decides that this provision shall not apply with respect to procurement by the DPRK or the direct or indirect supply, sale or transfer to the DPRK, through their territories or by their nationals, or using their flag vessels or aircraft, and whether or not originating in their territories, of refined petroleum products in the amount of up to 500,000 barrels during an initial period of three months beginning on 1 October 2017 and ending on 31 December 2017, and refined petroleum products in the amount of up to 2,000,000 barrels per year during a period of twelve months beginning on 1 January 2018 and annually thereafter, provided that (a) the Member State notifies the Committee every thirty days of the amount of such supply, sale, or transfer to the DPRK of refined petroleum products along with information about all the parties to the transaction, (b) the supply, sale, or transfer of refined petroleum products involve no individuals or entities that are associated with the DPRK’s nuclear or ballistic missile programmes or other activities prohibited by resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), 2371 (2017) or this resolution, including designated individuals or entities, or individuals or entities acting on their behalf or at their direction, or entities owned or controlled by them, directly or indirectly, or individuals or entities assisting in the evasion of sanctions, and (c) the supply, sale, or transfer of refined petroleum products are exclusively for livelihood purposes of DPRK nationals and unrelated to generating revenue for the DPRK’s nuclear or ballistic missile programmes or other activities prohibited by resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), 2371 (2017) or this resolution, directs the Committee Secretary to notify all Member States when an aggregate amount of refined petroleum products sold, supplied, or transferred to the DPRK of 75 per cent of the aggregate amount for the period between 1 October 2017 and 31 December 2017 has been reached, and again notify all Member States when 90 percent and 95 percent of such aggregate amount has been reached, directs the Committee Secretary beginning on 1 January 2018 to notify all Member States when an aggregate amount of refined petroleum products sold, supplied, or transferred to the DPRK of 75 per cent of the aggregate yearly amounts have been reached, also directs the Committee Secretary beginning on 1 January 2018 to notify all Member States when an aggregate amount of refined petroleum products sold, supplied, or transferred to the DPRK of 90 per cent of the aggregate yearly amounts have been reached, and further directs the Committee Secretary beginning on 1 January 2018 to notify all Member States when an aggregate amount of refined petroleum products sold, supplied, or transferred to the DPRK of 95 per cent of the aggregate yearly amounts have been reached and to inform them that they must immediately cease selling, supplying, or transferring refined petroleum products to the DPRK for the remainder of the year, directs the Committee to make publicly available on its website the total amount of refined petroleum products sold, supplied, or transferred to the DPRK by month and by source country, directs the Committee to update this information on a real-time basis as it receives notifications from Member States, calls upon all Member States to regularly review this website to comply with the annual limits for refined petroleum products established by this provision, directs the Panel of Experts to closely monitor the implementation efforts of all Member States to provide assistance and ensure full and global compliance, and requests the Secretary-General to make the necessary arrangements to this effect and provide additional resources in this regard;

15. Decides that all Member States shall not supply, sell, or transfer to the DPRK in any period of twelve months after the date of adoption of this resolution an amount of crude oil that is in excess of the amount that the Member State supplied,
sold or transferred in the period of twelve months prior to adoption of this resolution, unless the Committee approves in advance on a case-by-case basis a shipment of crude oil is exclusively for livelihood purposes of DPRK nationals and unrelated to the DPRK’s nuclear or ballistic missile programmes or other activities prohibited by resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), 2371 (2017) or this resolution;

16. **Decides** that the DPRK shall not supply, sell or transfer, directly or indirectly, from its territory or by its nationals or using its flag vessels or aircraft, textiles (including but not limited to fabrics and partially or fully completed apparel products), and that all States shall prohibit the procurement of such items from the DPRK by their nationals, or using their flag vessels or aircraft, whether or not originating in the territory of the DPRK, unless the Committee approves on a case-by-case basis in advance, and further *decides* that for such sales, supplies, and transfers of textiles (including but not limited to fabrics and partially or fully completed apparel products) for which written contracts have been finalized prior to the adoption of this resolution, all States may allow those shipments to be imported into their territories up to 90 days from the date of adoption of this resolution with notification provided to the Committee containing details on those imports by no later than 135 days after the date of adoption of this resolution;

17. **Decides** that all Member States shall not provide work authorizations for DPRK nationals in their jurisdictions in connection with admission to their territories unless the Committee determines on a case-by-case basis in advance that employment of DPRK nationals in a member state’s jurisdiction is required for the delivery of humanitarian assistance, denuclearization or any other purpose consistent with the objectives of resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), 2371 (2017), or this resolution, and *decides* that this provision shall not apply with respect to work authorizations for which written contracts have been finalized prior to the adoption of this resolution;

**Joint Ventures**

18. **Decides** that States shall prohibit, by their nationals or in their territories, the opening, maintenance, and operation of all joint ventures or cooperative entities, new and existing, with DPRK entities or individuals, whether or not acting for or on behalf of the government of the DPRK, unless such joint ventures or cooperative entities, in particular those that are non-commercial, public utility infrastructure projects not generating profit, have been approved by the Committee in advance on a case-by-case basis, *further decides* that States shall close any such existing joint venture or cooperative entity within 120 days of the adoption of this resolution if such joint venture or cooperative entity has not been approved by the Committee on a case-by-case basis, and States shall close any such existing joint venture or cooperative entity within 120 days after the Committee has denied a request for approval, and *decides* that this provision shall not apply with respect to existing China-DPRK hydroelectric power infrastructure projects and the Russia-DPRK Rajin-Khasan port and rail project solely to export Russia-origin coal as permitted by paragraph 8 of resolution 2371 (2017);

**Sanctions Implementation**

19. **Decides** that Member States shall report to the Security Council within ninety days of the adoption of this resolution, and thereafter upon request by the Committee, on concrete measures they have taken in order to implement effectively the provisions of this resolution, *requests* the Panel of Experts, in cooperation with other UN sanctions monitoring groups, to continue its efforts to assist Member States in preparing and submitting such reports in a timely manner;
20. **Calls upon** all Member States to redouble efforts to implement in full the measures in resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), 2371 (2017), and this resolution and to cooperate with each other in doing so, particularly with respect to inspecting, detecting and seizing items the transfer of which is prohibited by these resolutions;

21. **Decides** that the mandate of the Committee, as set out in paragraph 12 of resolution 1718 (2006), shall apply with respect to the measures imposed in this resolution and **further decides** that the mandate of the Panel of Experts, as specified in paragraph 26 of resolution 1874 (2009) and modified in paragraph 1 of resolution 2345 (2017), shall also apply with respect to the measures imposed in this resolution;

22. **Decides** to authorize all Member States to, and that all Member States shall, seize and dispose (such as through destruction, rendering inoperable or unusable, storage, or transferring to a State other than the originating or destination States for disposal) of items the supply, sale, transfer, or export of which is prohibited by resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), 2371 (2017), or this resolution that are identified in inspections, in a manner that is not inconsistent with their obligations under applicable Security Council resolutions, including resolution 1540 (2004), as well as any obligations of parties to the NPT, the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Development of 29 April 1997, and the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction of 10 April 1972;

23. **Emphasizes** the importance of all States, including the DPRK, taking the necessary measures to ensure that no claim shall lie at the instance of the DPRK, or of any person or entity in the DPRK, or of persons or entities designated for measures set forth in resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), 2371 (2017), or this resolution, that are in connection with any contract or other transaction where its performance was prevented by reason of the measures imposed by this resolution or previous resolutions;

**Political**

24. **Reiterates** its deep concern at the grave hardship that the people in the DPRK are subjected to, **condemns** the DPRK for pursuing nuclear weapons and ballistic missiles instead of the welfare of its people while people in the DPRK have great unmet needs, and **emphasizes** the necessity of the DPRK respecting and ensuring the welfare and inherent dignity of people in the DPRK;

25. **Regrets** the DPRK’s massive diversion of its scarce resources toward its development of nuclear weapons and a number of expensive ballistic missile programs, **notes** the findings of the United Nations Office for the Coordination of Humanitarian Assistance that well over half of the people in the DPRK suffer from major insecurities in food and medical care, including a very large number of pregnant and lactating women and under-five children who are at risk of malnutrition and nearly a quarter of its total population suffering from chronic malnutrition, and, in this context, **expresses** deep concern at the grave hardship to which the people in the DPRK are subjected;

26. **Reaffirms** that the measures imposed by resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), 2371 (2017) and this resolution are not intended to have adverse humanitarian consequences for the civilian population of the DPRK or to affect negatively or restrict those activities, including economic activities and cooperation, food aid and
S/RES/2375 (2017)

humanitarian assistance, that are not prohibited by resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), 2371 (2017) and this resolution, and the work of international and non-governmental organizations carrying out assistance and relief activities in the DPRK for the benefit of the civilian population of the DPRK and decides that the Committee may, on a case-by-case basis, exempt any activity from the measures imposed by these resolutions if the committee determines that such an exemption is necessary to facilitate the work of such organizations in the DPRK or for any other purpose consistent with the objectives of these resolutions;

27. Emphasizes that all Member States should comply with the provisions of paragraphs 8 (a) (iii) and 8 (d) of resolution 1718 (2006) without prejudice to the activities of the diplomatic missions in the DPRK pursuant to the Vienna Convention on Diplomatic Relations;

28. Reaffirms its support for the Six Party Talks, calls for their resumption, and reiterates its support for the commitments set forth in the Joint Statement of 19 September 2005 issued by China, the DPRK, Japan, the Republic of Korea, the Russian Federation, and the United States, including that the goal of the Six-Party Talks is the verifiable denuclearization of the Korean Peninsula in a peaceful manner, that the United States and the DPRK undertook to respect each other’s sovereignty and exist peacefully together, that the Six Parties undertook to promote economic cooperation, and all other relevant commitments;

29. Reiterates the importance of maintaining peace and stability on the Korean Peninsula and in north-east Asia at large, expresses its commitment to a peaceful, diplomatic, and political solution to the situation, and welcomes efforts by the Council members as well as other States to facilitate a peaceful and comprehensive solution through dialogue and stresses the importance of working to reduce tensions in the Korean Peninsula and beyond;

30. Urges further work to reduce tensions so as to advance the prospects for a comprehensive settlement;

31. Underscores the imperative of achieving the goal of complete, verifiable and irreversible denuclearization of the Korean Peninsula in a peaceful manner;

32. Affirms that it shall keep the DPRK’s actions under continuous review and is prepared to strengthen, modify, suspend or lift the measures as may be needed in light of the DPRK’s compliance, and, in this regard, expresses its determination to take further significant measures in the event of a further DPRK nuclear test or launch;

33. Decides to remain seized of the matter.
Annex I

Travel Ban/Asset Freeze (Individuals)

1. PAK YONG SIK
   a. *Description:* Pak Yong Sik is a member of the Workers’ Party of Korea Central Military Commission, which is responsible for the development and implementation of the Workers’ Party of Korea military policies, commands and controls the DPRK’s military, and helps direct the country’s military defense industries.
   b. *AKA:* n/a
   c. *Identifiers:* YOB: 1950; Nationality: DPRK
Annex II

Asset Freeze (Entities)

1. CENTRAL MILITARY COMMISSION OF THE WORKERS’ PARTY OF KOREA (CMC)
   a. Description: The Central Military Commission is responsible for the development and implementation of the Workers’ Party of Korea’s military policies, commands and controls the DPRK’s military, and directs the country’s military defense industries in coordination with the State Affairs Commission.
   b. AKA: n/a
   c. Location: Pyongyang, DPRK

2. ORGANIZATION AND GUIDANCE DEPARTMENT (OGD)
   a. Description: The Organization and Guidance Department is a very powerful body of the Worker’s Party of Korea. It directs key personnel appointments for the Workers’ Party of Korea, the DPRK’s military, and the DPRK’s government administration. It also purports to control the political affairs of all of the DPRK and is instrumental in implementing the DPRK’s censorship policies.
   b. AKA: n/a
   c. Location: DPRK

3. PROPAGANDA AND AGITATION DEPARTMENT (PAD)
   a. Description: The Propaganda and Agitation Department has full control over the media, which it uses as a tool to control the public on behalf of the DPRK leadership. The Propaganda and Agitation Department also engages in or is responsible for censorship by the Government of the DPRK, including newspaper and broadcast censorship.
   b. AKA: n/a
   c. Location: Pyongyang, DPRK
NASA finds ingredients for life spewing out of Saturn’s icy moon Enceladus

By Sarah Kaplan  April 13

The geysers of Saturn's moon Enceladus are gushing food for life, scientists say.

Researchers report Thursday in the journal Science that the jets of ice and gas coming from the moon's south pole contain molecular hydrogen, a chemical characteristic of hydrothermal activity. On Earth, hydrogen provides fuel for communities of organisms that live around vents on the seafloor. Its presence on Saturn's icy moon suggests that this alien world, which harbors a saltwater ocean encased in a frozen crust, has the right conditions to give rise to microbial life.

"For a microbiologist thinking about energy for microbes, hydrogen is like the gold coin of energy currency," said Peter Girguis, a deep sea biologist at Harvard University who was not involved in the research. "If you had to have one thing, one chemical compound, coming out of a vent that would lead you to think there's energy to support microbial life, hydrogen is at the top of that list."

"It makes the Enceladus ocean seem a heck of a lot more habitable than we were thinking yesterday," agreed Ariel Anbar, an astrobiologist at Arizona State University. "And wouldn’t we like to know, is there life living there?"

Everything scientists know about biology on Earth suggests that life is irrepressible. It thrives in clouds, in caves, in lakes of meltwater buried half a mile beneath the ice sheets of Antarctica, in boiling water plumes that gush from the ocean's deepest, darkest depths. Almost no environment is too extreme, as long as water, organic molecules and a bit of energy are available for organisms to exploit.

Enceladus (pronounced “en-SELL-a-dis”) provides all three. It's looking more and more like the most habitable spot in our solar system beyond Earth, and scientists' best target yet in the search for alien organisms.

And it might not be alone. Images from the Hubble Space Telescope suggest that plumes much like those on Enceladus are also spewing from Jupiter's moon Europa, NASA announced today.
Like Enceladus, Europa harbors a subsurface saltwater ocean and could contain organic molecules. NASA hopes that Europa's geyser plumes are likewise connected to the moon's watery interior. In the coming decade, the space agency will send a probe called the Europa Clipper to seek signs of life on Jupiter's moon by flying through those plumes.

“In the NASA strategy for searching for life, the key ingredients have always been water, building blocks like carbon, oxygen, nitrogen ... and a source of energy,” said Mary Voytek, a senior scientist for astrobiology at NASA who was not involved in the research. Knowing that two worlds in the solar system might meet these requirements, “it’s very possible that we have life out on one of those moons,” Voytek said.

Enceladus's geyser plumes have made it a target in the search for extraterrestrial organisms ever since the NASA space probe Cassini detected them in 2005. The plumes are rich with water and organic molecules, and the force with which they gush from the surface suggests that they are driven by a hydrothermal system 2½ times as powerful as the one that powers Yellowstone’s geysers and bubbling hot springs. They are also physical evidence of the water in the moon's interior, which is heated by the gravitational pull of Saturn.

In October 2015, Cassini flew deeper into the geysers than it ever had before, skimming a mere 30 miles above the moon’s surface. The probe trapped particles from the plume inside its Ion Neutral Mass Spectrometer — a “sniffing” instrument that sorts material into its component parts based on mass — and analyzed the icy spray.

The results suggest that the geysers contain a surprising ratio of molecular hydrogen, carbon dioxide and methane. The molecules are in “thermodynamic disequilibrium,” the researchers say; that is, they're chemically out of whack. Molecular hydrogen (a compound made of two hydrogen atoms) is a very volatile gas, and is not easily trapped on a small, icy world like Enceladus. Its presence in the geyser plume indicates that there are processes beneath the surface constantly replenishing the supply of molecular hydrogen.

The paper's authors examined a number of possible reasons for this chemical imbalance in their paper. The most likely explanation, they conclude, is something called serpenitinization. As hot water from Enceladus’s ocean flows through cracks in the seafloor, it reacts with the iron-rich rock to form molecular hydrogen.

This exact phenomenon is known to happen around Earth's hydrothermal vents, where it fuels entire ecosystems of chemosynthetic organisms. Instead of deriving energy from the light of the sun, as photosynthetic plants do, these creatures feed on chemical imbalances. They power themselves by getting hydrogen to react with carbon dioxide to form methane, a process called methanogenesis, just as a lightbulb is powered by electric charges moving across a circuit.

Methanogenesis is one of the oldest metabolic processes on the planet. It predates photosynthesis; it may even have powered Earth's very first life. The fact that Enceladus produces the same chemical imbalances that drive chemosynthetic life on Earth is intriguing.

“But it's not necessarily an indication for or against life” on Saturn's moon, cautioned co-author Hunter Waite of the Southwest Research Institute in Texas (SWRI).
Waite compared the surplus of molecular hydrogen on Enceladus to a stack of pizzas piled up outside a house. On the one hand, if there was anyone living in the house, you would think that the inhabitants would be eating it. The fact that the hydrogen persists could be evidence that there are no microbes around to use it for fuel. On the other hand, maybe there's so much pizza arriving every day that the residents can't keep up. There may be other factors limiting how much hydrogen the hypothetical microbes can process, allowing some molecules to escape up to the surface.

If there is life on Enceladus, the scientists know how much energy is available for it to consume based on the ratio of hydrogen in the plume. Co-author Christopher Glein, a geochemist at SWRI, called it “the first assessment of the calorie count in an alien ocean.” He and his colleagues found that the moon’s hydrothermal activity supplies more than enough energy to power a chemosynthetic ecosystem — the equivalent of 300 pizzas per hour.

Clearly, Enceladus's sea floor is a veritable hydrogen pizza party. But is anyone eating?

“We're going to have to go back with new missions and more focused instrumentation to answer that question,” Waite said.

Cassini won't have any more opportunities to sample the geyser plumes. After orbiting Saturn for more than a decade, the spacecraft is scheduled to start dives between the planet and its rings next week. In September, Cassini will plunge straight into Saturn, burning up almost as soon as it hits the gas giant’s atmosphere. The command sequence for this final mission was transmitted to the probe by NASA’s Deep Space Network on Tuesday.

It’s Enceladus's fault that Cassini must die — NASA doesn’t want to risk the spacecraft inadvertently contaminating the potentially habitable moon, so they cannot leave it hanging out in space after it runs out of fuel.

Yet the space probe has already dramatically exceeded scientists’ expectations. When Cassini launched toward Saturn in 1997, NASA didn’t even know that Enceladus had geysers, let alone an ocean that could harbor life, and the spacecraft wasn’t equipped with instruments that could test for biomarkers (the instrument used in this study was initially designed to study a different moon entirely). If scientists want to search for life on Enceladus in earnest, they will need to send another probe to the moon.

Glein is working on a proposal for exactly such a mission. But right now, NASA has no project in the works to revisit the Saturnian system. It could be more than a decade before we go back.

“It’s frustrating and thrilling at the same time,” Glein said.

Fortunately, Enceladus no longer appears to be the only ocean world spitting its contents into space. The news that Europa also has geysers comes just as NASA begins the preliminary design phase of the Europa Clipper mission, which is slated to orbit Jupiter and perform 45 flybys of the planet's icy moon.

This is not the first time scientists have detected evidence of geysers on Europa; Hubble has spotted similar plumes several times before. But this detection provides further evidence for the activity and will help scientists figure out the timing of
Europa's geysers in advance of the Clipper mission.

The plumes were detected by the Hubble Space Telescope as Europa passed in front of Jupiter. Silhouetted against the hot, glowing form of its host planet, scientists could see gusts of material shooting upward. The jets were so powerful that they extended 50 kilometers above the moon's surface — Old Faithful, the famous geyser at Yellowstone, only reaches 184 feet.

When the Clipper arrives in the mid-2020s, it will carry instruments specifically designed to sample Europa's plumes and test for organic molecules. Unlike Cassini, which had no idea what it would encounter when it detected Enceladus's geysers for the first time, the spacecraft should be well-equipped to detect life — if there's any life to be found.

Voytek said that her boss, NASA's planetary science director Jim Green, is determined to find organisms beyond Earth before he retires. “You've got a couple of years,” he told her, jokingly, when they heard about the Enceladus discovery.

Green is optimistic about his chances.

“We're just on the precipice of moving this whole activity forward,” he told The Washington Post. “I think in our lifetime we'll be able to answer the question, 'Are we alone?'”

Read more:

There's an 'Earthlike' planet with an atmosphere just 39 light-years away

What does a black hole look like? Astronomers are on a quest to find out.

Scientists discover 7 'Earthlike' planets orbiting a nearby star

You can now spell 'Earthling' with a capital 'E,' and here's why

No, NASA didn’t find life on Saturn's moon. But deep sea life on Earth is pretty alien.

Sarah Kaplan is a reporter for Speaking of Science. Follow @sarahkaplan48
For Immediate Release

May 11, 2017

The White House
Office of the Press Secretary

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

EXECUTIVE ORDER
By the authority vested in me as President by the Constitution and the laws of the United States of America, and to protect American innovation and values, it is hereby ordered as follows:

Section 1. Cybersecurity of Federal Networks.

(a) Policy. The executive branch operates its information technology (IT) on behalf of the American people. Its IT and data should be secured responsibly using all United States Government capabilities. The President will hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises. In addition, because risk management decisions made by agency heads can affect the risk to the executive branch as a whole, and to national security, it is also the policy of the United States to manage cybersecurity risk as an executive branch enterprise.

(b) Findings.

(i) Cybersecurity risk management comprises the full range of activities undertaken to protect IT and data from unauthorized access and other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents adversely affecting IT and data, and to mitigate the impact of, respond to, and recover from incidents. Information sharing facilitates and supports all of these activities.

(ii) The executive branch has for too long accepted antiquated and difficult-to-defend IT.

(iii) Effective risk management involves more than just protecting IT and data currently in place. It also requires planning so that maintenance, improvements, and modernization occur in a coordinated way and with appropriate regularity.

(iv) Known but unmitigated vulnerabilities are among the highest cybersecurity risks faced by executive departments and agencies (agencies). Known vulnerabilities include using operating systems or hardware beyond the vendor's support lifecycle, declining to implement a vendor's security patch, or failing to execute security-specific configuration guidance.

(v) Effective risk management requires agency heads to lead integrated teams of senior executives with expertise in IT, security, budgeting, acquisition, law, privacy, and human resources.

(c) Risk Management.
(i) Agency heads will be held accountable by the President for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data. They will also be held accountable by the President for ensuring that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes, in accordance with chapter 35, subchapter II of title 44, United States Code.

(ii) Effective immediately, each agency head shall use The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology, or any successor document, to manage the agency’s cybersecurity risk. Each agency head shall provide a risk management report to the Secretary of Homeland Security and the Director of the Office of Management and Budget (OMB) within 90 days of the date of this order. The risk management report shall:

(A) document the risk mitigation and acceptance choices made by each agency head as of the date of this order, including:

(1) the strategic, operational, and budgetary considerations that informed those choices; and

(2) any accepted risk, including from unmitigated vulnerabilities; and

(B) describe the agency's action plan to implement the Framework.

(iii) The Secretary of Homeland Security and the Director of OMB, consistent with chapter 35, subchapter II of title 44, United States Code, shall jointly assess each agency’s risk management report to determine whether the risk mitigation and acceptance choices set forth in the reports are appropriate and sufficient to manage the cybersecurity risk to the executive branch enterprise in the aggregate (the determination).

(iv) The Director of OMB, in coordination with the Secretary of Homeland Security, with appropriate support from the Secretary of Commerce and the Administrator of General Services, and within 60 days of receipt of the agency risk management reports outlined in subsection (c)(ii) of this section, shall submit to the President, through the Assistant to the President for Homeland Security and Counterterrorism, the following:

(A) the determination; and

(B) a plan to:
(1) adequately protect the executive branch enterprise, should the determination identify insufficiencies;

(2) address immediate unmet budgetary needs necessary to manage risk to the executive branch enterprise;

(3) establish a regular process for reassessing and, if appropriate, reissuing the determination, and addressing future, recurring unmet budgetary needs necessary to manage risk to the executive branch enterprise;

(4) clarify, reconcile, and reissue, as necessary and to the extent permitted by law, all policies, standards, and guidelines issued by any agency in furtherance of chapter 35, subchapter II of title 44, United States Code, and, as necessary and to the extent permitted by law, issue policies, standards, and guidelines in furtherance of this order; and

(5) align these policies, standards, and guidelines with the Framework.

(v) The agency risk management reports described in subsection (c)(ii) of this section and the determination and plan described in subsections (c)(iii) and (iv) of this section may be classified in full or in part, as appropriate.

(vi) Effective immediately, it is the policy of the executive branch to build and maintain a modern, secure, and more resilient executive branch IT architecture.

(A) Agency heads shall show preference in their procurement for shared IT services, to the extent permitted by law, including email, cloud, and cybersecurity services.

(B) The Director of the American Technology Council shall coordinate a report to the President from the Secretary of Homeland Security, the Director of OMB, and the Administrator of General Services, in consultation with the Secretary of Commerce, as appropriate, regarding modernization of Federal IT. The report shall:

(1) be completed within 90 days of the date of this order; and

(2) describe the legal, policy, and budgetary considerations relevant to -- as well as the technical feasibility and cost effectiveness, including timelines and milestones, of -- transitioning all agencies, or a subset of agencies, to:

(aa) one or more consolidated network architectures; and
(bb) shared IT services, including email, cloud, and cybersecurity services.

(C) The report described in subsection (c)(vi)(B) of this section shall assess the effects of transitioning all agencies, or a subset of agencies, to shared IT services with respect to cybersecurity, including by making recommendations to ensure consistency with section 227 of the Homeland Security Act (6 U.S.C. 148) and compliance with policies and practices issued in accordance with section 3553 of title 44, United States Code. All agency heads shall supply such information concerning their current IT architectures and plans as is necessary to complete this report on time.

(vii) For any National Security System, as defined in section 3552(b)(6) of title 44, United States Code, the Secretary of Defense and the Director of National Intelligence, rather than the Secretary of Homeland Security and the Director of OMB, shall implement this order to the maximum extent feasible and appropriate. The Secretary of Defense and the Director of National Intelligence shall provide a report to the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism describing their implementation of subsection (c) of this section within 150 days of the date of this order. The report described in this subsection shall include a justification for any deviation from the requirements of subsection (c), and may be classified in full or in part, as appropriate.

Sec. 2. Cybersecurity of Critical Infrastructure.

(a) Policy. It is the policy of the executive branch to use its authorities and capabilities to support the cybersecurity risk management efforts of the owners and operators of the Nation's critical infrastructure (as defined in section 5195c(e) of title 42, United States Code) (critical infrastructure entities), as appropriate.

(b) Support to Critical Infrastructure at Greatest Risk. The Secretary of Homeland Security, in coordination with the Secretary of Defense, the Attorney General, the Director of National Intelligence, the Director of the Federal Bureau of Investigation, the heads of appropriate sector-specific agencies, as defined in Presidential Policy Directive 21 of February 12, 2013 (Critical Infrastructure Security and Resilience) (sector-specific agencies), and all other appropriate agency heads, as identified by the Secretary of Homeland Security, shall:

(i) identify authorities and capabilities that agencies could employ to support the cybersecurity efforts of critical infrastructure entities identified pursuant to section 9 of Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), to be at greatest risk of attacks that could reasonably result in
catastrophic regional or national effects on public health or safety, economic security, or national security (section 9 entities);

(ii) engage section 9 entities and solicit input as appropriate to evaluate whether and how the authorities and capabilities identified pursuant to subsection (b)(i) of this section might be employed to support cybersecurity risk management efforts and any obstacles to doing so;

(iii) provide a report to the President, which may be classified in full or in part, as appropriate, through the Assistant to the President for Homeland Security and Counterterrorism, within 180 days of the date of this order, that includes the following:

(A) the authorities and capabilities identified pursuant to subsection (b)(i) of this section;

(B) the results of the engagement and determination required pursuant to subsection (b)(ii) of this section; and

(C) findings and recommendations for better supporting the cybersecurity risk management efforts of section 9 entities; and

(iv) provide an updated report to the President on an annual basis thereafter.

(c) Supporting Transparency in the Marketplace. The Secretary of Homeland Security, in coordination with the Secretary of Commerce, shall provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, that examines the sufficiency of existing Federal policies and practices to promote appropriate market transparency of cybersecurity risk management practices by critical infrastructure entities, with a focus on publicly traded critical infrastructure entities, within 90 days of the date of this order.

(d) Resilience Against Botnets and Other Automated, Distributed Threats. The Secretary of Commerce and the Secretary of Homeland Security shall jointly lead an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets). The Secretary of Commerce and the Secretary of Homeland Security shall consult with the Secretary of Defense, the Attorney General, the Director of the Federal Bureau of Investigation, the heads of sector-specific agencies, the Chairs of the Federal Communications Commission and Federal Trade Commission, other interested agency heads, and appropriate stakeholders in carrying out this subsection. Within 240 days of the date of this order, the Secretary of Commerce and the Secretary of Homeland Security shall make publicly available a preliminary report on this effort. Within 1
year of the date of this order, the Secretaries shall submit a final version of this report to the President.

(e) Assessment of Electricity Disruption Incident Response Capabilities. The Secretary of Energy and the Secretary of Homeland Security, in consultation with the Director of National Intelligence, with State, local, tribal, and territorial governments, and with others as appropriate, shall jointly assess:

(i) the potential scope and duration of a prolonged power outage associated with a significant cyber incident, as defined in Presidential Policy Directive 41 of July 26, 2016 (United States Cyber Incident Coordination), against the United States electric subsector;

(ii) the readiness of the United States to manage the consequences of such an incident; and

(iii) any gaps or shortcomings in assets or capabilities required to mitigate the consequences of such an incident.

The assessment shall be provided to the President, through the Assistant to the President for Homeland Security and Counterterrorism, within 90 days of the date of this order, and may be classified in full or in part, as appropriate.

(f) Department of Defense Warfighting Capabilities and Industrial Base. Within 90 days of the date of this order, the Secretary of Defense, the Secretary of Homeland Security, and the Director of the Federal Bureau of Investigation, in coordination with the Director of National Intelligence, shall provide a report to the President, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, on cybersecurity risks facing the defense industrial base, including its supply chain, and United States military platforms, systems, networks, and capabilities, and recommendations for mitigating these risks. The report may be classified in full or in part, as appropriate.

Sec. 3. Cybersecurity for the Nation.

(a) Policy. To ensure that the internet remains valuable for future generations, it is the policy of the executive branch to promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft. Further, the United States seeks to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace.
(b) Deterrence and Protection. Within 90 days of the date of this order, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Secretary of Commerce, the Secretary of Homeland Security, and the United States Trade Representative, in coordination with the Director of National Intelligence, shall jointly submit a report to the President, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, on the Nation’s strategic options for deterring adversaries and better protecting the American people from cyber threats.

(c) International Cooperation. As a highly connected nation, the United States is especially dependent on a globally secure and resilient internet and must work with allies and other partners toward maintaining the policy set forth in this section. Within 45 days of the date of this order, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Secretary of Commerce, and the Secretary of Homeland Security, in coordination with the Attorney General and the Director of the Federal Bureau of Investigation, shall submit reports to the President on their international cybersecurity priorities, including those concerning investigation, attribution, cyber threat information sharing, response, capacity building, and cooperation. Within 90 days of the submission of the reports, and in coordination with the agency heads listed in this subsection, and any other agency heads as appropriate, the Secretary of State shall provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, documenting an engagement strategy for international cooperation in cybersecurity.

(d) Workforce Development. In order to ensure that the United States maintains a long-term cybersecurity advantage:

(i) The Secretary of Commerce and the Secretary of Homeland Security, in consultation with the Secretary of Defense, the Secretary of Labor, the Secretary of Education, the Director of the Office of Personnel Management, and other agencies identified jointly by the Secretary of Commerce and the Secretary of Homeland Security, shall:

(A) jointly assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education; and

(B) within 120 days of the date of this order, provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, with findings and recommendations regarding how to support the growth and sustainment of the Nation’s cybersecurity workforce in both the public and private sectors.
(ii) The Director of National Intelligence, in consultation with the heads of other agencies identified by the Director of National Intelligence, shall:

(A) review the workforce development efforts of potential foreign cyber peers in order to help identify foreign workforce development practices likely to affect long-term United States cybersecurity competitiveness; and

(B) within 60 days of the date of this order, provide a report to the President through the Assistant to the President for Homeland Security and Counterterrorism on the findings of the review carried out pursuant to subsection (d)(ii)(A) of this section.

(iii) The Secretary of Defense, in coordination with the Secretary of Commerce, the Secretary of Homeland Security, and the Director of National Intelligence, shall:

(A) assess the scope and sufficiency of United States efforts to ensure that the United States maintains or increases its advantage in national-security-related cyber capabilities; and

(B) within 150 days of the date of this order, provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, with findings and recommendations on the assessment carried out pursuant to subsection (d)(iii)(A) of this section.

(iv) The reports described in this subsection may be classified in full or in part, as appropriate.

Sec. 4. Definitions. For the purposes of this order:

(a) The term "appropriate stakeholders" means any non-executive-branch person or entity that elects to participate in an open and transparent process established by the Secretary of Commerce and the Secretary of Homeland Security under section 2(d) of this order.

(b) The term "information technology" (IT) has the meaning given to that term in section 11101(6) of title 40, United States Code, and further includes hardware and software systems of agencies that monitor and control physical equipment and processes.

(c) The term "IT architecture" refers to the integration and implementation of IT within an agency.

(d) The term "network architecture" refers to the elements of IT architecture that enable or facilitate communications between two or more IT assets.
Sec. 5. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods. Nothing in this order shall be construed to supersede measures established under authority of law to protect the security and integrity of specific activities and associations that are in direct support of intelligence or law enforcement operations.

(d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

DONALD J. TRUMP

THE WHITE HOUSE,
FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 AMENDMENTS ACT OF 2008
TITLE I—FOREIGN INTELLIGENCE SURVEILLANCE

SEC. 101. ADDITIONAL PROCEDURES REGARDING CERTAIN PERSONS OUTSIDE THE UNITED STATES.

(a) IN GENERAL.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended—
(1) by striking title VII; and
(2) by adding at the end the following:

“TITLE VII—ADDITIONAL PROCEDURES REGARDING CERTAIN PERSONS OUTSIDE THE UNITED STATES

“SEC. 701. DEFINITIONS.


“(b) ADDITIONAL DEFINITIONS.—

“(1) CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term ‘congressional intelligence committees’ means—

“(A) the Select Committee on Intelligence of the Senate; and

“(B) the Permanent Select Committee on Intelligence of the House of Representatives.

“(2) FOREIGN INTELLIGENCE SURVEILLANCE COURT; COURT.—The terms ‘Foreign Intelligence Surveillance Court’ and ‘Court’ mean the court established under section 103(a).

“(3) FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW; COURT OF REVIEW.—The terms ‘Foreign Intelligence Surveillance Court of Review’ and ‘Court of Review’ mean the court established under section 103(b).

“(4) ELECTRONIC COMMUNICATION SERVICE PROVIDER.—The term ‘electronic communication service provider’ means—

“(A) a telecommunications carrier, as that term is defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);

“(B) a provider of electronic communication service, as that term is defined in section 2510 of title 18, United States Code;

“(C) a provider of a remote computing service, as that term is defined in section 2711 of title 18, United States Code;

“(D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or

“(E) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).
“(5) INTELLIGENCE COMMUNITY.—The term ‘intelligence community’ has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

50 USC 1881a.

“SEC. 702. PROCEDURES FOR TARGETING CERTAIN PERSONS OUTSIDE THE UNITED STATES OTHER THAN UNITED STATES PERSONS.

“(a) AUTHORIZATION.—Notwithstanding any other provision of law, upon the issuance of an order in accordance with subsection (i)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.

“(b) LIMITATIONS.—An acquisition authorized under subsection (a)—

“(1) may not intentionally target any person known at the time of acquisition to be located in the United States;

“(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;

“(3) may not intentionally target a United States person reasonably believed to be located outside the United States;

“(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and

“(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

“(c) CONDUCT OF ACQUISITION.—

“(1) IN GENERAL.—An acquisition authorized under subsection (a) shall be conducted only in accordance with—

“(A) the targeting and minimization procedures adopted in accordance with subsections (d) and (e); and

“(B) upon submission of a certification in accordance with subsection (g), such certification.

“(2) DETERMINATION.—A determination under this paragraph and for purposes of subsection (a) is a determination by the Attorney General and the Director of National Intelligence that exigent circumstances exist because, without immediate implementation of an authorization under subsection (a), intelligence important to the national security of the United States may be lost or not timely acquired and time does not permit the issuance of an order pursuant to subsection (i)(3) prior to the implementation of such authorization.

“(3) TIMING OF DETERMINATION.—The Attorney General and the Director of National Intelligence may make the determination under paragraph (2)—

“(A) before the submission of a certification in accordance with subsection (g); or

“(B) by amending a certification pursuant to subsection (i)(1)(C) at any time during which judicial review under subsection (i) of such certification is pending.

“(4) CONSTRUCTION.—Nothing in title I shall be construed to require an application for a court order under such title
for an acquisition that is targeted in accordance with this section at a person reasonably believed to be located outside the United States.

"(d) Targeting Procedures.—

"(1) Requirement to Adopt.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt targeting procedures that are reasonably designed to—

"(A) ensure that any acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and

"(B) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

"(2) Judicial Review.—The procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (i).

"(e) Minimization Procedures.—

"(1) Requirement to Adopt.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt minimization procedures that meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate, for acquisitions authorized under subsection (a).

"(2) Judicial Review.—The minimization procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (i).

"(f) Guidelines for Compliance with Limitations.—

"(1) Requirement to Adopt.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt guidelines to ensure—

"(A) compliance with the limitations in subsection (b); and

"(B) that an application for a court order is filed as required by this Act.

"(2) Submission of Guidelines.—The Attorney General shall provide the guidelines adopted in accordance with paragraph (1) to—

"(A) the congressional intelligence committees;

"(B) the Committees on the Judiciary of the Senate and the House of Representatives; and

"(C) the Foreign Intelligence Surveillance Court.

"(g) Certification.—

"(1) In General.—

"(A) Requirement.—Subject to subparagraph (B), prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall provide to the Foreign Intelligence Surveillance Court a written certification and any supporting affidavit, under oath and under seal, in accordance with this subsection.

"(B) Exception.—If the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2) and time does not permit the submission of a certification under this subsection prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall submit to the Court a certification for
such authorization as soon as practicable but in no event later than 7 days after such determination is made.

“(2) REQUIREMENTS.—A certification made under this subsection shall—

“(A) attest that—

“(i) there are procedures in place that have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court that are reasonably designed to—

“(I) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and

“(II) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States;

“(ii) the minimization procedures to be used with respect to such acquisition—

“(I) meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate; and

“(II) have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court;

“(iii) guidelines have been adopted in accordance with subsection (f) to ensure compliance with the limitations in subsection (b) and to ensure that an application for a court order is filed as required by this Act;

“(iv) the procedures and guidelines referred to in clauses (i), (ii), and (iii) are consistent with the requirements of the fourth amendment to the Constitution of the United States;

“(v) a significant purpose of the acquisition is to obtain foreign intelligence information;

“(vi) the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider; and

“(vii) the acquisition complies with the limitations in subsection (b);

“(B) include the procedures adopted in accordance with subsections (d) and (e);

“(C) be supported, as appropriate, by the affidavit of any appropriate official in the area of national security who is—

“(i) appointed by the President, by and with the advice and consent of the Senate; or

“(ii) the head of an element of the intelligence community;

“(D) include—

“(i) an effective date for the authorization that is at least 30 days after the submission of the written certification to the court; or
“(ii) if the acquisition has begun or the effective date is less than 30 days after the submission of the written certification to the court, the date the acquisition began or the effective date for the acquisition; and

“(E) if the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2), include a statement that such determination has been made.

“(3) CHANGE IN EFFECTIVE DATE.—The Attorney General and the Director of National Intelligence may advance or delay the effective date referred to in paragraph (2)(D) by submitting an amended certification in accordance with subsection (i)(1)(C) to the Foreign Intelligence Surveillance Court for review pursuant to subsection (i).

“(4) LIMITATION.—A certification made under this subsection is not required to identify the specific facilities, places, premises, or property at which an acquisition authorized under subsection (a) will be directed or conducted.

“(5) MAINTENANCE OF CERTIFICATION.—The Attorney General or a designee of the Attorney General shall maintain a copy of a certification made under this subsection.

“(6) REVIEW.—A certification submitted in accordance with this subsection shall be subject to judicial review pursuant to subsection (i).

“(h) DIRECTIVES AND JUDICIAL REVIEW OF DIRECTIVES.—

“(1) AUTHORITY.—With respect to an acquisition authorized under subsection (a), the Attorney General and the Director of National Intelligence may direct, in writing, an electronic communication service provider to—

“(A) immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition; and

“(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain.

“(2) COMPENSATION.—The Government shall compensate, at the prevailing rate, an electronic communication service provider for providing information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

“(3) RELEASE FROM LIABILITY.—No cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

“(4) CHALLENGING OF DIRECTIVES.—

“(A) AUTHORITY TO CHALLENGE.—An electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition to modify or set
aside such directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.

“(B) ASSIGNMENT.—The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established under section 103(e)(1) not later than 24 hours after the filing of such petition.

“(C) STANDARDS FOR REVIEW.—A judge considering a petition filed under subparagraph (A) may grant such petition only if the judge finds that the directive does not meet the requirements of this section, or is otherwise unlawful.

“(D) PROCEDURES FOR INITIAL REVIEW.—A judge shall conduct an initial review of a petition filed under subparagraph (A) not later than 5 days after being assigned such petition. If the judge determines that such petition does not consist of claims, defenses, or other legal contentions that are warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law, the judge shall immediately deny such petition and affirm the directive or any part of the directive that is the subject of such petition and order the recipient to comply with the directive or any part of it. Upon making a determination under this subparagraph or promptly thereafter, the judge shall provide a written statement for the record of the reasons for such determination.

“(E) PROCEDURES FOR PLENARY REVIEW.—If a judge determines that a petition filed under subparagraph (A) requires plenary review, the judge shall affirm, modify, or set aside the directive that is the subject of such petition not later than 30 days after being assigned such petition. If the judge does not set aside the directive, the judge shall immediately affirm or affirm with modifications the directive, and order the recipient to comply with the directive in its entirety or as modified. The judge shall provide a written statement for the record of the reasons for a determination under this subparagraph.

“(F) CONTINUED EFFECT.—Any directive not explicitly modified or set aside under this paragraph shall remain in full effect.

“(G) CONTEMPT OF COURT.—Failure to obey an order issued under this paragraph may be punished by the Court as contempt of court.

“(5) ENFORCEMENT OF DIRECTIVES.—

“(A) ORDER TO COMPEL.—If an electronic communication service provider fails to comply with a directive issued pursuant to paragraph (1), the Attorney General may file a petition for an order to compel the electronic communication service provider to comply with the directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.

“(B) ASSIGNMENT.—The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established under section
103(e)(1) not later than 24 hours after the filing of such petition.

“(C) PROCEDURES FOR REVIEW.—A judge considering a petition filed under subparagraph (A) shall, not later than 30 days after being assigned such petition, issue an order requiring the electronic communication service provider to comply with the directive or any part of it, as issued or as modified, if the judge finds that the directive meets the requirements of this section and is otherwise lawful. The judge shall provide a written statement for the record of the reasons for a determination under this paragraph.

“(D) CONTEMPT OF COURT.—Failure to obey an order issued under this paragraph may be punished by the Court as contempt of court.

“(E) PROCESS.—Any process under this paragraph may be served in any judicial district in which the electronic communication service provider may be found.

“(6) APPEAL.—

“(A) APPEAL TO THE COURT OF REVIEW.—The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition with the Foreign Intelligence Surveillance Court of Review for review of a decision issued pursuant to paragraph (4) or (5). The Court of Review shall have jurisdiction to consider such petition and shall provide a written statement for the record of the reasons for a decision under this subparagraph.

“(B) CERTIORARI TO THE SUPREME COURT.—The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

“(i) JUDICIAL REVIEW OF CERTIFICATIONS AND PROCEDURES.—

“(1) IN GENERAL.—

“(A) REVIEW BY THE FOREIGN INTELLIGENCE SURVEILLANCE COURT.—The Foreign Intelligence Surveillance Court shall have jurisdiction to review a certification submitted in accordance with subsection (g) and the targeting and minimization procedures adopted in accordance with subsections (d) and (e), and amendments to such certification or such procedures.

“(B) TIME PERIOD FOR REVIEW.—The Court shall review a certification submitted in accordance with subsection (g) and the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and shall complete such review and issue an order under paragraph (3) not later than 30 days after the date on which such certification and such procedures are submitted.

“(C) AMENDMENTS.—The Attorney General and the Director of National Intelligence may amend a certification submitted in accordance with subsection (g) or the targeting and minimization procedures adopted in accordance with subsections (d) and (e) as necessary at any time, including
if the Court is conducting or has completed review of such certification or such procedures, and shall submit the amended certification or amended procedures to the Court not later than 7 days after amending such certification or such procedures. The Court shall review any amendment under this subparagraph under the procedures set forth in this subsection. The Attorney General and the Director of National Intelligence may authorize the use of an amended certification or amended procedures pending the Court's review of such amended certification or amended procedures.

"(2) Review.—The Court shall review the following:
   "(A) Certification.—A certification submitted in accordance with subsection (g) to determine whether the certification contains all the required elements.
   "(B) Targeting procedures.—The targeting procedures adopted in accordance with subsection (d) to assess whether the procedures are reasonably designed to—
      "(i) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and
      "(ii) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.
   "(C) Minimization procedures.—The minimization procedures adopted in accordance with subsection (e) to assess whether such procedures meet the definition of minimization procedures under section 101(h) or section 301(4), as appropriate.

"(3) Orders.—
   "(A) Approval.—If the Court finds that a certification submitted in accordance with subsection (g) contains all the required elements and that the targeting and minimization procedures adopted in accordance with subsections (d) and (e) are consistent with the requirements of those subsections and with the fourth amendment to the Constitution of the United States, the Court shall enter an order approving the certification and the use, or continued use in the case of an acquisition authorized pursuant to a determination under subsection (c)(2), of the procedures for the acquisition.
   "(B) Correction of deficiencies.—If the Court finds that a certification submitted in accordance with subsection (g) does not contain all the required elements, or that the procedures adopted in accordance with subsections (d) and (e) are not consistent with the requirements of those subsections or the fourth amendment to the Constitution of the United States, the Court shall issue an order directing the Government to, at the Government's election and to the extent required by the Court's order—
      "(i) correct any deficiency identified by the Court's order not later than 30 days after the date on which the Court issues the order; or
“(ii) cease, or not begin, the implementation of the authorization for which such certification was submitted.

“(C) REQUIREMENT FOR WRITTEN STATEMENT.—In support of an order under this subsection, the Court shall provide, simultaneously with the order, for the record a written statement of the reasons for the order.

“(4) APPEAL.—

“(A) APPEAL TO THE COURT OF REVIEW.—The Government may file a petition with the Foreign Intelligence Surveillance Court of Review for review of an order under this subsection. The Court of Review shall have jurisdiction to consider such petition. For any decision under this subparagraph affirming, reversing, or modifying an order of the Foreign Intelligence Surveillance Court, the Court of Review shall provide for the record a written statement of the reasons for the decision.

“(B) CONTINUATION OF ACQUISITION PENDING REHEARING OR APPEAL.—Any acquisition affected by an order under paragraph (3)(B) may continue—

“(i) during the pendency of any rehearing of the order by the Court en banc; and

“(ii) if the Government files a petition for review of an order under this section, until the Court of Review enters an order under subparagraph (C).

“(C) IMPLEMENTATION PENDING APPEAL.—Not later than 60 days after the filing of a petition for review of an order under paragraph (3)(B) directing the correction of a deficiency, the Court of Review shall determine, and enter a corresponding order regarding, whether all or any part of the correction order, as issued or modified, shall be implemented during the pendency of the review.

“(D) CERTIORARI TO THE SUPREME COURT.—The Government may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

“(5) SCHEDULE.—

“(A) REAUTHORIZATION OF AUTHORIZATIONS IN EFFECT.—If the Attorney General and the Director of National Intelligence seek to reauthorize or replace an authorization issued under subsection (a), the Attorney General and the Director of National Intelligence shall, to the extent practicable, submit to the Court the certification prepared in accordance with subsection (g) and the procedures adopted in accordance with subsections (d) and (e) at least 30 days prior to the expiration of such authorization.

“(B) REAUTHORIZATION OF ORDERS, AUTHORIZATIONS, AND DIRECTIVES.—If the Attorney General and the Director of National Intelligence seek to reauthorize or replace an authorization issued under subsection (a) by filing a certification pursuant to subparagraph (A), that authorization, and any directives issued thereunder and any order related thereto, shall remain in effect, notwithstanding the expiration provided for in subsection (a), until the Court issues
an order with respect to such certification under paragraph (3) at which time the provisions of that paragraph and paragraph (4) shall apply with respect to such certification.

“(j) JUDICIAL PROCEEDINGS.—

“(1) EXPEDITED JUDICIAL PROCEEDINGS.—Judicial proceedings under this section shall be conducted as expeditiously as possible.

“(2) TIME LIMITS.—A time limit for a judicial decision in this section shall apply unless the Court, the Court of Review, or any judge of either the Court or the Court of Review, by order for reasons stated, extends that time as necessary for good cause in a manner consistent with national security.

“(k) MAINTENANCE AND SECURITY OF RECORDS AND PROCEEDINGS.—

“(1) STANDARDS.—The Foreign Intelligence Surveillance Court shall maintain a record of a proceeding under this section, including petitions, appeals, orders, and statements of reasons for a decision, under security measures adopted by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

“(2) FILING AND REVIEW.—All petitions under this section shall be filed under seal. In any proceedings under this section, the Court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions of a submission, which may include classified information.

“(3) RETENTION OF RECORDS.—The Attorney General and the Director of National Intelligence shall retain a directive or an order issued under this section for a period of not less than 10 years from the date on which such directive or such order is issued.

“(l) ASSESSMENTS AND REVIEWS.—

“(1) SEMIANNUAL ASSESSMENT.—Not less frequently than once every 6 months, the Attorney General and Director of National Intelligence shall assess compliance with the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f) and shall submit each assessment to—

“(A) the Foreign Intelligence Surveillance Court; and

“(B) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

“(i) the congressional intelligence committees; and

“(ii) the Committees on the Judiciary of the House of Representatives and the Senate.

“(2) AGENCY ASSESSMENT.—The Inspector General of the Department of Justice and the Inspector General of each element of the intelligence community authorized to acquire foreign intelligence information under subsection (a), with respect to the department or element of such Inspector General—

“(A) are authorized to review compliance with the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f);

“(B) with respect to acquisitions authorized under subsection (a), shall review the number of disseminated intelligence reports containing a reference to a United States-
person identity and the number of United States-person identities subsequently disseminated by the element concerned in response to requests for identities that were not referred to by name or title in the original reporting;

"(C) with respect to acquisitions authorized under subsection (a), shall review the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and

"(D) shall provide each such review to—

"(i) the Attorney General;

"(ii) the Director of National Intelligence; and

"(iii) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

"(I) the congressional intelligence committees;

and

"(II) the Committees on the Judiciary of the House of Representatives and the Senate.

"(3) ANNUAL REVIEW.—

"(A) REQUIREMENT TO CONDUCT.—The head of each element of the intelligence community conducting an acquisition authorized under subsection (a) shall conduct an annual review to determine whether there is reason to believe that foreign intelligence information has been or will be obtained from the acquisition. The annual review shall provide, with respect to acquisitions authorized under subsection (a)—

"(i) an accounting of the number of disseminated intelligence reports containing a reference to a United States-person identity;

"(ii) an accounting of the number of United States-person identities subsequently disseminated by that element in response to requests for identities that were not referred to by name or title in the original reporting;

"(iii) the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and

"(iv) a description of any procedures developed by the head of such element of the intelligence community and approved by the Director of National Intelligence to assess, in a manner consistent with national security, operational requirements and the privacy interests of United States persons, the extent to which the acquisitions authorized under subsection (a) acquire the communications of United States persons, and the results of any such assessment.

"(B) USE OF REVIEW.—The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall use each such review to evaluate the adequacy of the minimization procedures utilized by such element and, as appropriate, the application of the minimization procedures to a particular acquisition authorized under subsection (a).
“(C) Provision of Review.—The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall provide such review to—

“(i) the Foreign Intelligence Surveillance Court;
“(ii) the Attorney General;
“(iii) the Director of National Intelligence; and
“(iv) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

“(I) the congressional intelligence committees; and

“(II) the Committees on the Judiciary of the House of Representatives and the Senate.

“SEC. 703. CERTAIN ACQUISITIONS INSIDE THE UNITED STATES TARGETING UNITED STATES PERSONS OUTSIDE THE UNITED STATES.

“(a) Jurisdiction of the Foreign Intelligence Surveillance Court.—

“(1) In General.—The Foreign Intelligence Surveillance Court shall have jurisdiction to review an application and to enter an order approving the targeting of a United States person reasonably believed to be located outside the United States to acquire foreign intelligence information, if the acquisition constitutes electronic surveillance or the acquisition of stored electronic communications or stored electronic data that requires an order under this Act, and such acquisition is conducted within the United States.

“(2) Limitation.—If a United States person targeted under this subsection is reasonably believed to be located in the United States during the effective period of an order issued pursuant to subsection (c), an acquisition targeting such United States person under this section shall cease unless the targeted United States person is again reasonably believed to be located outside the United States while an order issued pursuant to subsection (c) is in effect. Nothing in this section shall be construed to limit the authority of the Government to seek an order or authorization under, or otherwise engage in any activity that is authorized under, any other title of this Act.

“(b) Application.—

“(1) In General.—Each application for an order under this section shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under subsection (a)(1). Each application shall require the approval of the Attorney General based upon the Attorney General’s finding that it satisfies the criteria and requirements of such application, as set forth in this section, and shall include—

“(A) the identity of the Federal officer making the application;

“(B) the identity, if known, or a description of the United States person who is the target of the acquisition;

“(C) a statement of the facts and circumstances relied upon to justify the applicant’s belief that the United States person who is the target of the acquisition is—
“(i) a person reasonably believed to be located outside the United States; and
“(ii) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;
“(D) a statement of proposed minimization procedures that meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate;
“(E) a description of the nature of the information sought and the type of communications or activities to be subjected to acquisition;
“(F) a certification made by the Attorney General or an official specified in section 104(a)(6) that—
“(i) the certifying official deems the information sought to be foreign intelligence information;
“(ii) a significant purpose of the acquisition is to obtain foreign intelligence information;
“(iii) such information cannot reasonably be obtained by normal investigative techniques;
“(iv) designates the type of foreign intelligence information being sought according to the categories described in section 101(e); and
“(v) includes a statement of the basis for the certification that—
“(I) the information sought is the type of foreign intelligence information designated; and
“(II) such information cannot reasonably be obtained by normal investigative techniques;
“(G) a summary statement of the means by which the acquisition will be conducted and whether physical entry is required to effect the acquisition;
“(H) the identity of any electronic communication service provider necessary to effect the acquisition, provided that the application is not required to identify the specific facilities, places, premises, or property at which the acquisition authorized under this section will be directed or conducted;
“(I) a statement of the facts concerning any previous applications that have been made to any judge of the Foreign Intelligence Surveillance Court involving the United States person specified in the application and the action taken on each previous application; and
“(J) a statement of the period of time for which the acquisition is required to be maintained, provided that such period of time shall not exceed 90 days per application.
“(2) OTHER REQUIREMENTS OF THE ATTORNEY GENERAL.—
The Attorney General may require any other affidavit or certification from any other officer in connection with the application.
“(3) OTHER REQUIREMENTS OF THE JUDGE.—The judge may require the applicant to furnish such other information as may be necessary to make the findings required by subsection (c)(1).
“(c) ORDER.—
“(1) FINDINGS.—Upon an application made pursuant to subsection (b), the Foreign Intelligence Surveillance Court shall enter an ex parte order as requested or as modified by the Court approving the acquisition if the Court finds that—
“(A) the application has been made by a Federal officer and approved by the Attorney General;

“(B) on the basis of the facts submitted by the applicant, for the United States person who is the target of the acquisition, there is probable cause to believe that the target is—

“(i) a person reasonably believed to be located outside the United States; and

“(ii) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;

“(C) the proposed minimization procedures meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate; and

“(D) the application that has been filed contains all statements and certifications required by subsection (b) and the certification or certifications are not clearly erroneous on the basis of the statement made under subsection (b)(1)(F)(v) and any other information furnished under subsection (b)(3).

“(2) PROBABLE CAUSE.—In determining whether or not probable cause exists for purposes of paragraph (1)(B), a judge having jurisdiction under subsection (a)(1) may consider past activities of the target and facts and circumstances relating to current or future activities of the target. No United States person may be considered a foreign power, agent of a foreign power, or officer or employee of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

“(3) REVIEW.—

“(A) LIMITATION ON REVIEW.—Review by a judge having jurisdiction under subsection (a)(1) shall be limited to that required to make the findings described in paragraph (1).

“(B) REVIEW OF PROBABLE CAUSE.—If the judge determines that the facts submitted under subsection (b) are insufficient to establish probable cause under paragraph (1)(B), the judge shall enter an order so stating and provide a written statement for the record of the reasons for the determination. The Government may appeal an order under this subparagraph pursuant to subsection (f).

“(C) REVIEW OF MINIMIZATION PROCEDURES.—If the judge determines that the proposed minimization procedures referred to in paragraph (1)(C) do not meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate, the judge shall enter an order so stating and provide a written statement for the record of the reasons for the determination. The Government may appeal an order under this subparagraph pursuant to subsection (f).

“(D) REVIEW OF CERTIFICATION.—If the judge determines that an application pursuant to subsection (b) does not contain all of the required elements, or that the certification or certifications are clearly erroneous on the basis of the statement made under subsection (b)(1)(F)(v) and any other information furnished under subsection (b)(3), the judge shall enter an order so stating and provide a written statement for the record of the reasons for the
determination. The Government may appeal an order under this subparagraph pursuant to subsection (f).

"(4) SPECIFICATIONS.—An order approving an acquisition under this subsection shall specify—

"(A) the identity, if known, or a description of the United States person who is the target of the acquisition identified or described in the application pursuant to subsection (b)(1)(B);

"(B) if provided in the application pursuant to subsection (b)(1)(H), the nature and location of each of the facilities or places at which the acquisition will be directed;

"(C) the nature of the information sought to be acquired and the type of communications or activities to be subjected to acquisition;

"(D) a summary of the means by which the acquisition will be conducted and whether physical entry is required to effect the acquisition; and

"(E) the period of time during which the acquisition is approved.

"(5) DIRECTIVES.—An order approving an acquisition under this subsection shall direct—

"(A) that the minimization procedures referred to in paragraph (1)(C), as approved or modified by the Court, be followed;

"(B) if applicable, an electronic communication service provider to provide to the Government forthwith all information, facilities, or assistance necessary to accomplish the acquisition authorized under such order in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition;

"(C) if applicable, an electronic communication service provider to maintain under security procedures approved by the Attorney General any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain; and

"(D) if applicable, that the Government compensate, at the prevailing rate, such electronic communication service provider for providing such information, facilities, or assistance.

"(6) DURATION.—An order approved under this subsection shall be effective for a period not to exceed 90 days and such order may be renewed for additional 90-day periods upon submission of renewal applications meeting the requirements of subsection (b).

"(7) COMPLIANCE.—At or prior to the end of the period of time for which an acquisition is approved by an order or extension under this section, the judge may assess compliance with the minimization procedures referred to in paragraph (1)(C) by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

"(d) EMERGENCY AUTHORIZATION.—

"(1) AUTHORITY FOR EMERGENCY AUTHORIZATION.—Notwithstanding any other provision of this Act, if the Attorney General reasonably determines that—
“(A) an emergency situation exists with respect to the acquisition of foreign intelligence information for which an order may be obtained under subsection (c) before an order authorizing such acquisition can with due diligence be obtained, and

(B) the factual basis for issuance of an order under this subsection to approve such acquisition exists.

the Attorney General may authorize such acquisition if a judge having jurisdiction under subsection (a)(1) is informed by the Attorney General, or a designee of the Attorney General, at the time of such authorization that the decision has been made to conduct such acquisition and if an application in accordance with this section is made to a judge of the Foreign Intelligence Surveillance Court as soon as practicable, but not more than 7 days after the Attorney General authorizes such acquisition.

“(2) MINIMIZATION PROCEDURES.—If the Attorney General authorizes an acquisition under paragraph (1), the Attorney General shall require that the minimization procedures referred to in subsection (c)(1)(C) for the issuance of a judicial order be followed.

“(3) TERMINATION OF EMERGENCY AUTHORIZATION.—In the absence of a judicial order approving an acquisition under paragraph (1), such acquisition shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.

“(4) USE OF INFORMATION.—If an application for approval submitted pursuant to paragraph (1) is denied, or in any other case where the acquisition is terminated and no order is issued approving the acquisition, no information obtained or evidence derived from such acquisition, except under circumstances in which the target of the acquisition is determined not to be a United States person, shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such acquisition shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

“(e) RELEASE FROM LIABILITY.—No cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with an order or request for emergency assistance issued pursuant to subsection (c) or (d), respectively.

“(f) APPEAL.—

“(1) APPEAL TO THE FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW.—The Government may file a petition with the Foreign Intelligence Surveillance Court of Review for review of an order issued pursuant to subsection (c). The Court of Review shall have jurisdiction to consider such petition and shall provide a written statement for the record of the reasons for a decision under this paragraph.
“(g) CONSTRUCTION.—Except as provided in this section, nothing in this Act shall be construed to require an application for a court order for an acquisition that is targeted in accordance with this section at a United States person reasonably believed to be located outside the United States.

**SEC. 704. OTHER ACQUISITIONS TARGETING UNITED STATES PERSONS OUTSIDE THE UNITED STATES.**

“(a) JURISDICTION AND SCOPE.—

“(1) JURISDICTION.—The Foreign Intelligence Surveillance Court shall have jurisdiction to enter an order pursuant to subsection (c).

“(2) SCOPE.—No element of the intelligence community may intentionally target, for the purpose of acquiring foreign intelligence information, a United States person reasonably believed to be located outside the United States under circumstances in which the targeted United States person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes, unless a judge of the Foreign Intelligence Surveillance Court has entered an order with respect to such targeted United States person or the Attorney General has authorized an emergency acquisition pursuant to subsection (c) or (d), respectively, or any other provision of this Act.

“(3) LIMITATIONS.—

“(A) MOVING OR MISIDENTIFIED TARGETS.—If a United States person targeted under this subsection is reasonably believed to be located in the United States during the effective period of an order issued pursuant to subsection (c), an acquisition targeting such United States person under this section shall cease unless the targeted United States person is again reasonably believed to be located outside the United States during the effective period of such order.

“(B) APPLICABILITY.—If an acquisition for foreign intelligence purposes is to be conducted inside the United States and could be authorized under section 703, the acquisition may only be conducted if authorized under section 703 or in accordance with another provision of this Act other than this section.

“(C) CONSTRUCTION.—Nothing in this paragraph shall be construed to limit the authority of the Government to seek an order or authorization under, or otherwise engage in any activity that is authorized under, any other title of this Act.

“(b) APPLICATION.—Each application for an order under this section shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under subsection (a)(1). Each application shall require the approval of the Attorney General based upon the Attorney General’s finding that it satisfies the
criteria and requirements of such application as set forth in this section and shall include—

“(1) the identity of the Federal officer making the application;

“(2) the identity, if known, or a description of the specific United States person who is the target of the acquisition;

“(3) a statement of the facts and circumstances relied upon to justify the applicant’s belief that the United States person who is the target of the acquisition is—

“(A) a person reasonably believed to be located outside the United States; and

“(B) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;

“(4) a statement of proposed minimization procedures that meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate;

“(5) a certification made by the Attorney General, an official specified in section 104(a)(6), or the head of an element of the intelligence community that—

“(A) the certifying official deems the information sought to be foreign intelligence information; and

“(B) a significant purpose of the acquisition is to obtain foreign intelligence information;

“(6) a statement of the facts concerning any previous applications that have been made to any judge of the Foreign Intelligence Surveillance Court involving the United States person specified in the application and the action taken on each previous application; and

“(7) a statement of the period of time for which the acquisition is required to be maintained, provided that such period of time shall not exceed 90 days per application.

“(c) ORDER.—

“(1) FINDINGS.—Upon an application made pursuant to subsection (b), the Foreign Intelligence Surveillance Court shall enter an ex parte order as requested or as modified by the Court if the Court finds that—

“(A) the application has been made by a Federal officer and approved by the Attorney General;

“(B) on the basis of the facts submitted by the applicant, for the United States person who is the target of the acquisition, there is probable cause to believe that the target is—

“(i) a person reasonably believed to be located outside the United States; and

“(ii) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;

“(C) the proposed minimization procedures, with respect to their dissemination provisions, meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate; and

“(D) the application that has been filed contains all statements and certifications required by subsection (b) and the certification provided under subsection (b)(5) is not clearly erroneous on the basis of the information furnished under subsection (b).

“(2) PROBABLE CAUSE.—In determining whether or not probable cause exists for purposes of paragraph (1)(B), a judge
having jurisdiction under subsection (a)(1) may consider past activities of the target and facts and circumstances relating to current or future activities of the target. No United States person may be considered a foreign power, agent of a foreign power, or officer or employee of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

“(3) Review.—

“(A) Limitations on review.—Review by a judge having jurisdiction under subsection (a)(1) shall be limited to that required to make the findings described in paragraph (1). The judge shall not have jurisdiction to review the means by which an acquisition under this section may be conducted.

“(B) Review of probable cause.—If the judge determines that the facts submitted under subsection (b) are insufficient to establish probable cause to issue an order under this subsection, the judge shall enter an order so stating and provide a written statement for the record of the reasons for such determination. The Government may appeal an order under this subparagraph pursuant to subsection (e).

“(C) Review of minimization procedures.—If the judge determines that the minimization procedures applicable to dissemination of information obtained through an acquisition under this subsection do not meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate, the judge shall enter an order so stating and provide a written statement for the record of the reasons for such determination. The Government may appeal an order under this subparagraph pursuant to subsection (e).

“(D) Scope of review of certification.—If the judge determines that an application under subsection (b) does not contain all the required elements, or that the certification provided under subsection (b)(5) is clearly erroneous on the basis of the information furnished under subsection (b), the judge shall enter an order so stating and provide a written statement for the record of the reasons for such determination. The Government may appeal an order under this subparagraph pursuant to subsection (e).

“(4) Duration.—An order under this paragraph shall be effective for a period not to exceed 90 days and such order may be renewed for additional 90-day periods upon submission of renewal applications meeting the requirements of subsection (b).

“(5) Compliance.—At or prior to the end of the period of time for which an order or extension is granted under this section, the judge may assess compliance with the minimization procedures referred to in paragraph (1)(C) by reviewing the circumstances under which information concerning United States persons was disseminated, provided that the judge may not inquire into the circumstances relating to the conduct of the acquisition.

“(d) Emergency Authorization.—
“(1) Authority for emergency authorization.—Notwithstanding any other provision of this section, if the Attorney General reasonably determines that—

“(A) an emergency situation exists with respect to the acquisition of foreign intelligence information for which an order may be obtained under subsection (c) before an order under that subsection can, with due diligence, be obtained, and

“(B) the factual basis for the issuance of an order under this section exists,

the Attorney General may authorize the emergency acquisition if a judge having jurisdiction under subsection (a)(1) is informed by the Attorney General or a designee of the Attorney General at the time of such authorization that the decision has been made to conduct such acquisition and if an application in accordance with this section is made to a judge of the Foreign Intelligence Surveillance Court as soon as practicable, but not more than 7 days after the Attorney General authorizes such acquisition.

“(2) Minimization procedures.—If the Attorney General authorizes an emergency acquisition under paragraph (1), the Attorney General shall require that the minimization procedures referred to in subsection (c)(1)(C) be followed.

“(3) Termination of emergency authorization.—In the absence of an order under subsection (c), an emergency acquisition under paragraph (1) shall terminate when the information sought is obtained, if the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.

“(4) Use of information.—If an application submitted to the Court pursuant to paragraph (1) is denied, or in any other case where the acquisition is terminated and no order with respect to the target of the acquisition is issued under subsection (c), no information obtained or evidence derived from such acquisition, except under circumstances in which the target of the acquisition is determined not to be a United States person, shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such acquisition shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

“(e) Appeal.—

“(1) Appeal to the court of review.—The Government may file a petition with the Foreign Intelligence Surveillance Court of Review for review of an order issued pursuant to subsection (c). The Court of Review shall have jurisdiction to consider such petition and shall provide a written statement for the record of the reasons for a decision under this paragraph.

“(2) Certiorari to the Supreme Court.—The Government may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under paragraph (1).
The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.”

“SEC. 705. JOINT APPLICATIONS AND CONCURRENT AUTHORIZATIONS.

“(a) Joint Applications and Orders.—If an acquisition targeting a United States person under section 703 or 704 is proposed to be conducted both inside and outside the United States, a judge having jurisdiction under section 703(a)(1) or 704(a)(1) may issue simultaneously, upon the request of the Government in a joint application complying with the requirements of sections 703(b) and 704(b), orders under sections 703(c) and 704(c), as appropriate.

“(b) Concurrent Authorization.—If an order authorizing electronic surveillance or physical search has been obtained under section 105 or 304, the Attorney General may authorize, for the effective period of that order, without an order under section 703 or 704, the targeting of that United States person for the purpose of acquiring foreign intelligence information while such person is reasonably believed to be located outside the United States.

“SEC. 706. USE OF INFORMATION ACQUIRED UNDER TITLE VII.

“(a) Information Acquired Under Section 702.—Information acquired from an acquisition conducted under section 702 shall be deemed to be information acquired from an electronic surveillance pursuant to title I for purposes of section 106, except for the purposes of subsection (j) of such section.

“(b) Information Acquired Under Section 703.—Information acquired from an acquisition conducted under section 703 shall be deemed to be information acquired from an electronic surveillance pursuant to title I for purposes of section 106.

“SEC. 707. CONGRESSIONAL OVERSIGHT.

“(a) Semiannual Report.—Not less frequently than once every 6 months, the Attorney General shall fully inform, in a manner consistent with national security, the congressional intelligence committees and the Committees on the Judiciary of the Senate and the House of Representatives, consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution, concerning the implementation of this title.

“(b) Content.—Each report under subsection (a) shall include—

“(1) with respect to section 702—

“(A) any certifications submitted in accordance with section 702(g) during the reporting period;

“(B) with respect to each determination under section 702(c)(2), the reasons for exercising the authority under such section;

“(C) any directives issued under section 702(h) during the reporting period;

“(D) a description of the judicial review during the reporting period of such certifications and targeting and minimization procedures adopted in accordance with subsections (d) and (e) of section 702 and utilized with respect to an acquisition under such section, including a copy of an order or pleading in connection with such review that contains a significant legal interpretation of the provisions of section 702;
“(E) any actions taken to challenge or enforce a directive under paragraph (4) or (5) of section 702(h);
“(F) any compliance reviews conducted by the Attorney General or the Director of National Intelligence of acquisitions authorized under section 702(a);
“(G) a description of any incidents of noncompliance—
“(i) with a directive issued by the Attorney General and the Director of National Intelligence under section 702(h), including incidents of noncompliance by a specified person to whom the Attorney General and Director of National Intelligence issued a directive under section 702(h); and
“(ii) by an element of the intelligence community with procedures and guidelines adopted in accordance with subsections (d), (e), and (f) of section 702; and
“(H) any procedures implementing section 702;
“(2) with respect to section 703—
“(A) the total number of applications made for orders under section 703(b);
“(B) the total number of such orders—
“(i) granted;
“(ii) modified; and
“(iii) denied; and
“(C) the total number of emergency acquisitions authorized by the Attorney General under section 703(d) and the total number of subsequent orders approving or denying such acquisitions; and
“(3) with respect to section 704—
“(A) the total number of applications made for orders under section 704(b);
“(B) the total number of such orders—
“(i) granted;
“(ii) modified; and
“(iii) denied; and
“(C) the total number of emergency acquisitions authorized by the Attorney General under section 704(d) and the total number of subsequent orders approving or denying such applications.

SEC. 708. SAVINGS PROVISION.

“Nothing in this title shall be construed to limit the authority of the Government to seek an order or authorization under, or otherwise engage in any activity that is authorized under, any other title of this Act.”.

(b) TABLE OF CONTENTS.—The table of contents in the first section of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended—
(1) by striking the item relating to title VII;
(2) by striking the item relating to section 701; and
(3) by adding at the end the following:

“TITLE VII—ADDITIONAL PROCEDURES REGARDING CERTAIN PERSONS OUTSIDE THE UNITED STATES

“Sec. 701. Definitions.
“Sec. 702. Procedures for targeting certain persons outside the United States other than United States persons.
“Sec. 703. Certain acquisitions inside the United States targeting United States persons outside the United States.
“Sec. 704. Other acquisitions targeting United States persons outside the United States.
“Sec. 705. Joint applications and concurrent authorizations.
“Sec. 706. Use of information acquired under title VII.
“Sec. 707. Congressional oversight.
“Sec. 708. Savings provision.”.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) TITLE 18, UNITED STATES CODE.—Section 2511(2)(a)(ii)(A) of title 18, United States Code, is amended by inserting “or a court order pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978” after “assistance”.

(2) FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.—Section 601(a)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1871(a)(1)) is amended—

(A) in subparagraph (C), by striking “and”; and

(B) by adding at the end the following new subparagraphs:

“(E) acquisitions under section 703; and

“(F) acquisitions under section 704.”.

SEC. 102. STATEMENT OF EXCLUSIVE MEANS BY WHICH ELECTRONIC SURVEILLANCE AND INTERCEPTION OF CERTAIN COMMUNICATIONS MAY BE CONDUCTED.

(a) STATEMENT OF EXCLUSIVE MEANS.—Title I of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by adding at the end the following new section:

“STATEMENT OF EXCLUSIVE MEANS BY WHICH ELECTRONIC SURVEILLANCE AND INTERCEPTION OF CERTAIN COMMUNICATIONS MAY BE CONDUCTED

SEC. 112. (a) Except as provided in subsection (b), the procedures of chapters 119, 121, and 206 of title 18, United States Code, and this Act shall be the exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted.

(b) Only an express statutory authorization for electronic surveillance or the interception of domestic wire, oral, or electronic communications, other than as an amendment to this Act or chapters 119, 121, or 206 of title 18, United States Code, shall constitute an additional exclusive means for the purpose of subsection (a).”.

(b) OFFENSE.—Section 109(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1809(a)) is amended by striking “authorized by statute” each place it appears and inserting “authorized by this Act, chapter 119, 121, or 206 of title 18, United States Code, or any express statutory authorization that is an additional exclusive means for conducting electronic surveillance under section 112.”; and

(c) CONFORMING AMENDMENTS.—

(1) TITLE 18, UNITED STATES CODE.—Section 2511(2)(a) of title 18, United States Code, is amended by adding at the end the following:

“(iii) If a certification under subparagraph (ii)(B) for assistance to obtain foreign intelligence information is based on statutory authority, the certification shall identify the specific statutory provision and shall certify that the statutory requirements have been met.”; and

50 USC 1812.
SEC. 102. TABLE OF CONTENTS.—The table of contents in the first section of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by inserting after the item relating to section 111, the following new item:

“Sec. 112. Statement of exclusive means by which electronic surveillance and interception of certain communications may be conducted.”

SEC. 103. SUBMITTAL TO CONGRESS OF CERTAIN COURT ORDERS UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(a) INCLUSION OF CERTAIN ORDERS IN SEMIANNUAL REPORTS OF ATTORNEY GENERAL.—Subsection (a)(5) of section 601 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1871) is amended by striking “(not including orders)” and inserting “, orders.”.

(b) REPORTS BY ATTORNEY GENERAL ON CERTAIN OTHER ORDERS.—Such section 601 is further amended by adding at the end the following:

“(c) SUBMISSIONS TO CONGRESS.—The Attorney General shall submit to the committees of Congress referred to in subsection (a)—

“(1) a copy of any decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review that includes significant construction or interpretation of any provision of this Act, and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion, not later than 45 days after such decision, order, or opinion is issued; and

“(2) a copy of each such decision, order, or opinion, and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion, that was issued during the 5-year period ending on the date of the enactment of the FISA Amendments Act of 2008 and not previously submitted in a report under subsection (a).

“(d) PROTECTION OF NATIONAL SECURITY.—The Attorney General, in consultation with the Director of National Intelligence, may authorize redactions of materials described in subsection (c) that are provided to the committees of Congress referred to in subsection (a), if such redactions are necessary to protect the national security of the United States and are limited to sensitive sources and methods information or the identities of targets.”.

(c) DEFINITIONS.—Such section 601, as amended by subsections (a) and (b), is further amended by adding at the end the following:

“(e) DEFINITIONS.—In this section:

“(1) FOREIGN INTELLIGENCE SURVEILLANCE COURT.—The term ‘Foreign Intelligence Surveillance Court’ means the court established under section 103(a).

“(2) FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW.—The term ‘Foreign Intelligence Surveillance Court of Review’ means the court established under section 103(b).”.

SEC. 104. APPLICATIONS FOR COURT ORDERS.

Section 104 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1804) is amended—

(1) in subsection (a)—

(A) by striking paragraphs (2) and (11);
(B) by redesignating paragraphs (3) through (10) as paragraphs (2) through (9), respectively;
(C) in paragraph (5), as redesignated by subparagraph (B) of this paragraph, by striking “detailed”;
(D) in paragraph (6), as redesignated by subparagraph (B) of this paragraph, in the matter preceding subpara-
graph (A)—
(1) by striking “Affairs or” and inserting “Affairs,”;
and
(ii) by striking “Senate—” and inserting “Senate,
or the Deputy Director of the Federal Bureau of Investi-
gation, if designated by the President as a certifying
official—”;
(E) in paragraph (7), as redesignated by subparagraph
(B) of this paragraph, by striking “statement of” and
inserting “summary statement of”;
(F) in paragraph (8), as redesignated by subparagraph
(B) of this paragraph, by adding “and” at the end; and
(G) in paragraph (9), as redesignated by subparagraph
(B) of this paragraph, by striking “; and” and inserting
a period;
(2) by striking subsection (b);
(3) by redesignating subsections (c) through (e) as sub-
sections (b) through (d), respectively; and
(4) in paragraph (1)(A) of subsection (d), as redesignated
by paragraph (3) of this subsection, by striking “or the Director
of National Intelligence” and inserting “the Director of National
Intelligence, or the Director of the Central Intelligence Agency”.

SEC. 105. ISSUANCE OF AN ORDER.

(a) In General.—Section 105 of the Foreign Intelligence
Surveillance Act of 1978 (50 U.S.C. 1805) is amended—
(1) in subsection (a)—
(A) by striking paragraph (1); and
(B) by redesignating paragraphs (2) through (5) as
paragraphs (1) through (4), respectively;
(2) in subsection (b), by striking “(a)(3)” and inserting
“(a)(2)”;
(3) in subsection (c)(1)—
(A) in subparagraph (D), by adding “and” at the end;
(B) in subparagraph (E), by striking “; and” and
inserting a period; and
(C) by striking subparagraph (F);
(4) by striking subsection (d);
(5) by redesignating subsections (e) through (i) as sub-
sections (d) through (h), respectively;
(6) by amending subsection (e), as redesignated by para-
graph (5) of this section, to read as follows:
“(e)(1) Notwithstanding any other provision of this title, the
Attorney General may authorize the emergency employment of
electronic surveillance if the Attorney General—
(A) reasonably determines that an emergency situation
exists with respect to the employment of electronic surveillance
to obtain foreign intelligence information before an order
authorizing such surveillance can with due diligence be
obtained;
“(B) reasonably determines that the factual basis for the issuance of an order under this title to approve such electronic surveillance exists;

“(C) informs, either personally or through a designee, a judge having jurisdiction under section 103 at the time of such authorization that the decision has been made to employ emergency electronic surveillance; and

“(D) makes an application in accordance with this title to a judge having jurisdiction under section 103 as soon as practicable, but not later than 7 days after the Attorney General authorizes such surveillance.

“(2) If the Attorney General authorizes the emergency employment of electronic surveillance under paragraph (1), the Attorney General shall require that the minimization procedures required by this title for the issuance of a judicial order be followed.

“(3) In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.

“(4) A denial of the application made under this subsection may be reviewed as provided in section 103.

“(5) In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

“(6) The Attorney General shall assess compliance with the requirements of paragraph (5).”; and

(7) by adding at the end the following:

“(i) In any case in which the Government makes an application to a judge under this title to conduct electronic surveillance involving communications and the judge grants such application, upon the request of the applicant, the judge shall also authorize the installation and use of pen registers and trap and trace devices, and direct the disclosure of the information set forth in section 402(d)(2).”.

(b) CONFORMING AMENDMENT.—Section 108(a)(2)(C) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1808(a)(2)(C)) is amended by striking “105(f)” and inserting “105(e)”.

SEC. 106. USE OF INFORMATION.

Subsection (i) of section 106 of the Foreign Intelligence Surveillance Act of 1978 (8 U.S.C. 1806) is amended by striking “radio communication” and inserting “communication”.

SEC. 107. AMENDMENTS FOR PHYSICAL SEARCHES.

(a) APPLICATIONS.—Section 303 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1823) is amended—
(1) in subsection (a)—
   (A) by striking paragraph (2);
   (B) by redesignating paragraphs (3) through (9) as paragraphs (2) through (8), respectively;
   (C) in paragraph (2), as redesignated by subparagraph (B) of this paragraph, by striking “detailed”;
   (D) in paragraph (3)(C), as redesignated by subparagraph (B) of this paragraph, by inserting “or is about to be” before “owned”; and
   (E) in paragraph (6), as redesignated by subparagraph (B) of this paragraph, in the matter preceding subparagraph (A)—
      (i) by striking “Affairs or” and inserting “Affairs,”;
      and
      (ii) by striking “Senate—” and inserting “Senate, or the Deputy Director of the Federal Bureau of Investigation, if designated by the President as a certifying official—”;
   and
   (2) in subsection (d)(1)(A), by striking “or the Director of National Intelligence” and inserting “the Director of National Intelligence, or the Director of the Central Intelligence Agency”.

(b) ORDERS.—Section 304 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1824) is amended—
   (1) in subsection (a)—
      (A) by striking paragraph (1);
      (B) by redesignating paragraphs (2) through (5) as paragraphs (1) through (4), respectively; and
      (C) in paragraph (2)(B), as redesignated by subparagraph (B) of this paragraph, by inserting “or is about to be” before “owned”; and
   (2) by amending subsection (e) to read as follows:
     “(e)(1) Notwithstanding any other provision of this title, the Attorney General may authorize the emergency employment of a physical search if the Attorney General—
       “(A) reasonably determines that an emergency situation exists with respect to the employment of a physical search to obtain foreign intelligence information before an order authorizing such physical search can with due diligence be obtained;
       “(B) reasonably determines that the factual basis for issuance of an order under this title to approve such physical search exists;
       “(C) informs, either personally or through a designee, a judge of the Foreign Intelligence Surveillance Court at the time of such authorization that the decision has been made to employ an emergency physical search; and
       “(D) makes an application in accordance with this title to a judge of the Foreign Intelligence Surveillance Court as soon as practicable, but not more than 7 days after the Attorney General authorizes such physical search.
     “(2) If the Attorney General authorizes the emergency employment of a physical search under paragraph (1), the Attorney General shall require that the minimization procedures required by this title for the issuance of a judicial order be followed.
     “(3) In the absence of a judicial order approving such physical search, the physical search shall terminate when the information sought is obtained, when the application for the order is denied,
or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.

“(4) A denial of the application made under this subsection may be reviewed as provided in section 103.

“(5) In the event that such application for approval is denied, or in any other case where the physical search is terminated and no order is issued approving the physical search, no information obtained or evidence derived from such physical search shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such physical search shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

“(6) The Attorney General shall assess compliance with the requirements of paragraph (5).”.

(c) CONFORMING AMENDMENTS.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended—

(1) in section 304(a)(4), as redesignated by subsection (b) of this section, by striking “303(a)(7)(E)” and inserting “303(a)(6)(E)”;

(2) in section 305(k)(2), by striking “303(a)(7)” and inserting “303(a)(6)”.

SEC. 108. AMENDMENTS FOR EMERGENCY PEN REGISTERS AND TRAP AND TRACE DEVICES.

Section 403 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1843) is amended—

(1) in subsection (a)(2), by striking “48 hours” and inserting “7 days”; and

(2) in subsection (c)(1)(C), by striking “48 hours” and inserting “7 days”.

SEC. 109. FOREIGN INTELLIGENCE SURVEILLANCE COURT.

(a) DESIGNATION OF JUDGES.—Subsection (a) of section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803) is amended by inserting “at least” before “seven of the United States judicial circuits”.

(b) EN BANC AUTHORITY.—

(1) IN GENERAL.—Subsection (a) of section 103 of the Foreign Intelligence Surveillance Act of 1978, as amended by subsection (a) of this section, is further amended—

(A) by inserting “(1)” after “(a)”;

(B) by adding at the end the following new paragraph:

“(2)(A) The court established under this subsection may, on its own initiative, or upon the request of the Government in any proceeding or a party under section 501(f) or paragraph (4) or (5) of section 702(h), hold a hearing or rehearing, en banc, when ordered by a majority of the judges that constitute such court upon a determination that—

(i) en banc consideration is necessary to secure or maintain uniformity of the court’s decisions; or

(ii) the proceeding involves a question of exceptional importance.
“(B) Any authority granted by this Act to a judge of the court established under this subsection may be exercised by the court en banc. When exercising such authority, the court en banc shall comply with any requirements of this Act on the exercise of such authority.

“(C) For purposes of this paragraph, the court en banc shall consist of all judges who constitute the court established under this subsection.”.

(2) CONFORMING AMENDMENTS.—The Foreign Intelligence Surveillance Act of 1978 is further amended—

(A) in subsection (a) of section 103, as amended by this subsection, by inserting “(except when sitting en banc under paragraph (2))” after “no judge designated under this subsection”; and

(B) in section 302(c) (50 U.S.C. 1822(c)), by inserting “(except when sitting en banc)” after “except that no judge”.

(c) STAY OR MODIFICATION DURING AN APPEAL.—Section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803) is amended—

(1) by redesignating subsection (f) as subsection (g); and

(2) by inserting after subsection (e) the following new subsection:

“(f)(1) A judge of the court established under subsection (a), the court established under subsection (b) or a judge of that court, or the Supreme Court of the United States or a justice of that court, may, in accordance with the rules of their respective courts, enter a stay of an order or an order modifying an order of the court established under subsection (a) or the court established under subsection (b) entered under any title of this Act, while the court established under subsection (a) conducts a rehearing, while an appeal is pending to the court established under subsection (b), or while a petition of certiorari is pending in the Supreme Court of the United States, or during the pendency of any review by that court.

“(2) The authority described in paragraph (1) shall apply to an order entered under any provision of this Act.”.

(d) AUTHORITY OF FOREIGN INTELLIGENCE SURVEILLANCE COURT.—Section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803), as amended by this Act, is amended by adding at the end the following:

“(i) Nothing in this Act shall be construed to reduce or contravene the inherent authority of the court established under subsection (a) to determine or enforce compliance with an order or a rule of such court or with a procedure approved by such court.”.

SEC. 110. WEAPONS OF MASS DESTRUCTION.

(a) DEFINITIONS.—

(1) FOREIGN POWER.—Subsection (a) of section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(a)) is amended—

(A) in paragraph (5), by striking “persons; or” and inserting “persons;”;

(B) in paragraph (6) by striking the period and inserting “; or”; and

(C) by adding at the end the following new paragraph:
“(7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.”.

(2) AGENT OF A FOREIGN POWER.—Subsection (b)(1) of such section 101 is amended—

(A) in subparagraph (B), by striking “or” at the end;

(B) in subparagraph (C), by striking “or” at the end; and

(C) by adding at the end the following new subparagraphs:

“(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or

“(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor for or on behalf of a foreign power; or”.

(3) FOREIGN INTELLIGENCE INFORMATION.—Subsection (e)(1)(B) of such section 101 is amended by striking “sabotage or international terrorism” and inserting “sabotage, international terrorism, or the international proliferation of weapons of mass destruction”.

(4) WEAPON OF MASS DESTRUCTION.—Such section 101 is amended by adding at the end the following new subsection:

“(p) ‘Weapon of mass destruction’ means—

“(1) any explosive, incendiary, or poison gas device that is designed, intended, or has the capability to cause a mass casualty incident;

“(2) any weapon that is designed, intended, or has the capability to cause death or serious bodily injury to a significant number of persons through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors;

“(3) any weapon involving a biological agent, toxin, or vector (as such terms are defined in section 178 of title 18, United States Code) that is designed, intended, or has the capability to cause death, illness, or serious bodily injury to a significant number of persons; or

“(4) any weapon that is designed, intended, or has the capability to release radiation or radioactivity causing death, illness, or serious bodily injury to a significant number of persons.”.

(b) USE OF INFORMATION.—

(1) IN GENERAL.—Section 106(k)(1)(B) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1806(k)(1)(B)) is amended by striking “sabotage or international terrorism” and inserting “sabotage, international terrorism, or the international proliferation of weapons of mass destruction”.

(2) PHYSICAL SEARCHES.—Section 305(k)(1)(B) of such Act (50 U.S.C. 1825(k)(1)(B)) is amended by striking “sabotage or international terrorism” and inserting “sabotage, international terrorism, or the international proliferation of weapons of mass destruction”.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—The Foreign Intelligence Surveillance Act of 1978 is further amended—

(1) in paragraph (2) of section 105(d) (50 U.S.C. 1805(d)), as redesignated by section 105(a)(5) of this Act, by striking “section 101(a) (5) or (6)” and inserting “paragraph (5), (6), or (7) of section 101(a)”;

50 USC 1801.
(2) in section 301(1) (50 U.S.C. 1821(1)), by inserting "weapon of mass destruction," after "person;"; and
(3) in section 304(d)(2) (50 U.S.C. 1824(d)(2)), by striking "section 101(a) (5) or (6)" and inserting "paragraph (5), (6), or (7) of section 101(a)".

TITLE II—PROTECTIONS FOR ELECTRONIC COMMUNICATION SERVICE PROVIDERS

SEC. 201. PROCEDURES FOR IMPLEMENTING STATUTORY DEFENSES UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), as amended by section 101, is further amended by adding at the end the following new title:

"TITLE VIII—PROTECTION OF PERSONS ASSISTING THE GOVERNMENT

"SEC. 801. DEFINITIONS.

"In this title:

"(1) ASSISTANCE.—The term 'assistance' means the provision of, or the provision of access to, information (including communication contents, communications records, or other information relating to a customer or communication), facilities, or another form of assistance.

"(2) CIVIL ACTION.—The term 'civil action' includes a covered civil action.

"(3) CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term 'congressional intelligence committees' means—

"(A) the Select Committee on Intelligence of the Senate; and

"(B) the Permanent Select Committee on Intelligence of the House of Representatives.

"(4) CONTENTS.—The term 'contents' has the meaning given that term in section 101(n).

"(5) COVERED CIVIL ACTION.—The term 'covered civil action' means a civil action filed in a Federal or State court that—

"(A) alleges that an electronic communication service provider furnished assistance to an element of the intelligence community; and

"(B) seeks monetary or other relief from the electronic communication service provider related to the provision of such assistance.

"(6) ELECTRONIC COMMUNICATION SERVICE PROVIDER.—The term 'electronic communication service provider' means—

"(A) a telecommunications carrier, as that term is defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);

"(B) a provider of electronic communication service, as that term is defined in section 2510 of title 18, United States Code;
“(C) a provider of a remote computing service, as that term is defined in section 2711 of title 18, United States Code;
“(D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored;
“(E) a parent, subsidiary, affiliate, successor, or assignee of an entity described in subparagraph (A), (B), (C), or (D); or
“(F) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), (D), or (E).
“(7) INTELLIGENCE COMMUNITY.—The term ‘intelligence community’ has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).
“(8) PERSON.—The term ‘person’ means—
“(A) an electronic communication service provider; or
“(B) a landlord, custodian, or other person who may be authorized or required to furnish assistance pursuant to—
“(i) an order of the court established under section 103(a) directing such assistance;
“(ii) a certification in writing under section 2511(2)(a)(ii)(B) or 2709(b) of title 18, United States Code; or
“(iii) a directive under section 102(a)(4), 105B(e), as added by section 2 of the Protect America Act of 2007 (Public Law 110–55), or 702(h).
“(9) STATE.—The term ‘State’ means any State, political subdivision of a State, the Commonwealth of Puerto Rico, the District of Columbia, and any territory or possession of the United States, and includes any officer, public utility commission, or other body authorized to regulate an electronic communication service provider.

“SEC. 802. PROCEDURES FOR IMPLEMENTING STATUTORY DEFENSES.
“(a) REQUIREMENT FOR CERTIFICATION.—Notwithstanding any other provision of law, a civil action may not lie or be maintained in a Federal or State court against any person for providing assistance to an element of the intelligence community, and shall be promptly dismissed, if the Attorney General certifies to the district court of the United States in which such action is pending that—
“(1) any assistance by that person was provided pursuant to an order of the court established under section 103(a) directing such assistance;
“(2) any assistance by that person was provided pursuant to a certification in writing under section 2511(2)(a)(ii)(B) or 2709(b) of title 18, United States Code;
“(3) any assistance by that person was provided pursuant to a directive under section 102(a)(4), 105B(e), as added by section 2 of the Protect America Act of 2007 (Public Law 110–55), or 702(h) directing such assistance;
“(4) in the case of a covered civil action, the assistance alleged to have been provided by the electronic communication service provider was—
“(A) in connection with an intelligence activity involving communications that was—
“(i) authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007; and

“(ii) designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, against the United States; and

“(B) the subject of a written request or directive, or a series of written requests or directives, from the Attorney General or the head of an element of the intelligence community (or the deputy of such person) to the electronic communication service provider indicating that the activity was—

“(i) authorized by the President; and

“(ii) determined to be lawful; or

“(5) the person did not provide the alleged assistance.

“(b) JUDICIAL REVIEW.—

“(1) REVIEW OF CERTIFICATIONS.—A certification under subsection (a) shall be given effect unless the court finds that such certification is not supported by substantial evidence provided to the court pursuant to this section.

“(2) SUPPLEMENTAL MATERIALS.—In its review of a certification under subsection (a), the court may examine the court order, certification, written request, or directive described in subsection (a) and any relevant court order, certification, written request, or directive submitted pursuant to subsection (d).

“(c) LIMITATIONS ON DISCLOSURE.—If the Attorney General files a declaration under section 1746 of title 28, United States Code, that disclosure of a certification made pursuant to subsection (a) or the supplemental materials provided pursuant to subsection (b) or (d) would harm the national security of the United States, the court shall—

“(1) review such certification and the supplemental materials in camera and ex parte; and

“(2) limit any public disclosure concerning such certification and the supplemental materials, including any public order following such in camera and ex parte review, to a statement as to whether the case is dismissed and a description of the legal standards that govern the order, without disclosing the paragraph of subsection (a) that is the basis for the certification.

“(d) ROLE OF THE PARTIES.—Any plaintiff or defendant in a civil action may submit any relevant court order, certification, written request, or directive to the district court referred to in subsection (a) for review and shall be permitted to participate in the briefing or argument of any legal issue in a judicial proceeding conducted pursuant to this section, but only to the extent that such participation does not require the disclosure of classified information to such party. To the extent that classified information is relevant to the proceeding or would be revealed in the determination of an issue, the court shall review such information in camera and ex parte, and shall issue any part of the court’s written order that would reveal classified information in camera and ex parte and maintain such part under seal.

“(e) NONDELEGATION.—The authority and duties of the Attorney General under this section shall be performed by the Attorney General (or Acting Attorney General) or the Deputy Attorney General.
(f) Appeal.—The courts of appeals shall have jurisdiction of appeals from interlocutory orders of the district courts of the United States granting or denying a motion to dismiss or for summary judgment under this section.

(g) Removal.—A civil action against a person for providing assistance to an element of the intelligence community that is brought in a State court shall be deemed to arise under the Constitution and laws of the United States and shall be removable under section 1441 of title 28, United States Code.

(h) Relationship to Other Laws.—Nothing in this section shall be construed to limit any otherwise available immunity, privilege, or defense under any other provision of law.

(i) Applicability.—This section shall apply to a civil action pending on or filed after the date of the enactment of the FISA Amendments Act of 2008.

SEC. 803. PREEMPTION.

(a) In General.—No State shall have authority to—

(1) conduct an investigation into an electronic communication service provider's alleged assistance to an element of the intelligence community;

(2) require through regulation or any other means the disclosure of information about an electronic communication service provider's alleged assistance to an element of the intelligence community;

(3) impose any administrative sanction on an electronic communication service provider for assistance to an element of the intelligence community; or

(4) commence or maintain a civil action or other proceeding to enforce a requirement that an electronic communication service provider disclose information concerning alleged assistance to an element of the intelligence community.

(b) Suits by the United States.—The United States may bring suit to enforce the provisions of this section.

(c) Jurisdiction.—The district courts of the United States shall have jurisdiction over any civil action brought by the United States to enforce the provisions of this section.

(d) Application.—This section shall apply to any investigation, action, or proceeding that is pending on or commenced after the date of the enactment of the FISA Amendments Act of 2008.

SEC. 804. REPORTING.

(a) Semiannual Report.—Not less frequently than once every 6 months, the Attorney General shall, in a manner consistent with national security, the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution, fully inform the congressional intelligence committees, the Committee on the Judiciary of the Senate, and the Committee on the Judiciary of the House of Representatives concerning the implementation of this title.

(b) Content.—Each report made under subsection (a) shall include—

(1) any certifications made under section 802;

(2) a description of the judicial review of the certifications made under section 802; and

(3) any actions taken to enforce the provisions of section 803.”.
SEC. 202. TECHNICAL AMENDMENTS.

The table of contents in the first section of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), as amended by section 101(b), is further amended by adding at the end the following:

“TITLE VIII—PROTECTION OF PERSONS ASSISTING THE GOVERNMENT

Sec. 801. Definitions.
Sec. 802. Procedures for implementing statutory defenses.
Sec. 803. Preemption.
Sec. 804. Reporting.”.

TITLE III—REVIEW OF PREVIOUS ACTIONS

SEC. 301. REVIEW OF PREVIOUS ACTIONS.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term “appropriate committees of Congress” means—

(A) the Select Committee on Intelligence and the Committee on the Judiciary of the Senate; and

(B) the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives.

(2) FOREIGN INTELLIGENCE SURVEILLANCE COURT.—The term “Foreign Intelligence Surveillance Court” means the court established under section 103(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(a)).

(3) PRESIDENT’S SURVEILLANCE PROGRAM AND PROGRAM.—The terms “President’s Surveillance Program” and “Program” mean the intelligence activity involving communications that was authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007, including the program referred to by the President in a radio address on December 17, 2005 (commonly known as the Terrorist Surveillance Program).

(b) REVIEWS.—

(1) REQUIREMENT TO CONDUCT.—The Inspectors General of the Department of Justice, the Office of the Director of National Intelligence, the National Security Agency, the Department of Defense, and any other element of the intelligence community that participated in the President’s Surveillance Program, shall complete a comprehensive review of, with respect to the oversight authority and responsibility of each such Inspector General—

(A) all of the facts necessary to describe the establishment, implementation, product, and use of the product of the Program;

(B) access to legal reviews of the Program and access to information about the Program;

(C) communications with, and participation of, individuals and entities in the private sector related to the Program;

(D) interaction with the Foreign Intelligence Surveillance Court and transition to court orders related to the Program; and
(E) any other matters identified by any such Inspector General that would enable that Inspector General to complete a review of the Program, with respect to such Department or element.

(2) COOPERATION AND COORDINATION.—

(A) COOPERATION.—Each Inspector General required to conduct a review under paragraph (1) shall—

(i) work in conjunction, to the extent practicable, with any other Inspector General required to conduct such a review; and

(ii) utilize, to the extent practicable, and not unnecessarily duplicate or delay, such reviews or audits that have been completed or are being undertaken by any such Inspector General or by any other office of the Executive Branch related to the Program.

(B) INTEGRATION OF OTHER REVIEWS.—The Counsel of the Office of Professional Responsibility of the Department of Justice shall provide the report of any investigation conducted by such Office on matters relating to the Program, including any investigation of the process through which legal reviews of the Program were conducted and the substance of such reviews, to the Inspector General of the Department of Justice, who shall integrate the factual findings and conclusions of such investigation into its review.

(C) COORDINATION.—The Inspectors General shall designate one of the Inspectors General required to conduct a review under paragraph (1) that is appointed by the President, by and with the advice and consent of the Senate, to coordinate the conduct of the reviews and the preparation of the reports.

(c) REPORTS.—

(1) PRELIMINARY REPORTS.—Not later than 60 days after the date of the enactment of this Act, the Inspectors General of the Department of Justice, the Office of the Director of National Intelligence, the National Security Agency, the Department of Defense, and any other Inspector General required to conduct a review under subsection (b)(1), shall submit to the appropriate committees of Congress an interim report that describes the planned scope of such review.

(2) FINAL REPORT.—Not later than 1 year after the date of the enactment of this Act, the Inspectors General of the Department of Justice, the Office of the Director of National Intelligence, the National Security Agency, the Department of Defense, and any other Inspector General required to conduct a review under subsection (b)(1), shall submit to the appropriate committees of Congress, in a manner consistent with national security, a comprehensive report on such reviews that includes any recommendations of any such Inspectors General within the oversight authority and responsibility of any such Inspector General with respect to the reviews.

(3) FORM.—A report under this subsection shall be submitted in unclassified form, but may include a classified annex. The unclassified report shall not disclose the name or identity of any individual or entity of the private sector that participated in the Program or with whom there was communication about the Program, to the extent that information is classified.
(d) **Resources.**—

(1) **Expedited Security Clearance.**—The Director of National Intelligence shall ensure that the process for the investigation and adjudication of an application by an Inspector General or any appropriate staff of an Inspector General for a security clearance necessary for the conduct of the review under subsection (b)(1) is carried out as expeditiously as possible.

(2) **Additional Personnel for the Inspectors General.**—An Inspector General required to conduct a review under subsection (b)(1) and submit a report under subsection (c) is authorized to hire such additional personnel as may be necessary to carry out such review and prepare such report in a prompt and timely manner. Personnel authorized to be hired under this paragraph—

(A) shall perform such duties relating to such a review as the relevant Inspector General shall direct; and

(B) are in addition to any other personnel authorized by law.

(3) **Transfer of Personnel.**—The Attorney General, the Secretary of Defense, the Director of National Intelligence, the Director of the National Security Agency, or the head of any other element of the intelligence community may transfer personnel to the relevant Office of the Inspector General required to conduct a review under subsection (b)(1) and submit a report under subsection (c) and, in addition to any other personnel authorized by law, are authorized to fill any vacancy caused by such a transfer. Personnel transferred under this paragraph shall perform such duties relating to such review as the relevant Inspector General shall direct.

### TITLE IV—OTHER PROVISIONS

**Sec. 401. Severability.**

If any provision of this Act, any amendment made by this Act, or the application thereof to any person or circumstances is held invalid, the validity of the remainder of the Act, of any such amendments, and of the application of such provisions to other persons and circumstances shall not be affected thereby.

**Sec. 402. Effective Date.**

Except as provided in section 404, the amendments made by this Act shall take effect on the date of the enactment of this Act.

**Sec. 403. Repeals.**

(a) **Repeal of Protect America Act of 2007 Provisions.**—

(1) **Amendments to FISA.**—

(A) **In General.**—Except as provided in section 404, sections 105A, 105B, and 105C of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805a, 1805b, and 1805c) are repealed.

(B) **Technical and Conforming Amendments.**—

(i) **Table of Contents.**—The table of contents in the first section of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by
striking the items relating to sections 105A, 105B, and 105C.

(ii) CONFORMING AMENDMENTS.—Except as provided in section 404, section 103(e) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(e)) is amended—

(I) in paragraph (1), by striking “105B(h) or 501(f)(1)” and inserting “501(f)(1) or 702(h)(4)”; and

(II) in paragraph (2), by striking “105B(h) or 501(f)(1)” and inserting “501(f)(1) or 702(h)(4)”.

(2) REPORTING REQUIREMENTS.—Except as provided in section 404, section 4 of the Protect America Act of 2007 (Public Law 110–55; 121 Stat. 555) is repealed.

(3) TRANSITION PROCEDURES.—Except as provided in section 404, subsection (b) of section 6 of the Protect America Act of 2007 (Public Law 110–55; 121 Stat. 556) is repealed.

(b) FISA AMENDMENTS ACT OF 2008.—

(1) IN GENERAL.—Except as provided in section 404, effective December 31, 2012, title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101(a), is repealed.

(2) TECHNICAL AND CONFORMING AMENDMENTS.—Effective December 31, 2012—

(A) the table of contents in the first section of such Act (50 U.S.C. 1801 et seq.) is amended by striking the items related to title VII;

(B) except as provided in section 404, subsection (a)(1) of such Act (50 U.S.C. 1871(a)(1)) is amended to read as such section read on the day before the date of the enactment of this Act; and

(C) except as provided in section 404, section 2511(2)(a)(ii)(A) of title 18, United States Code, is amended by striking “or a court order pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978”.

SEC. 404. TRANSITION PROCEDURES.

(a) Transition Procedures for Protect America Act of 2007 Provisions.—

(1) CONTINUED EFFECT OF ORDERS, AUTHORIZATIONS, DIRECTIVES.—Except as provided in paragraph (7), notwithstanding any other provision of law, any order, authorization, or directive issued or made pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007 (Public Law 110–55; 121 Stat. 552), shall continue in effect until the expiration of such order, authorization, or directive.

(2) APPLICABILITY OF PROTECT AMERICA ACT OF 2007 TO CONTINUED ORDERS, AUTHORIZATIONS, DIRECTIVES.—Notwithstanding any other provision of this Act, any amendment made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)—

(A) subject to paragraph (3), section 105A of such Act, as added by section 2 of the Protect America Act of 2007 (Public Law 110–55; 121 Stat. 552), shall continue to apply to any acquisition conducted pursuant to an order, authorization, or directive referred to in paragraph (1); and
(B) sections 105B and 105C of the Foreign Intelligence Surveillance Act of 1978, as added by sections 2 and 3, respectively, of the Protect America Act of 2007, shall continue to apply with respect to an order, authorization, or directive referred to in paragraph (1) until the later of—

(i) the expiration of such order, authorization, or directive; or

(ii) the date on which final judgment is entered for any petition or other litigation relating to such order, authorization, or directive.

(3) Use of Information.—Information acquired from an acquisition conducted pursuant to an order, authorization, or directive referred to in paragraph (1) shall be deemed to be information acquired from an electronic surveillance pursuant to title I of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) for purposes of section 106 of such Act (50 U.S.C. 1806), except for purposes of subsection (j) of such section.

(4) Protection from Liability.—Subsection (l) of section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007, shall continue to apply with respect to any directives issued pursuant to such section 105B.

(5) Jurisdiction of Foreign Intelligence Surveillance Court.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), section 103(e) of the Foreign Intelligence Surveillance Act (50 U.S.C. 1803(e)), as amended by section 5(a) of the Protect America Act of 2007 (Public Law 110–55; 121 Stat. 556), shall continue to apply with respect to a directive issued pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007, until the later of—

(A) the expiration of all orders, authorizations, or directives referred to in paragraph (1); or

(B) the date on which final judgment is entered for any petition or other litigation relating to such order, authorization, or directive.

(6) Reporting Requirements.—

(A) Continued Applicability.—Notwithstanding any other provision of this Act, any amendment made by this Act, the Protect America Act of 2007 (Public Law 110–55), or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), section 4 of the Protect America Act of 2007 shall continue to apply until the date that the certification described in subparagraph (B) is submitted.

(B) Certification.—The certification described in this subparagraph is a certification—

(i) made by the Attorney General;

(ii) submitted as part of a semi-annual report required by section 4 of the Protect America Act of 2007;

(iii) that states that there will be no further acquisitions carried out under section 105B of the Foreign Intelligence Surveillance Act of 1978, as added
by section 2 of the Protect America Act of 2007, after the date of such certification; and
(iv) that states that the information required to be included under such section 4 relating to any acquisition conducted under such section 105B has been included in a semi-annual report required by such section 4.

(7) REPLACEMENT OF ORDERS, AUTHORIZATIONS, AND DIRECTIVES.—

(A) IN GENERAL.—If the Attorney General and the Director of National Intelligence seek to replace an authorization issued pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007 (Public Law 110–55), with an authorization under section 702 of the Foreign Intelligence Surveillance Act of 1978 (as added by section 101(a) of this Act), the Attorney General and the Director of National Intelligence shall, to the extent practicable, submit to the Foreign Intelligence Surveillance Court (as such term is defined in section 701(b)(2) of such Act (as so added)) a certification prepared in accordance with subsection (g) of such section 702 and the procedures adopted in accordance with subsections (d) and (e) of such section 702 at least 30 days before the expiration of such authorization.

(B) CONTINUATION OF EXISTING ORDERS.—If the Attorney General and the Director of National Intelligence seek to replace an authorization made pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007 (Public Law 110–55; 121 Stat. 522), by filing a certification in accordance with subparagraph (A), that authorization, and any directives issued thereunder and any order related thereto, shall remain in effect, notwithstanding the expiration provided for in subsection (a) of such section 105B, until the Foreign Intelligence Surveillance Court (as such term is defined in section 701(b)(2) of the Foreign Intelligence Surveillance Act of 1978 (as so added)) issues an order with respect to that certification under section 702(i)(3) of such Act (as so added) at which time the provisions of that section and of section 702(i)(4) of such Act (as so added) shall apply.

(8) EFFECTIVE DATE.—Paragraphs (1) through (7) shall take effect as if enacted on August 5, 2007.

(b) TRANSITION PROCEDURES FOR FISA AMENDMENTS ACT OF 2008 PROVISIONS.—

(1) ORDERS IN EFFECT ON DECEMBER 31, 2012.—Notwithstanding any other provision of this Act, any amendment made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), any order, authorization, or directive issued or made under title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101(a), shall continue in effect until the date of the expiration of such order, authorization, or directive.

(2) APPLICABILITY OF TITLE VII OF FISA TO CONTINUED ORDERS, AUTHORIZATIONS, DIRECTIVES.—Notwithstanding any other provision of this Act, any amendment made by this Act,
or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), with respect to any order, authorization, or directive referred to in paragraph (1), title VII of such Act, as amended by section 101(a), shall continue to apply until the later of—

(A) the expiration of such order, authorization, or directive; or

(B) the date on which final judgment is entered for any petition or other litigation relating to such order, authorization, or directive.

(3) CHALLENGE OF DIRECTIVES; PROTECTION FROM LIABILITY; USE OF INFORMATION.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)—

(A) section 103(e) of such Act, as amended by section 403(a)(1)(B)(ii), shall continue to apply with respect to any directive issued pursuant to section 702(h) of such Act, as added by section 101(a);

(B) section 702(h)(3) of such Act (as so added) shall continue to apply with respect to any directive issued pursuant to section 702(h) of such Act (as so added);

(C) section 703(e) of such Act (as so added) shall continue to apply with respect to an order or request for emergency assistance under that section;

(D) section 706 of such Act (as so added) shall continue to apply to an acquisition conducted under section 702 or 703 of such Act (as so added); and

(E) section 2511(2)(a)(i)(A) of title 18, United States Code, as amended by section 101(c)(1), shall continue to apply to an order issued pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978, as added by section 101(a).

(4) REPORTING REQUIREMENTS.—

(A) CONTINUED APPLICABILITY.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), section 601(a) of such Act (50 U.S.C. 1871(a)), as amended by section 101(c)(2), and sections 702(l) and 707 of such Act, as added by section 101(a), shall continue to apply until the date that the certification described in subparagraph (B) is submitted.

(B) CERTIFICATION.—The certification described in this subparagraph is a certification—

(i) made by the Attorney General;

(ii) submitted to the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the Committees on the Judiciary of the Senate and the House of Representatives;

(iii) that states that there will be no further acquisitions carried out under title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101(a), after the date of such certification; and

(iv) that states that the information required to be included in a review, assessment, or report under section 601 of such Act, as amended by section 101(c), or section 702(l) or 707 of such Act, as added by section
101(a), relating to any acquisition conducted under title VII of such Act, as amended by section 101(a), has been included in a review, assessment, or report under such section 601, 702(l), or 707.

Deadline.

(5) Transition procedures concerning the targeting of United States persons overseas.—Any authorization in effect on the date of enactment of this Act under section 2.5 of Executive Order 12333 to intentionally target a United States person reasonably believed to be located outside the United States shall continue in effect, and shall constitute a sufficient basis for conducting such an acquisition targeting a United States person located outside the United States until the earlier of—

(A) the date that authorization expires; or

(B) the date that is 90 days after the date of the enactment of this Act.

Approved July 10, 2008.
QUESTION PRESENTED

Under the Texas Disciplinary Rules of Professional Conduct, may a lawyer communicate confidential information by email?

STATEMENT OF FACTS

Lawyers in a Texas law firm represent clients in family law, employment law, personal injury, and criminal law matters. When they started practicing law, the lawyers typically delivered written communication by facsimile or the U.S. Postal Service. Now, most of their written communication is delivered by web-based email, such as unencrypted Gmail.

Having read reports about email accounts being hacked and the National Security Agency obtaining email communications without a search warrant, the lawyers are concerned about whether it is proper for them to continue using email to communicate confidential information.

DISCUSSION

The Texas Disciplinary Rules of Professional Conduct do not specifically address the use of email in the practice of law, but they do provide for the protection of confidential information, defined broadly by Rule 1.05(a) to include both privileged and unprivileged client information, which might be transmitted by email.

Rule 1.05(b) provides that, except as permitted by paragraphs (c) and (d) of the Rule:
“a lawyer shall not knowingly:
(1) Reveal confidential information of a client or former client to:
   (i) a person that the client has instructed is not to receive the information; or
   (ii) anyone else, other than the client, the client's representatives, or the
        members, associates, or employees of the lawyer's law firm.”

A lawyer violates Rule 1.05 if the lawyer knowingly reveals confidential information to any person other than those persons who are permitted or required to receive the information under paragraphs (b), (c), (d), (e), or (f) of the Rule.

The Terminology section of the Rules states that “‘[k]nowingly’ . . . denotes actual knowledge of the fact in question” and that a “person’s knowledge may be inferred from circumstances.” A determination of whether a lawyer violates the Disciplinary Rules, as opposed to fiduciary obligations, the law, or best practices, by sending an email containing confidential information, requires a case-by-case evaluation of whether that lawyer knowingly revealed confidential information to a person who was not permitted to receive that information under Rule 1.05.


Those ethics opinions often make two points in support of the conclusion that email communication is proper. First, the risk an unauthorized person will gain access to confidential information is inherent in the delivery of any written communication including delivery by the U.S. Postal Service, a private mail service, a courier, or facsimile. Second, persons who use email have a reasonable expectation of privacy based, in part, upon statutes that make it a crime to intercept emails. See, e.g., Alaska Bar Ass’n Ethics Comm. Op. 98-2 (1998); D.C. Bar Legal Ethics Comm., Op. 281 (1998). The statute cited in those opinions is the Electronic Communication Privacy Act (ECPA), which makes it a crime to intercept electronic communication, to use the contents of the intercepted email, or to disclose the contents of intercepted email. 18 U.S.C. § 2510 et seq. Importantly, the statute provides that “[n]o otherwise privileged . . . electronic communication intercepted in accordance with, or in violation
of, the provisions of this chapter shall lose its privileged character.” 18 U.S.C. § 2517(4).

The ethics opinions from other jurisdictions are instructive, as is Texas Professional Ethics Committee Opinion 572 (June 2006). The issue in Opinion 572 was whether a lawyer may, without the client’s express consent, deliver the client’s privileged information to a copy service hired by the lawyer to perform services in connection with the client’s representation. Opinion 572 concluded that a lawyer may disclose privileged information to an independent contractor if the lawyer reasonably expects that the independent contractor will not disclose or use such items or their contents except as directed by the lawyer and will otherwise respect the confidential character of the information.

In general, considering the present state of technology and email usage, a lawyer may communicate confidential information by email. In some circumstances, however, a lawyer should consider whether the confidentiality of the information will be protected if communicated by email and whether it is prudent to use encrypted email or another form of communication. Examples of such circumstances are:

1. communicating highly sensitive or confidential information via email or unencrypted email connections;
2. sending an email to or from an account that the email sender or recipient shares with others;
3. sending an email to a client when it is possible that a third person (such as a spouse in a divorce case) knows the password to the email account, or to an individual client at that client’s work email account, especially if the email relates to a client’s employment dispute with his employer (see ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 11-459 (2011));
4. sending an email from a public computer or a borrowed computer or where the lawyer knows that the emails the lawyer sends are being read on a public or borrowed computer or on an unsecure network;
5. sending an email if the lawyer knows that the email recipient is accessing the email on devices that are potentially accessible to third persons or are not protected by a password; or
6. sending an email if the lawyer is concerned that the NSA or other law enforcement agency may read the lawyer’s email communication, with or without a warrant.

In the event circumstances such as those identified above are present, to prevent the unauthorized or inadvertent disclosure of confidential information, it may be appropriate for a lawyer to advise and caution a client as to the dangers inherent in sending or accessing emails from computers accessible to persons other than the client. A lawyer should also consider whether circumstances are present that would make it advisable to obtain the client’s informed consent to the use of email communication, including the use of unencrypted email. See Texas Rule 1.03(b) and ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 11-459 (2011). Additionally, a lawyer’s evaluation of the lawyer’s email technology and practices should be ongoing as there may be changes in the risk of interception of email communication over time that would indicate that certain or perhaps all communications should be sent by other means.
Under Rule 1.05, the issue in each case is whether a lawyer who sent an email containing confidential information knowingly revealed confidential information to a person who was not authorized to receive the information. The answer to that question depends on the facts of each case. Since a “knowing” disclosure can be based on actual knowledge or can be inferred, each lawyer must decide whether he or she has a reasonable expectation that the confidential character of the information will be maintained if the lawyer transmits the information by email.

This opinion discusses a lawyer’s obligations under the Texas Disciplinary Rules of Professional Conduct, but it does not address other issues such as a lawyer’s fiduciary obligations or best practices with respect to email communications. Furthermore, it does not address a lawyer’s obligations under various statutes, such as the Health Insurance Portability and Accountability Act (HIPAA), which may impose other duties.

CONCLUSION

Under the Texas Disciplinary Rules of Professional Conduct, and considering the present state of technology and email usage, a lawyer may generally communicate confidential information by email. Some circumstances, however, cause a lawyer to have a duty to advise a client regarding risks incident to the sending or receiving of emails arising from those circumstances and to consider whether it is prudent to use encrypted email or another form of communication.

Download a PDF version of this Opinion
What Would Zero Look Like? A Treaty for the Abolition of Nuclear Weapons

David A. Koplow
Georgetown University Law Center, koplow@law.georgetown.edu

This paper can be downloaded free of charge from: http://scholarship.law.georgetown.edu/facpub/1804

WHAT WOULD ZERO LOOK LIKE?
A TREATY FOR THE ABOLITION OF
NUCLEAR WEAPONS

DAVID A. KOPOLOW*

ABSTRACT

Nuclear disarmament—the comprehensive, universal, and permanent abolition of all nuclear weapons, pursuant to a verifiable, legally binding international agreement—has long been one of the most ambitious, controversial, and urgent items on the agenda for arms control. To date, however, most of the discussion of “getting to zero” has highlighted the political, military, technical and diplomatic dimensions of this complex problem, and there has been relatively little attention to the legal requirements for drafting such a novel treaty.

This Article fills that gap by offering two proposed agreements. The first, a non-legally-binding framework accord, would be designed for signature relatively soon (e.g., in 2015) to re-commit states to the goal of nuclear elimination and to energize their concerted individual and collective action on a set of prescribed steps in pursuit of it. The second, a legally-binding document, would be concluded at some point in the more distant future, when states had accomplished great reductions in their current nuclear arsenals and were ready, at last, to plunge forward to true abolition.

The Article describes the conditions necessary for the further articulation of these two novel agreements, and the text of each instrument carries numerous annotations that identify competing options, describe the negotiating range, and illuminate the drafter’s choices. The hope is that something novel can be gained—fresh insights can be suggested, and new questions can be raised (even if answering them remains elusive)—by advancing the dialogue about nuclear disarmament to the concrete stage of treaty drafting.

* Professor of Law, Georgetown University Law Center. The author gratefully thanks Robert (Bodie) Stewart and Kirsten A. Harmon for their extraordinarily careful and persistent research assistance; Dean William M. Treanor; participants in the Georgetown Law summer faculty research workshop; students in my “Issues in Disarmament: Proliferation and Terrorism” Seminar; and the following individuals who responded to my questions, commented upon prior drafts of this article, or otherwise generously assisted in its preparation: James M. Acton, Barry Blechman, James E. Goodby, Thomas Graham, Jr., Jonathan Granoff, Michael J. Mazarr, Christopher E. Paine, Steven Pifer, and Alyn Ware. © 2014, David A. Koplow.
GEORGETOWN JOURNAL OF INTERNATIONAL LAW

I. INTRODUCTION .................................................. 684

II. THE BACKGROUND FOR ZERO .................................. 687
A. The History of Zero ........................................... 688
B. The Law of Zero ................................................ 695
C. The Military Aspect of Zero ................................... 698
D. The Politics of Zero ............................................. 707
   2. Regional Nuclear Weapons Free Zone Treaties .......... 709

III. THE BIGGEST ISSUES ............................................ 711
A. Key Characteristics for a Valid Elimination Process ...... 711
B. Four Key Stumbling Points ................................... 715
   1. Definition of “Zero” ........................................ 715
   2. Verification and Enforcement ............................. 720
   3. Timing and the Negotiating Process ..................... 727
   4. Collateral Measures ....................................... 731

IV. DRAFT ZERO AGREEMENT ....................................... 734
V. DRAFT ZERO TREATY ........................................... 754
VI. CONCLUSION ..................................................... 779

"Where there is no vision, the people perish." Proverbs 29:18

I. INTRODUCTION

The vision of abolishing nuclear weapons—a goal to be achieved through a comprehensive, permanent, verifiable, and legally binding treaty—has been vigorously pursued with the Biblical objective of preventing the people around the world from perishing. This stunning image has become one of the most prominent, urgent, and controversial items on the contemporary international disarmament agenda, but the world today is so far from “getting to zero” that it is difficult, at our current heavily-armed, mutually-suspicious vantage point, even to imagine what such a profoundly different regime would look like.

Nuclear disarmament is also an idea that has experienced radical oscillations in attention, interest, and legitimacy. The goal of prohibiting nuclear weapons is as old as nuclear devices themselves, but the whole notion had long been derided as hopelessly idealistic or utopian, unfit for the deliberations of serious people and powerful countries. That dismissiveness, however, was suddenly punctured on January 4, 2007, when four of the most “realistic” senior U.S. statesmen—George P. Shultz, William J. Perry, Henry A. Kissinger, and Sam Nunn—
WHAT WOULD ZERO LOOK LIKE?

published a provocative essay, entitled "A World Free of Nuclear Weapons" in the Wall Street Journal. In that short piece, the Gang of Four upended the skeptics and inaugurated an outpouring of supportive reports and analyses, "me too" opinion columns from sympathetic converts to the cause of nuclear abolition, and endorsements by the President of the United States and by the Security Council of the United Nations.

To date, however, the wellspring of publication has been relatively heavy on the policy, strategy, technology, and military aspects of the question of nuclear abolition and relatively light on the legal dimension. This Article therefore posits that something additional can be gained—further insights can be achieved and additional questions can be posed, even if answering them remains puzzling—by advancing the dialogue to the stage of treaty drafting. The bulk of the Article, therefore, consists of two heavily annotated proposed international agreements (one intended for adoption relatively soon, the other for the distant future) describing in more concrete detail what a "zero regime" could look like.

The Article proceeds with the following structure: After this Introduction, Part II provides four elements of necessary background, including: (a) an abbreviated history of the concept of eliminating nuclear weapons, noting the erratic development, adoption, abandonment, and resurrection of the audacious idea; (b) an exploration of the fact that most of the countries of the world, including the United States, are already constrained by an important international legal obligation to pursue the objective of nuclear disarmament "in good faith"; (c) a survey of the world's existing nuclear arsenals, highlighting the clear and present dangers of proliferation and terrorism; and (d) an accounting of the contributions, but also the inadequacy, of historical and contemporary arms control efforts, including the Strategic Arms Limitation Treaties (SALT), the Strategic Arms Reduction Treaties (START) and an alphabet soup of other accords.

Part III then highlights several of the most difficult substantive issues emerging from the treaty-drafting exercise. Challenges such as: (a) the appropriate definition of "zero"; (b) the arrangements for verification and enforcement of the regime; (c) the articulation of the plausible series of intermediate stages on the road to abolition; and (d) important collateral questions such as the resolution or at least amelioration

---

of a range of vexing regional security issues are examined. The draft treaty texts cannot, at this point, offer definitive solutions, but may at least serve to highlight and clarify future challenges.

Parts IV and V present the heart of the matter: proposed texts for a Zero Agreement and a Zero Treaty. The first instrument would be a non-legally binding framework accord that could be adopted by participating states soon—perhaps in 2015—to re-commit themselves publicly, authoritatively, and collectively to the goal of nuclear elimination and to energize action on a prescribed pathway of specified steps in dedicated pursuit of that bold objective. The second document would be legally binding; it is intended for that point in the future when the countries of the world will have reduced their nuclear arsenals to very low levels and will have undertaken the other necessary precursor steps, so they will be ready, at last, to plunge forward to true abolition. The Zero Treaty is, necessarily, somewhat speculative—it will rely upon still undetermined technology and barely-imaginable political rapprochements to create more favorable conditions for accommodation, verification, and enforcement. For each document, the article presents a proposed text together with numerous annotations that highlight obvious and sub-surface problems, explain the drafter's choices, and suggest alternative formulations.

Finally, Part VI presents some conclusions and recommendations. The animating spirit for this effort is derived from a metaphor relied upon repeatedly by the Gang of Four, who liken the nuclear abolition exercise to undertaking to climb a distant mountain, when the top of the peak is now shrouded by clouds. From our current lowly starting point, we can only vaguely discern the shape of the summit, and we cannot ascertain what will be the most suitable path to scale it, how long it will take to ascend, or what severe challenges will have to be overcome en route. But we are determined to go forward, and we are dedicated to finding a route that will, somehow, empower eventual success.

Two special acknowledgements must be inserted. First, the author participated, under the leadership of retired ambassadors James E. Goodby and Thomas Graham, Jr., in a remarkable drafting exercise culminating in a high-level Joint Enterprise Workshop convened by George Shultz and William Perry at the Hoover Institution at Stanford University, July 25-26, 2012. Many of the issues articulated in this article and its draft documents were vetted at that conference, and the analysis was immensely improved thereby. Participants at that workshop, of course, are not responsible for what follows (still less for any errors or
WHAT WOULD ZERO LOOK LIKE?

omissions) and may not endorse the contents or concepts of this article, but they provided many important and useful insights.

Second, the author gratefully acknowledges the pioneering contributions of the one prior model for drafting a treaty in this area. An international consortium of legal, technical, and diplomatic experts, assembled by the Lawyers' Committee on Nuclear Policy, drafted a detailed and highly innovative Model Nuclear Weapons Convention (NWC) in 1997. The draft was submitted by Costa Rica to the United Nations, revised and updated in 2007, and distributed in 2008 by U.N. Secretary General Ban Ki-moon in his Five Point Proposal for Nuclear Disarmament as a starting point for multilateral negotiations. The materials contained in the current article differ significantly from the Model NWC (most prominently, in presenting two proposed documents, not just one) but the author has benefited greatly from consulting that first effort to articulate an operational legal text on point.

II. THE BACKGROUND FOR ZERO

As a preliminary matter, this section addresses, in turn, the (a) historical, (b) legal, (c) military, and (d) political dimensions of the pursuit of nuclear abolition. In the interest of space, each discussion is necessarily truncated, but the swelling literature regarding the elimination of nuclear weapons provides ample resources for further exploration.  


3. PHILIP TAUBMAN, THE PARTNERSHIP: FIVE COLD WARRIORS AND THEIR QUEST TO BAN THE BOMB (2012); GETTING TO ZERO: THE PATH TO NUCLEAR DISARMAMENT (Catherine McArdle Kelleher & Judith Reppy eds., 2011) [hereinafter GETTING TO ZERO]; REYKJAVIK REVISITED: STEPS TOWARD A WORLD FREE OF NUCLEAR WEAPONS (George P. Shultz et al. eds., 2008) [hereinafter REYKJAVIK REVISITED]; ELEMENTS OF A NUCLEAR DISARMAMENT TREATY (Barry M. Blechman & Alexander K. Bollfrass eds., 2010); CULTIVATING CONFIDENCE: VERIFICATION, MONITORING, AND ENFORCEMENT FOR A
A. The History of Zero

Even some of the scientists instrumental in the Manhattan Project, which centered on the development of atomic bombs during World War II, contemporaneously questioned whether the human species was capable of intelligently coping with the massive power then being unleashed, and almost immediately after the horror of Hiroshima and Nagasaki, populations around the world galvanized into political efforts to "ban the bomb." The new United Nations General Assembly devoted its very first resolution to the question of abolishing nuclear weapons, unanimously establishing an Atomic Energy Commission on January 24, 1946, and referring to it the urgent mission of developing specific proposals "for the elimination from national armaments of atomic weapons and of all other major weapons adaptable to mass destruction," and "for effective safeguards by way of inspection and other means to protect complying States against the hazards of violations and evasions."5

The most prominent early public expression of U.S. willingness to surrender its monopoly over nuclear weapons was the Baruch Plan, presented to the United Nations in June 1946. Under that remarkable structure, all existing atomic bombs would be destroyed and an international organization would succeed to all information and functions related to atomic energy—but only after the establishment of a strict
WHAT WOULD ZERO LOOK LIKE?

system of controls and immediate condign punishment for violations.  

The Soviet Union curtly rejected the Baruch Plan, apprehending it as a tool for Western espionage and domination, and insisting (in argumentation that echoes eerily into our own era) that the international control system should be effectuated only after the United States had dissolved its extant nuclear inventory and that any sanctions for violations should be imposed only by the Security Council (where Moscow retained a veto).  

The Cold War and its mutual suspiciousness then precluded any meaningful dialogue on nuclear weapons restraints through the 1950s. Partisans feuded inconclusively over whether any interim or partial measures of arms control could be concluded independently, as circumstances might permit, or would have to be inextricably linked to a pre-conceived overarching comprehensive program of universal arms control (soon known by the abbreviation GCD, for "general and complete disarmament"). During the 1960s and 1970s and into the 1980s, there was little talk about, and no appreciable progress toward, the ultimate desidera, and "serious people" rarely engaged in meaningful security consultation on that aspiration.  


A sudden, completely unforeseen—and wholly temporary—revival of interest in nuclear disarmament occurred at the October 11-12, 1986 summit meeting between U.S. President Ronald Reagan and Soviet General Secretary Mikhail Gorbachev in Reykjavik, Iceland. There, the two leaders—abandoning their respective cadres of national security advisors and running far beyond the anticipated modest agenda for the conference—came within a hair’s breadth of reaching an historic agreement to utterly eliminate their respective nuclear arsenals. At the last minute, such a tectonic shift eluded the leaders’ grasp, however, and its exact parameters—its precise content and timetable, the provisions for verification and enforcement, etc.—were never specified or reduced to draft text. Still, the Reykjavik “bolt from the blue” resonates through the international arms control community even today, empowering advocates of nuclear elimination to ponder what might have happened and emboldening them to contemplate its reprise.

Other insistent voices also helped sustain the goal of nuclear abolition. India’s Prime Minister Rajiv Gandhi, for example, presented his vision to the U.N. General Assembly in 1988. High-level international congresses—notably the 1996 Canberra Commission on the Elimination of Nuclear Weapons and the 2006 Blix Commission on Weapons of Mass Destruction—likewise kept the flame of disarmament alive.

---


10. See, e.g., IMPLICATIONS OF THE REYKJAVIK SUMMIT ON ITS TWENTIETH ANNIVERSARY (Sidney D. Drell & George P. Shultz eds., 2007); REYKJAVIK REVISITED, supra note 3; Thomas Blanton & Svetlana Savranskaya, Reykjavik: When Abolition Was Within Reach, ARMS CONTROL TODAY, Oct. 2011, available at http://www.armscontrol.org/act/201110/Reykjavik_When_Abolition_Was_Within_Reach.


Still, it is no exaggeration to claim that the commitment to nuclear disarmament had faded through the decades, almost to the point of extinction. Its occasional invocation felt largely ritualistic; it became basically devoid of impact on day-to-day national security policy and international negotiations. Hard-headed officials and their counterparts among the non-governmental cognoscenti simply ignored this objective and focused on other seemingly more tractable and proximate arms control issues. The goal of nuclear abolition had not been formally abandoned; it had just been overlooked for so long that it no longer hovered on the agenda for contemporary international action.14

Suddenly, however, the “Gang of Four” revivified the concept. This remarkable ad hoc assemblage consisted of George P. Shultz (Republican), Secretary of State in the Reagan administration, from 1982 to 1989;15 William J. Perry (Democrat), Secretary of Defense in the Clinton administration, from 1994 to 1997;16 Henry A. Kissinger (Republican), Secretary of State during the Nixon and Ford administrations, from 1973 to 1977;17 and Sam Nunn (Democrat), chairman of the Senate Foreign Relations Committee from 1987 to 1995.18 They are among the most prominent, authoritative, mainstream leaders on U.S. foreign and national security policy, with deep roots in the theory and practice of cold war strategy and diplomacy; individually—and certainly collectively—they command respect from across the U.S. and global national security community. When these four leaders speak in unison, others need not necessarily agree, but they have to pay attention—the mere act of endorsement by these elder statesmen guaranties that the concept of nuclear abolition can no longer be blithely dismissed as unrealistic, utopian, or impractical.

The Gang of Four—assisted and prodded by a cadre of senior associates who are themselves enormously prominent within the national security community, even if they are not quite “household names,”

---


14. See TAUBMAN, supra note 3, at 287 (reporting that for most nuclear experts in 2000, the idea of nuclear disarmament “bespoke a flaky idealism and profound ignorance about the realities of the nuclear age”); Frank Blackaby, Introduction and Summary, in NUCLEAR WEAPONS: THE ROAD TO ZERO 1, 6 (Joseph Rotblat ed., 1998) (noting that governments simply ignored recommendations to proceed toward nuclear disarmament).

15. See TAUBMAN, supra note 3, at 4.

16. See id. at 5.

17. See id. at 4.

18. See id. at 5.
such as Max Kampelman, Sidney Drell, and James Goodby—rattled the nuclear priesthood with their January 4, 2007 op-ed. They then persistently followed that initial broadside with additional salvos, also published in the Wall Street Journal, in 2008, 2010, 2011, and 2013, attracting renewed attention and a virtual “who’s who” of bipartisan endorsers.

Mikhail Gorbachev was an early ally, penning his own supportive column in the Wall Street Journal in January 2007; similar expressions soon came from prominent defense officials in the United Kingdom, Italy, Germany, and elsewhere. Of course, opposition voices were also...
emphatically expressed, including those of Harold Brown (Secretary of Defense in the Carter administration), James Schlesinger (Secretary of Defense under Presidents Nixon and Ford) and Richard Perle (Assistant Secretary of Defense under President Reagan). But a cottage industry of "zero" advocacy quickly sprang up, with a dramatic flow of books, articles, speeches, and movies; two non-governmental organizations adopted "getting to zero" as their pri-

---

30. Harold Brown & John Deutch, The Nuclear Disarmament Fantasy, WALL ST. J., Nov. 19, 2007, available at http://www.wagingpeace.org/articles/2007/11/26_brown_article_responses.php (arguing that "the goal, even the aspirational goal, of eliminating all nuclear weapons is counterproductive" and "there is no realistic path to a world free of nuclear weapons").

31. See Taubman, supra note 3, at 14 (quoting Schlesinger's 2010 speech stating that "[t]he dividing line between vision and hallucination is never very clear.").


33. Sidney D. Drell & James E. Goodby, A World Without Nuclear Weapons: End-State Issues (2009) [hereinafter END-STATE ISSUES]; IMPLICATIONS OF THE REYKJAVIK SUMMIT ON ITS TWENTIETH ANNIVERSARY (Sidney D. Drell & George P. Shultz eds., 2007); REYKJAVIK REVISITED, supra note 3; GETTING TO ZERO, supra note 3; CULTIVATING CONFIDENCE, supra note 3; RUSSIA AND THE DILEMMAS OF NUCLEAR DISARMAMENT (Alexei Arbatov et al. eds., 2012).


35. See Taubman, supra note 3, at 458 (listing speeches related to nuclear disarmament after the Gang of Four Op Ed columns). Notably, during the 2008 presidential election campaign, both Barack Obama and John McCain formally endorsed the concept of nuclear disarmament. Id. at 335, 342-43.

36. Id. at 340 (describing “Countdown to Zero” and “Nuclear Tipping Point”).

37. Id. at 338-40 (noting shared goals, but different approaches by—and some tension between—the Nuclear Threat Institute (headed by Sam Nunn) and Global Zero (headed by Bruce Blair, Matt Brown and Barry Blechman)); see also Randy Rydell, Advocacy for Nuclear
mary mandate.38

The most important endorsement came from President Barack Obama, in his celebrated April 5, 2009 speech in Prague.39 There, citing the persistent and growing dangers of nuclear warfare, the imperative of avoiding any insidious "fatalism" about the inevitability of further proliferation, and the special responsibility of the United States, as the only country ever to have used nuclear weapons in combat, he declared:

So today, I state clearly and with conviction America's commitment to seek the peace and security of a world without nuclear weapons. I'm not naive. This goal will not be reached quickly—perhaps not in my lifetime. It will take patience and persistence. But now we, too, must ignore the voices who tell us that the world cannot change. We have to insist, "Yes, we can."40

Six months later, Obama chaired a heads-of-state session of the U.N. Security Council (the first time a U.S. president had done so) and led the advocacy in support of the unanimous adoption of resolution

Disarmament: A Global Revival?, in Getting to Zero, supra note 3, at 30-32 (identifying numerous public and private sector "recent initiatives" aimed at nuclear disarmament).

38. In 2012, the International Campaign to Abolish Nuclear Weapons reported that its survey of governmental positions regarding a proposed new treaty to ban nuclear weapons revealed that 146 countries supported the immediate commencement of negotiations leading to such a treaty, 22 were "on the fence," and 26 opposed. Tim Wright, Towards a Treaty Banning Nuclear Weapons: A Guide to Government Positions on a Nuclear Weapons Convention (2012).

39. Barack Obama, President of the United States, Speech in Prague, Czech Republic (Apr. 5, 2009), available at http://www.whitehouse.gov/the_press_office/Remarks-By-President-Barack-Obama-In-Prague-As-Delivered/ [hereinafter Prague Speech]. The concept was also endorsed in the April 2010 Nuclear Posture Review Report, the Department of Defense's top-level "roadmap for implementing President Obama's agenda for reducing nuclear risks to the United States, our allies and partners, and the international community." U.S. Dept. of Defense, Nuclear Posture Review Report (2010). In a section entitled "Looking Ahead: Toward a World Without Nuclear Weapons," the NPR Report concludes that "[t]he long-term goal of U.S. policy is the complete elimination of nuclear weapons. At this point, it is not clear when this goal can be achieved" and that "[t]he conditions that would ultimately permit the United States and others to give up their nuclear weapons without risking greater international instability and insecurity are very demanding . . . Clearly, such conditions do not exist today. But we can—and must—work actively to create those conditions." Id. at 45-49.

40. Prague Speech, supra note 39; see also Barack Obama, President of the United States and Dmitry Medvedev, President of the Russian Federation, Joint Statement, Apr. 1, 2009, in End-State Issues, supra note 33, at 1-2 (committing both countries to achieve a nuclear weapons free world).
1887. In it, the Security Council, "[r]esolving to seek a safer world for all and to create the conditions for a world without nuclear weapons," and "[r]eaffirming that proliferation of weapons of mass destruction, and their means of delivery, constitutes a threat to international peace and security," called upon parties to the 1968 Nuclear Non-Proliferation Treaty (NPT) to pursue the treaty-specified negotiations in good faith on nuclear arms reduction and disarmament, and similarly called on NPT non-parties to join that endeavor.

To conclude this chronology on a downbeat note, it must be observed that the momentum for taking meaningful steps toward the elimination of nuclear weapons has faded in 2011-2013. The advocates have not changed their minds or abandoned the enterprise, but no new major accomplishments have been recorded, and no new groundswell of additional political support has emerged—indeed, there has been retrograde movement, with a renewed emphasis on nuclear weapons and revivified nuclear postures. Whether this faltering signals that the wave of enthusiasm for zero has already crested, or whether it is merely a temporary pause before even greater political and popular support emerges, will soon be tested.

B. The Law of Zero

The lodestar for legal analysis of nuclear weapons is the Nuclear Non-Proliferation Treaty, arguably the most important arms control...
agreement in history. This instrument constitutes a grand bargain between the “nuclear weapon states” (NWS) (a set identical to the five permanent members (the P5) of the U.N. Security Council)\(^4^8\) and the “non-nuclear weapon states” (NNWS) (i.e., everyone else).\(^4^9\) The NPT rests upon three related “pillars”: non-proliferation (the NNWS pledge never to manufacture or otherwise acquire nuclear weapons\(^5^0\)); disarmament (the NWS commit to measures of arms control, as elaborated below\(^5^1\)); and peaceful uses of nuclear energy (all parties without discrimination retain the right to pursue the full array of non-military applications of nuclear energy, subject to international safeguards to prevent diversion of the materials, facilities and expertise into weapons programs\(^5^2\)).

Of special interest in this context is article VI of the NPT, which contains the fundamental commitment (levied upon the NWS and NNWS alike) regarding the disarmament pillar:

Each of the Parties to the Treaty undertakes to pursue negotiations in good faith on effective measures relating to cessation of the nuclear arms race at an early date and to nuclear disarmament, and on a Treaty on general and complete disarmament under strict and effective international control.\(^5^3\)

Article VI therefore constitutes a bold, explicit, and relatively clear-cut international law commitment, binding upon the treaty’s 189

\(^4^8\) In the NPT, “a nuclear-weapon State is one which has manufactured and exploded a nuclear weapon or other nuclear explosive device prior to January 1, 1967.” NPT, supra note 44, art. IX.3. This includes the United States, the Soviet Union/Russia, the United Kingdom, France, and China.

\(^4^9\) Regarding the history, structure, importance, and challenges of the NPT, see Arms Control I, supra note 4, at 288-309. See also William Epstein, The Non-Proliferation Treaty and the Review Conferences 1965 to the Present, in 2 Encyclopedia of Arms Control and Disarmament 855 (Richard Dean Burns ed., 1993); Arms Control II, supra note 4, at 148-72; Reviewing the Nuclear Nonproliferation Treaty (Henry Sokolski ed., 2010), available at http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=987; Rebuilding the NPT Consensus (Michael May ed., 2007).

\(^5^0\) NPT, supra note 44, art. II.

\(^5^1\) Id. art. VI.

\(^5^2\) Id. art IV.

\(^5^3\) Id. art. VI; see Scott D. Sagan, Good Faith and Nuclear Disarmament Negotiations, in Debate, supra note 3, at 203-12.
WHAT WOULD ZERO LOOK LIKE?

parties" (virtually all the states in the world except India, Israel, North Korea and Pakistan—each of which possesses nuclear weapons), obligating them to pursue nuclear disarmament in good faith.

Nevertheless, controversy has always surrounded the NPT, especially regarding insistent claims by several NNWS that the NWS have been insufficiently zealous and successful in their obligatory pursuit of nuclear disarmament, and have thereby perpetuated the "discriminatory" structure of the NPT.56 Particularly in 1995, when the treaty was "extended" beyond its original twenty-five year duration, the "have-not" countries extracted renewed commitments from the "have" states to accelerate their pursuit of zero; at the 2000 NPT Review Conference, that renewal of vows was captured in a series of specified "practical steps."57

The International Court of Justice (ICJ), the judicial organ of the United Nations,58 was drawn into the fray when the General Assembly requested an advisory opinion regarding the legality of the threat or use of nuclear weapons.59 In a 1996 decision correctly characterized as being both pathbreaking in its articulation of legal principles and confounding in its circumlocution and indecision, the ICJ determined,


55. Arms Control and Proliferation Profile: North Korea, Arms Control Ass’n, http://www.armscontrol.org/factsheets/northkoreaprofile (last updated Apr. 2013) (noting that North Korea had joined the NPT, then withdrew from it in 2003; the United Nations Security Council has ordered North Korea to return to the treaty, but it has not done so).

56. Ramesh Thakur, The Desirability of a Nuclear Weapon Free World, in Canberra Commission on the Elimination of Nuclear Weapons, Background Papers 74, 83-85 (1996) (arguing that "[t]he NPT is discriminatory, is seen as discriminatory, and will be progressively delegitimised unless there is continual movement towards nuclear disarmament."); Waheguru Pal Singh Sidhu, India and Nuclear Zero, in Getting to Zero, supra note 3, at 224, 232 (noting that India's longstanding critique of the NPT includes its discriminatory nature); Thomas Graham, Jr., NPT Article VI Origin and Interpretation, in Rebuilding the NPT Consensus, supra note 49, at 45, 51-61.


58. U.N. Charter art. 92; Statute of the International Court of Justice art. 1, June 26, 1945, 3 Bevans 1179.

inter alia, that: (a) nuclear weapons were governed by the same law of armed conflict principles applicable to all other weapons;\(^6\) (b) all parties to the NPT are bound by the article VI commitment not only to pursue nuclear disarmament in good faith, but to successfully conclude their negotiations and achieve the desired result;\(^6\) (c) the widespread, severe, and long-lasting effects of nuclear weapons mean that their use is "scarcely reconcilable" with the legal requirements of proportionality and avoidance of civilian casualties;\(^6\) and (d) nevertheless, the court could not definitively conclude that all possible uses of nuclear weapons would be illegitimate—such as firing against an isolated military target far removed from civilian areas, or in an instance where a nation’s very survival depended upon the application of such overwhelming force.\(^6\)

C. The Military Aspect of Zero

The current "box score" of global holdings of nuclear weapons is somewhat complex because it must differentiate states that currently possess nuclear weapons, states that formerly possessed them, states with considerable current potential to develop them, and other nuanced categories. The NPT acknowledges five of its parties as long-time NWS possessors of nuclear weapons: China, France, Russia, the United Kingdom, and the United States.\(^6\) In addition, three non-NPT states

---

60. ICJ Advisory Opinion on Nuclear Weapons, supra note 59, ¶ 105 (2) C and D (unanimously concluding that the provisions of the UN Charter and of international humanitarian law apply to the threat or use of nuclear weapons).

61. Id. ¶ 105 (2) F (unanimously).

62. Id. ¶ 95.

63. Id. ¶ 105 (2) E (by seven votes to seven, with the president of the court casting the deciding vote).

have overtly tested and produced nuclear weapons: India, North Korea, and Pakistan.\textsuperscript{65} Israel, another NPT non-party, is widely credited with a nuclear weapon inventory, but it has not publicly acknowledged that status.\textsuperscript{66}

In addition, a handful of other states formerly possessed nuclear weapons. When the U.S.S.R. dissolved in 1991, some of its massive nuclear arsenal was suddenly “inherited” by successor states Belarus, Kazakhstan, and Ukraine; after difficult negotiations, each of those new republics shipped the nuclear warheads back to Russia.\textsuperscript{67} South Africa is a special case of “rollback”: the apartheid regime had secretly constructed a small nuclear weapons stockpile in the 1980s, but then dismantled it and the weapons infrastructure, shortly before the institution of majority rule in the country.\textsuperscript{68} In addition, several states, including Cuba, Czechoslovakia, East and West Germany, Italy, South Korea, and Turkey, have allowed one of the superpowers to base nuclear weapons on their territories, under secret arrangements that may have afforded the host some degree of influence over any


\textsuperscript{66} See Arms Control and Proliferation Profile: Israel, ARMS CONTROL Ass’n, http://www.armscontrol.org/factsheets/israelprofile (last updated July, 2013) (noting that Israel is considered to have a substantial nuclear arsenal, although it has not officially acknowledged any, and maintains that it “will not be the first country to introduce nuclear weapons into the Middle East”); Country Profile: Israel, NUCLEAR THREAT INST, http://www.nti.org/country-profiles/israel/nuclear/ (last updated Aug., 2013); see generally Avner Cohen, Israel’s Nuclear Future: Iran, Opacity, and the Vision of Global Zero, in GETTING TO ZERO, supra note 3, at 187-205.


potential use.\textsuperscript{69}

The next category would embrace states that have pursued a nuclear weapons capability with some degree of vigor and some measure of success, without (at least yet) completing the program. Iran is currently the country most precariously poised on the threshold of acquiring a nuclear weapons capacity;\textsuperscript{70} Syria\textsuperscript{71} and Libya\textsuperscript{72} are similar relatively recent examples. Going somewhat further back in time, Argentina, Brazil, South Korea, and several others would fit the description.\textsuperscript{73} Moreover, there are several states that could probably develop nuclear weapons in short order—they possess the indigenous intellectual, physical, economic, and other resources—but they have as a policy and legal matter rejected that avenue. Perhaps forty countries—Australia, Canada, Germany, Japan, Sweden, Switzerland, and many other NATO members—would be characterized this way.\textsuperscript{74}

Finally, it must be acknowledged that just about any state potentially could be implicated in the acquisition of nuclear weapons or their critical components. Hypothetically, almost any location on earth could be utilized (with the active collaboration of the relevant government, or perhaps without its knowledge) by another state for secretly

---

\textsuperscript{69} Rose Gottemoeller, Eliminating Short-Range Nuclear Weapons Designed to Be Forward Deployed, in REYKJAVIK REVISTED, supra note 3, at 107, 155 (depicting U.S. short-range nuclear weapons deployed in seven European countries in 2005).


WHAT WOULD ZERO LOOK LIKE?

hiding a weapon or components or undertaking other key actions.\textsuperscript{75} An area beyond the jurisdiction of any country—such as the high seas or Antarctica—could likewise be exploited.\textsuperscript{76} So a disarmament treaty’s verification regime would have to be of universal application.

An additional set of definitional and taxonomic points must also be briefly addressed. The term “nuclear weapon” is itself ambiguous. Sometimes, that designator embraces both of the two indispensable elements: the nuclear explosive component (a missile warhead, artillery shell, bomb, etc.) and the “delivery vehicle” (the missile, projectile, aircraft, etc. that is used to transport the explosive to its target); sometimes, “weapon” refers only to the explosive. Usually (including in this article), discussion about eliminating nuclear weapons focuses principally upon the explosives, but any comprehensive treaty must also address the question of retention, limitation, or modification of nuclear-capable delivery systems.\textsuperscript{77}

Nuclear-armed delivery systems are often categorized by the mission they are assigned or the range they are capable of reaching; the vocabulary is not well standardized, but the customary three tiers are: “strategic” (consisting of inter-continental ballistic missiles (ICBMs), submarine-launched ballistic missiles (SLBMs), and heavy bombers,
with ranges generally exceeding 5500 kilometers);"intermediate,"
"theater," or "medium-range," and "tactical" or "battlefield" (with
ranges generally under 500 kilometers). Furthermore, weapons may
be classified as "deployed" (i.e., in operational status); "non-deployed"
(including systems that are undergoing repair or maintenance); "re-
serve" (not mated to a delivery system, but available in principle for a
return to deployed status); "retired" (removed from the active-duty
stockpile, with no intention of being maintained in operational condi-
tion); and "awaiting disassembly" (in the queue for dismantling—a
status that can linger for years, depending on the availability of appro-
priate facilities).

At a deeper level of detail, nuclear disarmament advocates must
address the "components" of a nuclear weapon—if a treaty regime

78. See Treaty Between the United States of America and the Russian Federation on Measures
for the Further Reduction and Limitation of Strategic Offensive Arms, U.S.-Russ., Protocol, Part 1,
nuclear weapons covered by the treaty); Amy F. Woolf, Cong. Research Serv., RL33640, U.S.

79. See Treaty Between the United States of America and the Union of Soviet Socialist
Republics On the Elimination of Their Intermediate-Range and Shorter-Range Missiles, U.S.-
Treaty]; Steven Pifer & Michael E. O’Hanlon, The Opportunity: Next Steps in Reducing
Nuclear Arms 81-112 (2012).

Steven P. Andreasen, Verifying Reductions and Elimination of Tactical Nuclear Weapons, in Cultivating
Confidence, supra note 3, at 213-28; Rose Gottemoeller, Eliminating Short-Range Nuclear Weapons
Designed to Be Forward Deployed, in Reykjavik Revisited, supra note 3, at 107-57; Viktor Esin,
Tactical Nuclear Weapons: Their Modern Military Role and Arms Control Proposals, and Steven Pifer,
Nonstrategic Nuclear Weapons, Policy and Arms Control; Issues for the United States, NATO and Russia, in
Natural Resources Defense Council, From Mutual Assured Destruction to Mutual Assured Stability:
Exploring a New Comprehensive Framework for U.S. and Russian Nuclear Arms Reductions 57,
March2013.pdf.

81. See U.S. Dept. of Defense, Fact Sheet: Increasing Transparency in the U.S. Nuclear Stock-
pile (May 3, 2010), http://www.defense.gov/npr/docs/10-05-03_Fact_Sheet_US_Nuclear_
Transparency_FINAL_w_Date.pdf (defining the "nuclear stockpile" as including "active" war-
heads (including strategic and non-strategic weapons maintained in an operational, ready-to-use
configuration, as well as weapons that could be available for deployment in a short time, and
spares) and "inactive" warheads (maintained at a depot in non-operational status); a "retired"
warhead has been removed from its delivery vehicle, is not functional, and is in a queue for
dismantlement; a "dismantled" warhead has been reduced to its component parts); U.S. Dept. of
mm/nm_book511/index.htm (describing composition of U.S. nuclear weapons stockpile);
New START, supra note 78, Protocol, Part 1, §§ 12-17, 47-52 (differentiating "deployed" from
"non-deployed" weapons). Other countries may not use the same categories or vocabulary.
requires "destruction" of a nuclear weapon, may a state nonetheless retain some disassembled pieces of the device, and if so, what are the appropriate accountable constituent elements? The phenomenon of "dual capability" is a persistent problem here—many of the same substances, equipment, facilities and knowledge that are essential to producing and sustaining nuclear weapons are also relevant to a full range of benign applications across the civilian economy.\textsuperscript{82}

The most important, unique ingredient in a nuclear explosive device is the fissile material—the highly-enriched uranium or plutonium that undergoes the fission reaction providing the massive amounts of explosive energy. The NWS have produced enormous inventories of fissile material—officially undisclosed, but estimated at 1,440 tons of highly enriched uranium and 485 tons of plutonium\textsuperscript{83}—some of which is adaptable not only for weapons, but also for use in nuclear power plants, naval reactors, nuclear medicine, isotopic thermal generators (for deep space missions), and other benign applications. Monitoring those secret mountains of hazardous radioactive elements will be a critical challenge; the International Atomic Energy Agency currently considers only twenty-five kilograms of highly enriched uranium, or eight kilograms of plutonium, to be a "significant quantity," approximating the minimum amount supposedly needed for a first-generation nuclear weapon, and therefore justifying the closest scrutiny.\textsuperscript{84}

---

\textsuperscript{82} Regarding dual capability of nuclear materials, equipment and technology, see Nuclear Suppliers Group, Guidelines for Transfers of Nuclear-Related Dual-Use Equipment, Materials, Software, and Related Technology, \url{http://www.nuclearsuppliersgroup.org/A_test/01-eng/09-guide.php?%20button=91} (last visited Nov. 10, 2013). See also Int’l Atomic Energy Agency [IAEA], Communications Received from Certain Member States Regarding Guidelines for Transfers of Nuclear-Related Dual-Use Equipment, Materials, Software and Related Technology, IAEA Doc. INFCIRC/254/Rev.7/Part 2a (Mar. 20, 2006), available at \url{http://www.iaea.org/Publications/Documents/Infcircs/2006/infcirc254r7p2.pdf}. Many of the ingredients of a nuclear weapon, such as the neutron reflector, are unique for this purpose and would not be suitable for many other functions; however, some components, such as the casing, the power supply, the fusing and arming systems, the altimeters, and the parachutes, might be more adaptable for some conventional weapons or for selected civil industrial purposes.


\textsuperscript{84} See Limits to the Safeguard System, Int’l Atomic Energy Agency (IAEA), \url{http://www.iaea.org/Publications/Booklets/Safeguards/pia3810.html} (last visited Nov, 10, 2013) (IAEA focuses on the approximate quantity of material necessary to manufacture a nuclear weapon—about 25kg of
Importantly, the disassembly of a nuclear weapon is not necessarily irrevocable; a crucial element in a zero regime would be procedures to guard against reconstitution of a weapons capacity that had apparently been eliminated. As long as a country retains the essential building blocks and knowledge, it has an inherent capability for reassembly, as well as for new construction "from scratch." The function of the legal regime, therefore, would be to ensure that any such nuclear renaissance would not be swift or secret.

Conceptually, a major issue in the strategic design of the verification apparatus is how far "backwards" it must extend into the production cycle for a nuclear weapon. That is, would it be sufficient for the future stability of the regime to ensure only the "first level" —the internationally monitored disassembly all nuclear weapons and the secure storage or destruction of the components? Or must the control system also intrude more deeply into the production process, ensuring the disassembly of those critical components, together with international scrutiny of the storage or destruction of the resulting subcomponents? Or, in pursuit of still greater long-term reliability, would the treaty mechanism have to apply safeguards to all the facilities at which weapons components and subcomponents are manufactured, processed, and assembled for various purposes, including purposes far removed from nuclear weaponry?

Finally, nuclear weapons require a considerable physical infrastructure: laboratories to design and develop the weaponry; sites to conduct explosive developmental and proof testing; specialized installations to assemble and maintain the devices; and military institutions to

highly enriched uranium or 8kg of plutonium); Christopher E. Paine, Thomas B. Cochran & Robert S. Norris, Technical Realities Confronting Transition to a Nuclear Weapon Free World, in CANBERRA COMMISSION ON THE ELIMINATION OF NUCLEAR WEAPONS, BACKGROUND PAPERS, supra note 56, at 109, 119-23 (criticizing the IAEA’s calculation of significant quantities).

85. Perkovich & Acton, supra note 8, at 102-104.

86. Simultaneously, the control system for a disarmament regime would have to ensure against diversion of nuclear materials from permitted peaceful nuclear applications, such as electricity generation.

87. The author is indebted to Chris Paine for this insight, as well as for the illustration of the application of the problem in Syria today, regarding chemical weapons. There, the international community seeks to preclude any future availability of chemical weapons, by destroying the existing arms, the precursor chemicals that could be combined to create new weapons, and the relevant production and handling facilities. See also Holdren, supra note 4; SIDNEY D. DREULI & RAYMOND JAENILAS, Nuclear Deterrence in a World Without Nuclear Weapons, in DETERRENCE: ITS PAST AND FUTURE 99-129 (George P. Shultz et al. eds., 2011).
Deploy the weapons and train the operators—all of which have possible implications for a treaty-drafting exercise.\(^{88}\)

Within those parameters, assessments vary about the current nuclear weapons holdings of individual countries, as intense secrecy usually surrounds all aspects of states’ nuclear arms. By some estimates, the United States has about 7,700 intact nuclear weapons, including 4,700 “stockpiled” weapons (about 1,700 deployed strategic weapons, 500 tactical weapons, and 2,500 weapons in reserve storage) and about 3,000 “retired” weapons.\(^{89}\) Russia is generally credited with about 8,500 total weapons, of which about 4,480 are currently in the stockpile (fewer deployed strategic weapons than the United States, but many more tactical weapons).\(^{90}\) Estimates for China (250),\(^{91}\) France (300)\(^{92}\) and the United Kingdom (225)\(^{93}\) are less detailed. The indications for

---

88. Christopher E. Paine, Thomas B. Cochran & Robert S. Norris, The Arsenals of the Nuclear Weapons Powers, in CANBERRA COMMISSION ON THE ELIMINATION OF NUCLEAR WEAPONS, BACKGROUND PAPERS, supra note 56, at 8, 28 (identifying major nuclear infrastructure elements—including assembly/disassembly plants, plutonium production reactors, uranium enrichment plants, and chief design labs—for each of the P5); DEBATE, supra note 3, at 53-54.


90. Kristensen & Norris, supra note 89, at 76, 79 (noting that Russia has 4,480 nuclear weapons in the stockpile (including 1,800 deployed) and 4,000 retired); PAVEL POPOV, IFRI SEC. STUDIES CTR., RUSSIA’S NUCLEAR FORCES: BETWEEN DISARMAMENT AND MODERNIZATION (2011).

91. Kristensen & Norris, supra note 89, at 79 (noting predictions that the Chinese nuclear arsenal is likely to increase); DEBATE, supra note 3, at 27.

92. Kristensen & Norris, supra note 89, at 79 (noting that France intends to reduce its arsenal to slightly fewer than 300); see generally Venance Journe, France’s Nuclear Stance: Independence, Unilateralism, and Adaptation, in GETTING TO ZERO, supra note 3, at 124-48; DEBATE, supra note 3, at 26.

93. Kristensen & Norris, Global Nuclear Weapons Inventories, supra note 89, at 79 (also noting that the United Kingdom plans to reduce its stockpile to 180 warheads, of which 120 will be operationally available and 40 deployed); see generally Ian Anthony, British Thinking on Nuclear Weapons, in GETTING TO ZERO, supra note 3 at 102-23; DEBATE, supra note 3, at 26.
the non-NPT members are even more speculative: India (110), Israel (80), North Korea (fewer than 10) and Pakistan (120). By all calculations, the current global population of nuclear weapons is far lower than at earlier times—at its peak, in 1967, the United States possessed 31,000 weapons; the zenith for the Soviet Union, in 1986, was over 40,000. However, this downward trend may now be ending with the United States, France, and the United Kingdom seemingly intending to make only modest reductions in the future, and the other states on an upward trajectory.

Non-state actors may be relevant to the story here, too. Unlike chemical or biological weapons, which might be home-brewed by a dedicated, well-funded terrorist organization, construction of an indigenous nuclear weapon, beginning with the production of the requisite fissile material, is beyond the reach of entities other than those affiliated with sophisticated states. But a technically competent non-state actor with access to plutonium or highly-enriched uranium could plausibly have the capability to assemble an effective improvised nuclear device with significant explosive power. Theft or donation of a quantity of fissile material from a failing or rogue state may be assessed as unlikely, but perhaps it is not as implausible as it should be; the specter of the world’s most deadly weapons in the hands of the world’s most violent actors therefore provides both a strong motivation for

94. Kristensen & Norris, supra note 89, at 80 (noting that Indian and Pakistani nuclear weapons are thought to be held in central storage, not operationally deployed).
95. Id. at 80.
96. Id. at 80 (noting that North Korea has not yet demonstrated that it has operationalized any nuclear weapons); Frank Valliere, Enforcement Scenario: North Korea, in ELEMENTS OF A NUCLEAR DISARMAMENT TREATY, supra note 3, at 271-91.
98. Id. at 78; FISSILE MATERIAL PANEL, supra note 85, at 50-58.
100. Id.
102. Andrew Mack, Nuclear 'Breakout': Risks and Possible Responses, in CANBERRA COMMISSION ON THE ELIMINATION OF NUCLEAR WEAPONS, BACKGROUND PAPERS, supra note 56, at 208, 217 (“Terrorist organizations do not have the scientific, technological, material or financial resources needed to produce fissile material.”). But see Harold A. Feiveson, Civilian Nuclear Power in a Nuclear-Weapon-Free World, in ELEMENTS OF A NUCLEAR DISARMAMENT TREATY, supra note 3, at 57, 70 (suggesting that a sophisticated sub-state group could construct a crude nuclear weapon).
WHAT WOULD ZERO LOOK LIKE?

pursuit of zero and a highly stressing set of conditions that a viable nuclear disarmament regime must satisfy. \(^{103}\)

D. The Politics of Zero

In pursuit of safety and security, the world’s leading countries—especially the United States and the Soviet Union/Russia, which have always possessed the lions’ share of the nuclear inventories—have negotiated a series of canonical, but only partially successful, bilateral, plurilateral, and multilateral nuclear arms control treaties. This sequence provides the edifice upon which any nuclear disarmament agreements would be constructed; it can be organized into three components.

1. Bilateral U.S.-U.S.S.R. Agreements

The oscillations of cold war, détente and contemporary politics have generated a sputtering stream of major nuclear arms control agreements, beginning in the SALT I (1972) negotiations\(^{104}\) which spawned two ground-breaking accords, the Anti-Ballistic Missile (ABM) Treaty\(^{105}\) (which sharply restricted defensive systems intended to shoot down incoming nuclear warheads) and the Interim Agreement on Strategic Offensive Arms\(^{106}\) (which essentially froze then-current inventories of ICBM and SLBM launchers). Both documents have terminated. The SALT II Treaty\(^{107}\) (1979), which would have continued the arms control process, failed to gain the consent of the U.S. Senate, and therefore never entered into force. The Intermediate Nuclear Forces

\(^{103}\) See 2010 Op Ed, supra note 24 ("We face a very real possibility that the deadliest weapons ever invented could fall into dangerous hands."); NWC, supra note 2, at 118-19 (discussing terrorist use of nuclear weapons).

\(^{104}\) CALVO-GOLLER & CALVO, supra note 77; ARMS CONTROL II, supra note 4, at 219-254; Thomas Graham, Jr., NPT Article VI Origin and Interpretation, in REBUILDING THE NPT CONSENSUS, supra note 49, at 34-49; Woolf, supra note 78.


(INF) Treaty\textsuperscript{108} (1987), banning land-based missiles of intermediate and shorter range, is of indefinite (i.e., permanent) duration.\textsuperscript{109}

The subsequent START I Treaty\textsuperscript{110} (1991) inaugurated actual reductions in U.S. and Soviet deployed strategic nuclear weapons (in contrast to merely capping their increases). It expired in 2009.\textsuperscript{111} A successor START II\textsuperscript{112} (1993) was negotiated and signed but never brought into force. The Strategic Offensive Arms Reduction Treaty\textsuperscript{113} (SORT or Moscow Treaty) (2002) was a very brief document, built upon START I, which further reduced the number of operationally-deployed strategic nuclear warheads each party was allowed; it was superseded and terminated in 2011.\textsuperscript{114} The New START Treaty (2010) is the currently-applicable bilateral strategic nuclear arms control instrument; it limits each party to 1,550 deployed warheads (counted in such a way that many are excluded from the official tally) and 700 operational delivery systems by 2018.\textsuperscript{115} As of this writing, no follow-on U.S.-Russia nuclear arms control negotiations are under way, with Moscow having repeatedly rebuffed U.S. overtures.\textsuperscript{116}

\begin{thebibliography}{99}

\bibitem{inf} INF Treaty, \textit{supra} note 79.
\bibitem{start-i-fact-sheet} \textit{Id.} art. XVII.2 (specifying a 15 year duration); \textit{START I Fact Sheet}, ARMS CONTROL ASSOCIATION, http://www.armscontrol.org/factsheets/start1 (last visited Mar. 25, 2014).
\bibitem{new-start} New START, \textit{supra} note 78, art. XIV.A.
\bibitem{new-start-art-ii} \textit{Id.} art. II.
\end{thebibliography}
WHAT WOULD ZERO LOOK LIKE?

2. Regional Nuclear Weapons Free Zone Treaties

In a series of local initiatives, the NNWS countries in several distinct geographic regions have united to foreclose any incipient nuclear arms races. The first of these, applicable to Latin America and the Caribbean, also attracted the participation of the NWS through a series of protocols in which they pledged to respect the nuclear weapons-free nature of the zone. It has been followed by cognate agreements regarding the South Pacific, South East Asia, Central Asia, and Africa, which have entered into force, but are still somewhat works-in-progress in terms of full zonal state and P5 participation. A similar zone has been proposed for the Middle East.

3. Global Treaties Related to Nuclear Weapons

In addition to the NPT, the world has crafted a series of specialized accords that regulate nuclear weapons in various respects. The Limited

---


Test Ban Treaty (LTBT)\textsuperscript{124} (1963) prohibits test explosions of nuclear weapons except in deep underground chambers, where the radioactive contaminants could be safely contained. The LTBT has attracted 126 parties.\textsuperscript{125} The Outer Space Treaty\textsuperscript{126} (1967), now joined by 101 states,\textsuperscript{127} includes a prohibition against placing nuclear weapons in orbit or installing them on the moon or other celestial bodies.\textsuperscript{128}

The Comprehensive Nuclear Test Ban Treaty (CTBT)\textsuperscript{129} (1996) extends the LTBT by banning nuclear tests in all environments, including underground, thereby arresting further development of additional nuclear weapons capabilities. By its terms, the CTBT will not enter into force until ratified by 44 designated countries, several of which (including the United States and China) have persistently failed to do so.\textsuperscript{130} Although the immediate prospects for prompt effectuation of this treaty are not bright, it is hard to imagine advanced progress toward nuclear disarmament until that is accomplished.\textsuperscript{131}


\textsuperscript{128} Outer Space Treaty, \textit{supra} note 126, art. IV.


\textsuperscript{130} \textit{Id.} art. XIV, annex 2; \textit{See Comprehensive Nuclear Test Ban Treaty, \textit{United Nations Office for Disarmament Affairs} (UNODA), http://disarmament.un.org/treaties/t/ctbt (last visited Nov. 12, 2013) (listing which required states have not yet ratified the treaty); OLA DAHLIN, JENIFER MACKBY, SVEIN MYKKELVETT & HEIN HAAT, \textit{Detect and Deter: Can Countries Verify the Nuclear Test Ban 13-20} (Springer 2011) (surveying prospects for ratification of the CTBT in the states whose membership is necessary for the treaty to enter into force); JONATHAN MEDALIA, Cong. Research Serv., RL 33548, \textit{Comprehensive Nuclear-Test-Ban Treaty: Background and Current Developments} (2013).

WHAT WOULD ZERO LOOK LIKE?

Finally, one other element on the multilateral nuclear arms control agenda must be noted. A Fissile Material Cutoff Treaty (FMCT) would constitute an agreement to bar the production of additional highly enriched uranium and plutonium for weapons; it could also include accounting of past production of the critical isotopes and more stringent controls upon stockpiles. FMCT has long been high on the list of arms control priorities; however, its pursuit has been persistently stifled by international political discord. Overcoming those frustrations would be an essential precondition for nuclear disarmament. For purposes of the draft treaty documents below, it is assumed that—somehow—a viable cutoff treaty will eventually be developed in the years to come.

III. THE BIGGEST ISSUES

Negotiators and drafters of the instruments designed to pursue nuclear disarmament will be compelled to confront a daunting array of challenges. Several of these choice-points are identified in multiple footnotes attached to the Zero Agreement and Zero Treaty in the subsequent sections of this article, but a few are so important and complex that further textual elaboration is required. This section will first describe the eleven characteristics necessary for an adequate elimination regime and will then continue by illuminating the critical problems of: (a) the definition of "zero"; (b) verification and enforcement of compliance; (c) timing and the negotiating process; and (d) collateral measures.

A. Key Characteristics for a Valid Elimination Process

Just as important as clarifying what the documents will attempt to incorporate is the articulation of what they will not undertake to do. In particular, the enterprise is decidedly not about "unilateral" or "immediate" disarmament, despite the (sometimes deliberate) mischaracter-

133. See Fissile Material Cut-Off Treaty (FMCT) at a Glance, supra note 85; James M. Acton, Fissile Materials and Disarmament: Long-term Goals, Short-term Steps, in GETTING TO ZERO, supra note 3, at 245-59; PIFER & O’HANLON, supra note 79, at 162-74; Robert J. Einhorn, Controlling Fissile Materials Worldwide: A Fissile Material Cutoff Treaty and Beyond, in REYKJAVIK REVISITED, supra note 5, at 279-311.

2014] 711
izations that too often proliferate. Instead, the following provides a list of eleven key characteristics that a valid nuclear weapons elimination process must possess; it comprises the metrics against which the feasibility and acceptability of a new treaty package would have to be judged and is reflected in the preambles of the draft documents in Parts IV and V.

1. *Global.* A zero agreement regime would ultimately have to be universal, covering (with varying degrees of intensity based upon the potential non-compliance risk they present) all countries and all physical environments in the world. Obviously, the states possessing nuclear weapons, as well as the states with advanced civil nuclear industries (and therefore the latent capacity to produce nuclear weapons relatively quickly), would have to be early participants. In addition, almost any country (as well as the high seas, outer space, and other locations outside the jurisdiction of any state) could potentially serve as a site for clandestine evasions of the treaty. Therefore, all would have to be subject, within some reasonable time period, to inclusion in the verification and enforcement regime. The various states need not participate immediately or in an equal or identical fashion, but proponents of abolition have repeatedly stressed that getting to zero will have to be a fully multilateral “joint enterprise.”

2. *Comprehensive.* The agreement would have to embrace all types of nuclear explosive devices, regardless of size, age, type, or status as deployed, non-deployed, retired, or otherwise, and regardless of the asserted purpose or function of the explosive. In addition, the critical components of nuclear weap-

---

134. Perkovich & Acton, *supra* note 8, at 16 (dismissing the “mistaken[] fear” that nuclear disarmament means “unilateral” disarmament).


136. Consideration of the purpose or function of a nuclear explosive device is relevant here in connection with the notion of “peaceful nuclear explosions” (PNEs). For many years, enthusiasts imagined that explosive nuclear power could be safely and inexpensively harnessed for civil engineering purposes, such as to excavate a canal or construct an underground storage chamber. For that reason, Article V of the NPT preserves for NNWS non-discriminatory access to PNE services. NPT, *supra* note 44, art. V. More recently, however, the ardor for PNEs has dampened, and the CTBT bans them as technologically indistinguishable from weapons tests. CTBT, *supra* note 129, art. I; Nina Tannenwald, *The Nuclear Taboo: The United States and the Non-Use of Nuclear Weapons Since 1945* 268-73 (2007).
ons, delivery systems, and supporting infrastructure assessed as having either a unique or a very strong identification with nuclear weapons design, engineering, production or maintenance would have to be brought inside the monitoring and control regime.

3. **Timely.** The process of climbing the mist-covered mountain will doubtless require many years; the world should start now, by re-affirming the goal, and by undertaking immediate steps in pursuit of it. It is impossible today to specify a reliable timetable for completion of the enterprise, and there may be pauses along the way, but taskmasters should hold the world community to a persistent effort.

4. **Balanced.** The sequence of steps in pursuit of nuclear disarmament should elicit appropriate contributions from each state. The cavalcade toward nuclear weapons elimination may include some temporary asymmetries, as different states undertake independent actions that have no exact corollary in other countries, but all should share the burdens and risks.

5. **Predictable.** The progression toward a world free of nuclear weapons should be fully transparent, so all participants can see where they stand vis-à-vis other states, and what steps are coming next, with no surprises.

6. **Secure.** Each stage in the progression toward nuclear abolition must itself be stable; the legitimate security interests of each participant must be safeguarded at all times, and no state should be unduly exposed or even temporarily jeopardized at any interim point.

7. **Verifiable.** The agreements would have to incorporate structures and functions that would enable parties to be confident that their neighbors were complying with the obligations. Insistence upon “perfect” verification would be unrealistic, but when dealing with such decisive weapons participants must know that militarily-significant cheating would be detected in sufficient time to enable an effective response. Although earlier arms control treaties have established many useful precedents for effective verification, significant advances in observation technology and in the sovereign acceptability of intrusive inspections will be required for a zero

---

137. See Pifer & O’Hanlon, supra note 79, at 176 (discussing the idea that there might be temporary pauses at “base camps” along the pathway up the mountain).
regime, with monitoring algorithms and political accommoda-
tions that we cannot now specify and can only barely imagine.

8. **Enforceable.** If a violation is detected, the international commu-
nity must be capable of mounting a timely, effective response. 
Again, the current impoverished array of legal tools—eco-
nomic sanctions, diplomatic retaliation, action through the 
U.N. Security Council, or self-help under the aegis of the 
Vienna Convention on the Law of Treaties\(^\text{138}\)—is inadequate. 
New international political and legal realities—including the 
possibility of the use of military force—will have to be devel-
oped both to deter and to respond to any “breakout” attempts.

9. **Sustainable.** The nuclear disarmament regime must be suffi-
ciently robust to be able to withstand the inevitable disrup-
tions that accompany international politics. The abolition of 
nuclear weapons cannot depend upon an idealistic vision of a 
conflict-free world, but must be capable of surviving all man-
ner of temporary (and even severe) perturbations.

10. **Irreversible.** One exceptional challenge is to make the zero 
regime permanent, perpetually guarding against the unwarr-
ranted resurrection of nuclear weapons. A special aspect of 
this problem, considered further \textit{infra}, is the possibility that 
one of the most effective national responses to one country’s 
cheating on the treaty obligations (e.g., Country X begins to 
re-create its nuclear weapons, or is found to have secretly 
retained some of its original stockpile) would be for other 
states to likewise re-constitute portions of their own earlier 
weapons (e.g., Country Y quickly returns to building its own 
offsetting nuclear force). Such a response—if done quickly, 
effectively and proportionally—might cancel any benefit that 
the cheater had hoped to attain, and thereby deter any such 
wayward moves in the first place. But that form of self-help 
retaliation is a challenge to the notion of a “permanent” 
eradication of nuclear weapons, and raises the discomfiting 
scenario of a dangerous “race to re-arm.”

11. **Legally-binding.** To be weighty and reliable, the ultimate Zero 
Treaty to abolish nuclear weapons must have the force of law, 
as article VI of the NPT already does. Non-legally-binding and

679 (\textit{entered into force} Jan. 27, 1980) [hereinafter VCLT].

714 [Vol. 45]
unilateral national steps, such as an initial Zero Agreement, can play a useful supporting role along the way.

B. Four Key Stumbling Points

With those predicates, therefore, the remainder of this section scrutinizes four key stumbling points that the nuclear disarmament process must find a way to overcome.

1. Definition of “Zero”

Everyone—especially lawyers—must recognize the importance of definitions in any viable legal instrument. For a complex arms control agreement, in particular, clarity about what is being regulated, in what way, is essential; definitions often perform a great deal of the substantive work of the document. Sometimes, these definitions are explicit: the Chemical Weapons Convention’s article II, for example, contains fourteen frequently-consulted definitions that establish the scope and content of the obligations, and the CWC’s Verification Annex adds a further twenty-six points to the lexicon.\(^{139}\) START I was even more painstaking; its Definitions Annex comprises no fewer than 124 terms.\(^{140}\)

In a Zero Agreement and Zero Treaty, the terms may not be separately designated in the same way, but a meeting of the minds is essential regarding precisely which items, activities, and facilities are to be outlawed, regulated, or excluded from the scope of the agreement.

In this connection, skeptics are fond of arguing that, as a practical matter, the elimination project is doomed to failure because “nuclear weapons cannot be un-invented.”\(^{141}\) They stress that even if all extant nuclear devices could somehow be identified, corralled and destroyed, the ability to construct replacements could not be eradicated, because

---


140. START I, supra note 110, Definitions Annex. New START, which was designed both to extend and simplify the original accord, contains definitions of ninety terms. New START, supra note 78, Protocol, Part I.

141. TAUBMAN, supra note 3, at 288 (quoting former National Security Advisor Brent Scowcroft saying “to me, the basic problem is that you cannot disinvent nuclear weapons”); see also Perkovich & Acton, supra note 8, at 11 (arguing that many technologies cannot be un-invented, but have nevertheless been effectively prohibited); Mack, supra note 102, at 208; NWC, supra note 2, at 140-41 (arguing that even if the knowledge about how to construct a nuclear weapon cannot be eradicated, the necessary infrastructure can be controlled).
the key ingredients could be quickly and quietly re-assembled and the know-how will persist in the human memory. Nuclear technology, after all, is old technology; the basics have long been de-classified and proliferated.\textsuperscript{142}

There is an important element of truth in those contentions, but, as discussed further below, the perpetual ability to re-create a nuclear weapons capability is not only a danger, it is also an important safeguard in a zero regime. The possibility that a country, imperiled by a rival’s “breakout” violation of the Zero Treaty, could undertake to establish or re-establish a small offsetting nuclear stockpile of its own constitutes a continuance of a “deterrence” regime—a dangerous and delicate relationship, to be sure, but not one fatal to the aspirations of abolitionists.

The phenomenon of “dual capability,” noted above, also complicates the treaty-makers’ task. Some weapons-related materials—the fissile uranium and plutonium, most prominently—are simply too precious to eliminate; they can be of immense value in generating electric power, in medicine, in agriculture, and in a host of other benign applications. The challenge is to preclude the future weapons functions while fostering the ubiquitous peaceful purposes; simple destruction or permanent warehousing would be unsuitable.\textsuperscript{143}

Those inescapable physical, technological, and economic facts therefore require that the Zero Treaty achieve clarity about what activities, equipment, and materials are either banned or included in the regime under strict, verifiable standards governing their avowed peaceful uses. In particular, how close to a nuclear weapons capability

\textsuperscript{142} John P. Holdren, Management of Surplus Nuclear Explosive Materials, in Canberra Commission on the Elimination of Nuclear Weapons, Background Papers, supra note 56, at 241, 242 (arguing that it is difficult to acquire nuclear explosive materials, but “the knowledge of how to use these materials to make (at least) crude nuclear weapons is very widely available, that is, available to virtually any country and to many subnational groups.”).

\textsuperscript{143} The primary weapons isotopes of uranium and plutonium have very long half-lives and will not decay on any human timescale. They can, however, be rendered relatively unusable for weapons, by down-blending (to dilute their explosive potential) or by mixing with contaminants. See id. at 247-50; Perkovich & Acton, supra note 8, at 51; Christopher E. Paine, Thomas B. Cochran, & Robert S. Norris, Practical Interim Steps Toward Nuclear Weapons Elimination and a Fissile Material Control Regime for Nuclear Weapon States, in Canberra Commission on the Elimination of Nuclear Weapons, Background Papers, supra note 56, at 99, 107 (noting that the United States has chosen a “spent fuel standard” as the criterion for disposition of excess plutonium, meaning that plutonium recovered from weapons should be rendered as difficult to retrieve as it is from spent civil reactor fuel); NWC, supra note 2, at 190-92 (discussing final disposition of fissile materials); Matthew Bunn, Transparent and Irreversible Dismantlement of Nuclear Weapons, in Reykjavik Revisited, supra note 3, at 205-27.
will states be allowed to hover, and for how long?\textsuperscript{144}

One approach to resolution of this conundrum lies in the consideration of the key "components" of a nuclear weapon, each of which may require its own regulatory regime.\textsuperscript{145} For this purpose, the primary constituents of a nuclear weapon include:

(a) fissile material, principally the highly-enriched uranium and plutonium, together with tritium or other "boosters" that enhance the chain reaction;

(b) specialized, conventional high explosives that initiate fissile core compression;

(c) the electronics package that symmetrically detonates the high explosive;

(d) the carbon fiber aeroshell (the missile re-entry vehicle) or aerodynamic gravity bomb casing/tail assembly that takes a warhead through the atmosphere to its target and contains the systems that arm and initiate the firing sequence; and

(e) the ballistic missile, bomber, cruise missile or other delivery system that transports the warhead or bomb from the launcher to or near its intended target.

In the proposed draft agreements, countries would be allowed to retain access to appropriate quantities of fissile material for civilian applications, under strict international monitoring; the anticipated Fissile Material Cutoff Treaty would likely establish some form of international ownership, operation, or regulation of the sensitive materials and other key components of the fuel cycle. The proposed Zero Treaty contemplates that even the fissile material recovered from

\textsuperscript{144} See Christopher E. Paine, Thomas B. Cochran, and Robert S. Norris, \textit{International Arrangements for the Transition to a Nuclear Weapon Free World}, in \textit{CANBERRA COMMISSION ON THE ELIMINATION OF NUCLEAR WEAPONS, BACKGROUND PAPERS, supra note 56, at 141} (evaluating eight possible "end states" for a nuclear disarmament process, in which participants would be subject to different types of ongoing limitations).

\textsuperscript{145} See \textit{END-STATE ISSUES, supra note 33, at 25-26} (describing the components of a nuclear weapon as including: "safety-certified advanced fusing and firing systems with permissive action links that must receive an authorized, pre-set code in order to initiate implosion of the metal primary pits; neutron generators; the high explosives that squeeze the nuclear-explosive material to critical densities to start the fission chain reaction; parts that control radiation flow; and gas-transfer boost systems with supplies of tritium gas that require regular replenishment"); Steve Fetter & Ivan Oelrich, \textit{Verifying a Prohibition on Nuclear Weapons}, in \textit{ELEMENTS OF A NUCLEAR DISARMAMENT TREATY, supra note 3, at 27, 42} (describing the key components of a nuclear weapon as including the fissile "pit" and non-nuclear elements such as "conventional explosives, arming, fusing, and firing systems, and structural elements."). Other relevant equipment includes radar fusing, batteries, and radar altimeters.
disassembled nuclear weapons would gradually be turned over to the appropriate international authority. But for some period of time, a country that was surrendering its NWS status would be allowed to retain a small secure stockpile of recovered weapons-grade fissile material, subject to tight international monitoring.

The retention of other critical chemical and electronic components—especially those that are most suitable only for nuclear weapons, without important alternative uses in the civilian economy—would be constrained even further. As these elements are extracted from nuclear weapons during the dismantling process, they would be reliably counted and impounded; most would be promptly destroyed under international inspection. The state would be allowed to retain only a limited inventory of such items for a limited period of time, under conditions that would preclude them from being quickly or secretly reunited into a weapon, but that would enable their reassembly in response to another state's violation.\footnote{146}

Likewise, the delivery systems would have to be strictly controlled. Many missiles, aircraft and other hardware are dual-capable—they can, with relatively modest refurbishment, be configured (or at least jury-rigged) to transport either nuclear or conventional weapons. As a practical matter, however, some weapons categories have been traditionally allocated exclusively to either a nuclear or a conventional mission. ICBMs and SLBMs, for example, are so expensive that they have been reserved essentially for nuclear missions.\footnote{147} Conversely, short-range systems now exclusively carry conventional ordnance; devices such as nuclear artillery, torpedoes, and land mines are mostly artifacts of the remote past, at least for the leading nuclear players.

The following draft Zero Treaty, therefore, proposes to abolish ICBMs and SLBMs at the same time as their nuclear payloads, but to allow retention of shorter-range ballistic and cruise missiles, as well as dual-capable aircraft, provided they are converted to conventional-only missions. It must be acknowledged that any such "conversion" is only imperfectly reliable—an advanced state could probably figure out a relatively expeditious way to re-adapt a conventional-armed bomber,

\footnote{146. It might be useful to differentiate between "disassembly" of a nuclear weapon (which could involve separation of the "nuclear explosives package" from the supporting non-nuclear components such as radars, altimeters, batteries, and fuzing and arming systems) and "dismantlement" of the nuclear explosive package (which would separate the fissile pit from the high explosive implosion mechanism).

147. See PIFER & O'HANLON, supra note 79, at 66-68 (discussing possible application of ICBMs for conventional prompt global strike missions).}
WHAT WOULD ZERO LOOK LIKE?

for example, to perform a reinvigorated nuclear mission in an emergency—but perhaps even this partial safeguard has some value.\(^{148}\)

In a similar fashion, the draft Zero Treaty posits the gradual elimination or conversion of key elements of the “nuclear weapons complex.” Facilities at which nuclear weapons have been designed and tested, for example, would need case-by-case regimens.\(^{149}\) The Nevada Test Site,\(^{150}\) for instance, and its counterparts in other countries, would be closed to nuclear weapons activities of any kind, and closely monitored; any equipment optimized for nuclear testing there would be destroyed and any existing tunnels or unused boreholes would be plugged or collapsed. Nuclear weapons laboratories, such as Sandia, Los Alamos, or Lawrence Livermore,\(^{151}\) pose a more subtle problem—they would certainly continue to perform other important (and highly classified) national security work, but would have to be subject to sufficient inspection to ensure that they were no longer in the business of designing, preparing, inspecting, or refining nuclear weapons. Facilities that have been used in the past to assemble nuclear weapons are likely to be the same sites employed for disassembly, so they will have to remain functional (and closely monitored) through the disarmament phase.\(^{152}\) Plants that process uranium, such as the Y-12 installation in

\(^{148}\) See CWC, supra note 139, art. V.12-13, Verification Annex, Part V, Sec. D (discussing conversion of chemical weapons production facilities to serve other purposes); New START, supra note 78, art. VI, Protocol Part 3 (conversion of strategic weapons and facilities).

\(^{149}\) Paine, Cochrane, & Norris, Arsenals, supra note 88, at 28 (listing major nuclear weapons infrastructure elements for NWS); Fissile Material Panel, supra note 83, at 24-25 (listing uranium enrichment and plutonium reprocessing plants around the world); James Leonard, Verification Arrangements, in CANBERRA COMMISSION ON THE ELIMINATION OF NUCLEAR WEAPONS, BACKGROUND PAPERS, supra note 56, at 156, 160 (noting that a party might temporarily “mothball” a facility (retaining an ability to restore it quickly to functionality), but eventually destruction or conversion would be required); NWC, supra note 2, at 142-46 (noting the conversion of nuclear infrastructure assets).

\(^{150}\) This site, larger than the state of Rhode Island, has been used for decades for nuclear tests and multiple other purposes; it is now known as the Nevada National Security Site. Nevada National Security Site, U.S. DEPT. OF ENERGY, http://www.nv.energy.gov/about/nts.aspx (last visited Apr. 17, 2013).


\(^{152}\) Leonard, supra note 149, at 158.
Oakridge, Tennessee, would also have to be dealt with on an individual basis.153

In this regard, therefore, even the eventual Zero Treaty would retain a vestige of the "discriminatory" nature of the NPT. The NWS (which could then be re-stylized as the "former NWS" or the "provisional NNWS," or less elegantly as the "countries that are in the process of eschewing their NWS status") would as a practical matter remain more capable of re-constituting their prior nuclear weapons capability than a typical NNWS would be of creating a nuclear weapon from scratch. Even when all nuclear weapons were eliminated, countries would, for a time, be asymmetrically positioned regarding their retention of residual stocks of weapons-related components and therefore in their lingering capability to craft a new nuclear weapon on short notice. Some would therefore refer to even this far-reaching proposal as establishing a "virtual zero," rather than an "absolute zero" regime.154 At some future point, perhaps, even these vestigial nuclear weapons-related components and infrastructure would be required to be eliminated, further leveling the playing field.

2. Verification and Enforcement

Verification and enforcement are actually two discrete questions, but they are related and both incessantly confound and energize the analysis of nuclear disarmament. "Verification," in this context, generically refers to the processes of detecting, monitoring, characterizing, and interpreting the behavior of another state, assessing that conduct against the requirements of an arms control accord, and reaching judgments about compliance or non-compliance. "Enforcement," the logically sequential step, is the process of responding to another party's exposed violation of an agreement, by compelling the other party to comply, punishing it for the violation, or offsetting any advantage it might have hoped to gain from its deviant practice. In each instance,

153. See Ralph Vartabedian, Estimate for Uranium Facility Goes from $600 Million to $11.6 Billion, L.A. TIMES (Sept. 24, 2013), http://articles.latimes.com/2013/sep/24/nation/la-na-bomb-factory-20130925 (cost of refurbishing the only U.S. facility that melts, casts, and machines bomb-grade uranium has soared to nineteen times the original estimate).

154. NWC, supra note 2, at 28 (citing Stansfield Turner); Marvin Miller, Verification Arrangements, in CANBERRA COMMISSION ON THE ELIMINATION OF NUCLEAR WEAPONS, BACKGROUND PAPERS, supra note 56, at 181, 186-87; David Holloway, Further Reductions in Nuclear Forces, in REYKJAVIK REVISTED, supra note 3, at 1, 23 (discussing "virtual deterrence," in the absence of any deployed nuclear weapons).
the objectives include deterrence of cheating by ensuring that any militarily significant violation will be reliably detected in sufficient time to enable the innocent states to effectuate a sufficient response—altering their own postures to deny any appreciable gain to the violator or effectively compelling remedial behavior by that delinquent.

Both verification and enforcement are essential ingredients in an effective arms control regime.\textsuperscript{155} Of course, the standard of accomplishment cannot reasonably be one of "perfection"—there will always be some chance that a determined, well-funded, and clever violator could temporarily escape detection of some trivial breach of an obligation or that an obdurate rogue could withstand outside pressure to conform. But the appropriate standard of "effective" or "adequate" oversight is whether participants could have sufficiently high confidence that any potential militarily-significant "breakout" attempt would be ferreted out in sufficient time to enable the other parties to mount appropriate, effective counter-moves.\textsuperscript{156}

Of course, as the stakes go up, the stresses on the verification and enforcement mechanisms also rise. That is, when a treaty regulates non-nuclear weapons that may be heinous, but inherently less decisive on the battlefield, perhaps less rigor in the supervisory functions is tolerable. Likewise, when a nuclear weapons limitation agreement aims to achieve only modest reductions, leaving each side with immense residual inventories, the "balance of power" may remain robust, unperturbed by any marginal cheating. But when an agreement pursues deeper cuts in nuclear arsenals—and, \textit{a fortiori}, when it seeks to eradicate nuclear weapons altogether—the margin for tolerating undetected or uncorrected breaches is reduced accordingly.

The Zero Treaty, therefore, will demand verification and enforcement mechanisms far beyond any measures that have been negotiated and implemented—or even seriously contemplated—today. The future system will require intrusions into installations and activities of sovereign states far surpassing the contemporary state of the art; today's Chemical Weapons Convention, New START Treaty, and CTBT only barely outline the types of data reporting, on-site inspection, dispute-resolution, and compliance mechanisms that must be conceived and

\begin{footnotesize}
\textsuperscript{155} Arms Control. Verification: The Technologies That Make It Possible (Kosta Tsipis et al. eds., 1986); Fetter & Oelrich, \textit{supra} note 145.

\textsuperscript{156} Articulation of this now-familiar standard of adequate verification is attributed to arms negotiator Paul Nitze, as the "Nitze criterion." See Fetter & Oelrich, \textit{supra} note 145, at 29.
\end{footnotesize}
The outlines of any such verification and enforcement routines are only barely imaginable in 2014. We can speculate about the possible configuration of treaty rights and responsibilities, but new monitoring modalities will have to be invented and new political relationships will have to evolve in order to make them operational and effective. A great deal of the time and energy between now and the adoption and implementation of a nuclear elimination accord will have to be devoted to the process of crafting these new anti-breakout devices, institutions and arrangements.\(^158\)

The draft Zero Agreement and Zero Treaty, therefore, only sketch these provisions in the broadest of strokes. Regarding verification, they identify certain generic categories of monitoring methodologies—the traditional “national technical means” of verification, as well as new

---


WHAT WOULD ZERO LOOK LIKE?

multilateral complements;\textsuperscript{150} submission of detailed relevant national data to a global information bank; routine on-site inspection; installation of “black box” sensors and seals; expanded concepts for “societal verification”;\textsuperscript{160} and challenge on-site inspection. Likewise, regarding enforcement, the proposed documents simply identify the relevant categories of mechanisms—diplomatic measures, invocation of legal institutions, economic sanctions, criminal prosecutions, and military operations—without detailing precisely what those procedures could eventually include. A great deal of creative and energetic analysis has been poured into the problems of verification and compliance, and more will be needed.\textsuperscript{161}

Regarding the mechanisms for enforcement of the commitments, two particular features of the future scheme deserve special consideration. First, the reference to “military measures” in the enforcement section conceals a major legal and political quandary. That is, under modern international law, a state (or a collection of states) is generally authorized to employ armed force across international boundaries only if it is acting in self-defense or pursuant to authori-

\textsuperscript{159} The term “national technical means of verification” refers to mechanisms such as photoreconnaissance satellites, long-distance seismometers, and sophisticated radars, which are operated by one country to gather data relevant to assessment of another state’s compliance with its obligations under an arms control treaty. These devices generally operate outside the territory of the targeted country, and do not require (very much) cooperation or support from within. “Multilateral technical means of verification” would be similar types of apparatus operated collectively by a consortium of countries. See generally \textsc{Amy F. Wolf, Cong. Research Serv., R41201, Monitoring and Verification in Arms Control} (Dec. 23, 2011); \textit{Arms Control Verification, Defense Threat Reduction Agency, http://www.dtra.mil/missions/ArmsControlVerification/ArmsControlVerificationHome.aspx} (last visited Nov. 13, 2013); \textit{Verification of Nuclear Arms Control and Disarmament Treaties, Nuclear Age Peace Foundation, http://www.nuclearfiles.org/menu/key-issues/nuclear-weapons/issues/arms-control-disarmament/verification/index.htm} (last visited Feb. 23, 2014); \textsc{Graham Jr., supra note 57}, at 37, 51-53, 58-59; New START, \textit{supra note 78}, art. X.

\textsuperscript{160} The concept of “societal verification” refers to mechanisms for enlisting private individuals, NGOs, and civil society in all countries in monitoring and “whistleblowing” capacities to provide greater transparency. The concept is not new, but the modern technology of social media will provide additional, currently unforeseeable opportunities for additional insights. See \textsc{Frank Blackaby, Societal Verification, in Canberra Commission on the Elimination of Nuclear Weapons, Background Papers, supra note 56}, at 264; \textsc{Leonard, supra note 150}, at 161; \textsc{Miller, supra note 155}, at 185-86; \textsc{NWC, supra note 2}, at 172-73; \textsc{Nima Gerami, Attracting a Crowd: What Societal Verification Means for Arms Control: The US Response, Bulletin of the Atomic Scientists, May 1, 2013}, at 14.

\textsuperscript{161} See \textsc{Perkovich & Acton, supra note 8}, at 47-49 (outlining one “standard model” concept for verifying the destruction of nuclear weapons under a treaty); \textit{id. at 83-97} (regarding options for enforcement); \textsc{Christopher E. Paine, Thomas B. Cochran, & Robert S. Norris, Techniques and
zation from the U.N. Security Council. That short statement of the law, of course, conceals a great deal of subtle and imprecise jurisprudence, but the critical point here is that even a neighbor’s significant violation of a major arms control treaty—including perhaps even a rival state’s breaching the Zero Treaty and starting to re-establish a prohibited nuclear weapons arsenal—might not justify an immediate, unilateral preemptive military strike designed to interrupt that re-armament. Unless the facts were clear, and the threatened state (or the collection of treaty parties generally) could reasonably interpret the mere act of violation to constitute an “imminent” threat, thereby justifying an act of “anticipatory self-defense,” or if it could win an endorsement from the Security Council, categorizing the nuclear breakout as a “threat to the peace,” it would ordinarily not be lawful for another state to vindicate its treaty rights via first-strike military means.

While it is possible that the permanent veto-wielding members of the Security Council would be united in a determined response to the threat of a new nuclear arms race, there can be no guaranty that all five would always interpret the situation identically. But if a military strike is not legal, and if other economic and diplomatic response mechanisms are insufficient to abort the danger posed by the rogue state’s violation of the Zero Treaty, what is to be done? Perhaps the United States or some other self-appointed enforcer of the treaty would undertake to violate international law by launching a military strike necessary to sustain international security and make the treaty system work—but it is not very satisfying to rest such an important treaty regime upon an implicit assumption of extra-legal responses. But what other mecha-

---

*Procedures for Verifying Nuclear Weapons Elimination, in Canberra Commission on the Elimination of Nuclear Weapons, Background Papers, supra note 56, at 167; Miller, supra note 154; Leonard, supra note 149; Fetter & Oelrich, supra note 145; Canberra Commission, supra note 12, at 74-98.

162. U.N. Charter, supra note 58, art. 42 (use of force pursuant to decision of the Security Council), art. 51 (actions in self-defense).

163. Compare, for example, with the ongoing debates in international law and policy regarding the propriety of military action, without a self-defense rationale or the authorization of the U.N. Security Council, under the rubric of “humanitarian intervention” or “responsibility to protect.” Some authorities argue that such extraordinary measures, intended to prevent or interrupt mass atrocities, would be “illegal but legitimate”; others find that categorization unsatisfying. See Jane Stromseth, Rethinking Humanitarian Intervention: The Case for Incremental Change, in Humanitarian Intervention: Ethical, Legal and Political Dilemmas 232 (J.L. Holzgreve & Robert O. Keohane eds., 2003); Independent International Commission on Kosovo, The Kosovo Report: Conflict, International Response, Lessons Learned 4 (2000); Kenneth Ander-
nisms could be crafted to put military muscle reliably and lawfully behind the agreement.\textsuperscript{164}

The second, related consideration builds upon the "self-help" remedy noted above. That is, because nuclear weapons cannot be "un-invented," some inherent residual capacity will always remain—especially the (former) NWS would have an important ability to resurrect their erstwhile nuclear weapons by re-assembling retained components. This implicit enforcement option could play an important stabilizing role, if the Zero Treaty's verification mechanisms were sufficiently muscular to sound a timely and authoritative alarm whenever a State X was beginning the process of violating the obligations by moving toward a renewed nuclear weapons capability. State Y could then be legally authorized to respond in like manner, temporarily suspending its own treaty commitments as a necessary and proportionate response to the prior violation, adroitly reestablishing its own offsetting nuclear force, and restoring a balance of power.\textsuperscript{165}

Of course, the integrity of that mechanism relies upon several disquieting uncertainties. Would State Y be able to re-build quickly enough to overcome State X's head start? Would State X know that the detection and response mechanisms were so stringent, or might it gamble that it could succeed with a covert violation for long enough to obtain a meaningful military edge? Might Y's information about X be somewhat ambiguous, or based upon classified sources that it was reluctant to disclose in public—and might it be strategically wise for Y to begin its offsetting re-armament crash course in secret, not alerting

\textsuperscript{164} Harald Müller, Enforcement of the Rules in a Nuclear Weapons-Free World, \textit{in Cultivating Confidence, supra note 3}, at 33-66; NWC, \textit{supra note 2}, at 109-10 (noting that both the United Nations Security Council and General Assembly could play roles in enforcement of a nuclear disarmament treaty; rejecting suggestions that the process could include turning over to the United Nations a small number of nuclear weapons to use in an enforcement action against a breakout attempt); Barry Blechman, \textit{Why We Need to Eliminate Nuclear Weapons—And How to Do It, in Elements of a Nuclear Disarmament Treaty, supra note 3}, at 17; Rebecca Bornstein, \textit{Enforcing a Nuclear Disarmament Treaty, in Elements of a Nuclear Disarmament Treaty, supra note 3}, at 149-66; Alexander Bollfrass, \textit{An International Reserve Force, in Elements of a Nuclear Disarmament Treaty, supra note 3}, at 167-78; \textit{Debate, supra note 3}, at 104-05, 118-20; Ernesto Zedillo, \textit{The Role of International Institutions in the Disarmament Process, in Debate, supra note 3}, at 287, 290.

\textsuperscript{165} See Taubman, \textit{supra note 3}, at 362-63 (noting that while, at first blush, the notion of any possible reconstitution of nuclear weapons "seems a double cross to pure abolitionists," it provides a necessary, realistic safeguard); Mack, \textit{supra note 102}, at 221. The possibility of reconstitution also implies that important elements of the current "deterrence" regime will continue to operate into
X about the detection and counter-measures? Would incipient little nuclear arms races of this sort proliferate under a Zero Treaty, and would they be even more dangerous and nerve-wracking than the current fully nuclear-armed structures? How would a self-help regime of this sort operate when there are not just two potential arms racers, but multiple states \( Z \), as well?

An important part of the solution to the riddle about the need for vast improvements in the verification and enforcement routines was suggested by Jonathan Schell, writing in *Foreign Affairs* in 2000.\(^{166}\) He submitted that the then-current paradigm of U.S.-Russia (or, today, P5 and broader) mutual suspicion and a relatively blasé attitude about proliferation would have to be replaced as outmoded. If the superpowers awoke to the realization that effective abolition of nuclear weapons was so profoundly in their respective national self-interests, and if they appreciated that air-tight verification and enforcement were indispensable to the safety and reliability of the regime, they would inevitably change their attitudes about intrusive inspections, rigorous implementation, and the whole concept of “openness.” They would abandon much of the paranoia about sovereign privacy and get much more serious about proliferation, effective verification and enforce-

---

the indefinite future, and it further carries the danger of incipient little “reconstitution races,” mimicking the arms races of the cold war. See End-State Issues, supra note 33, at 24; Perkovich & Acton, supra note 8, at 102-06; see also Jonathan Schell, The Fate of the Earth: The Abolition 181-231 (critiquing the concept of nuclear deterrence); Rebecca Bornstein, Enforcement Scenario: Iran, in Elements of a Nuclear Disarmament Treaty, supra note 3, at 156-57 (discussing possible suspension of treaty obligations in the event of another party’s breach); Pifer & O’Hanlon, supra note 79, at 191-97 (discussing reconstitution of weapons arsenals); Christopher A. Ford, Nuclear Weapons Reconstitution and its Discontents: Challenges of “Weaponless Deterrence,” in Deterrence: Its Past and Future 131-215 (George P. Shultz, Sidney D. Drell, & James E. Goodby eds., 2011).

Other “self-help” legal remedies may also be applicable. In response to a “material breach” of a treaty, an innocent party may generally suspend or terminate its counter-performance of treaty obligations. VCLT, supra note 138, art. 60. The doctrine of “countermeasures” may produce a similar result, enabling a state aggrieved by another state’s violation of a legal obligation, to respond by temporarily suspending its own performance in a timely, proportional fashion, intending to drive the first state back into compliance. See Art. 22 and commentary in Draft Articles on Responsibility of States for Internationally Wrongful Acts, [2001] 2 Y.B. Int'l L. Comm. 2 at 75, available at http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

---

166. Jonathan Schell, The Folly of Arms Control, 79 FOREIGN AFF. 22, Sept.-Oct. 2000; see also Perkovich & Acton, supra note 8, at 97 (arguing that if the leadership in just three countries—the United States, Russia and China—became fully committed to nuclear disarmament, then the concept could be made to work).
WHAT WOULD ZERO LOOK LIKE?

ment, insisting that all potential loopholes for cheating be conclusively foreclosed. They would simply not allow any other state—one of their erstwhile "clients," a neutral, or a rogue regime—to retain a nuclear weapons capacity that they were abandoning themselves.\textsuperscript{167} We cannot know today whether such epiphanies will actually occur among the P5, the other nuclear weapons possessing states, and the many other relevant players, but the progress toward the zero accords will have to foster such an evolution.

3. Timing and the Negotiating Process

In their first \textit{Wall Street Journal} piece, the Gang of Four skillfully articulated the necessary linkage between two essential components of the progression toward zero, calling for commitment to both the big-picture "vision" of a nuclear weapons-free world and the small-picture immediate "steps" necessary to pursue it. They wrote, "Without the bold vision, the actions will not be perceived as fair or urgent. Without the actions, the vision will not be perceived as realistic or possible."\textsuperscript{168}

One immediate implementation question concerns the appropriate forum within which the Zero negotiations on both "vision" and "steps" would optimally occur. There are many possibilities here, none of which commands automatic assent.\textsuperscript{169} The Conference on Disarmament (CD) is the UN-affiliated body that has been the primary venue for elaborating numerous prior arms control accords, including the NPT, CWC and CTBT.\textsuperscript{170} Alas, the CD has fallen into desuetude,
blocked by political discord and unable—for more than fifteen years—to engage in productive treaty-developing labor. A series of freestanding, ad hoc negotiating conferences could be convened instead—such processes generated the 1997 Ottawa agreement on anti-personnel land mines and the 2008 Oslo agreement on cluster munitions. Perhaps the NPT could supply the umbrella beneath which the negotiators convene, led by the P5 or by a sympathetic and symbolic leader such as Japan. The United Nations (the General Assembly or any of several subsidiary bodies) could also function as host, as it recently did for the 2013 Arms Trade Treaty. Finally, perhaps the Nuclear Security Summit process could be converted from its sole focus on retrieving and improving the security of nuclear weapons-useable materials to consider a broader disarmament agenda.

The draft Zero Agreement and Zero Treaty are agnostic regarding these procedural questions, not specifying any particular vehicle for conducting the negotiations. Likewise, the number and identities of the states directly participating in the negotiations remains an important variable “to be determined.”

A second frequently-asked question is “How long will all this take?” In 2006, 125 countries voted in favor of a U.N. General Assembly resolution calling for immediate commencement of nuclear disarmament negotiations, and the Zero Agreement presented here follows that...
WHAT WOULD ZERO LOOK LIKE?

Animating spirit. Beyond that prompt starting point, however, the viability and utility of crafting a specific timetable for getting to zero are debatable. In the 1950s and 1960s, activists boisterously championed the concept of a "time-bound" progression toward general disarmament, insisting that states should, in one swoop, specify the whole series of intermediate agreements (including restrictions on chemical, biological, and conventional forces, as well as nuclear) and specify a "due date" for each. More recently, Rajiv Gandhi's 1988 proposal for nuclear disarmament likewise sought to convert the aspiration into concrete terms, by establishing a deadline of 2010. The Global Zero Action plan does likewise, and the 2007 Model Nuclear Weapons Convention includes options for specific scheduling.

As these proposed schedules for arms control agreements were continuously frustrated, others became wary about the virtue of publishing specific (or even quite general) timetables. President Obama's open-ended articulation represents just about the full extent that many observers are willing to go, saying only, "This goal will not be reached quickly—perhaps not in my lifetime." In that spirit, the proposed Zero Agreement and Zero Treaty do not include projected timetables.


178. GANDHI'S ACTION PLAN, supra note 11, Annex I, at 186, (identifying three stages for the progression toward nuclear elimination, with complete nuclear disarmament being reached in 2010); see also ibid. at 133-40 (identifying several other contemporary disarmament proposals, many of which specify projected dates for getting to zero).


180. NWC, supra note 2, at 68-84 (citing articles VII-XII, presenting "phases" of progress toward zero, without specifying target dates); see also Barry Blechman, Why We Need to Eliminate Nuclear Weapons—And How to Do It, in ELEMENTS OF A NUCLEAR DISARMAMENT TREATY, supra note 3, at 17; Rebecca Bornstein, Enforcing a Nuclear Disarmament Treaty, in ELEMENTS OF A NUCLEAR DISARMAMENT TREATY, supra note 3, at 23 (presenting a timeline for the progression to nuclear disarmament); Cathleen Fisher, The Phased Elimination of Nuclear Weapons, in NUCLEAR WEAPONS: THE ROAD TO ZERO 39, 49-51 (Joseph Rotblat ed., 1998) (discussing the debate about whether it is useful to establish a deadline date).

The notion is that the process could commence soon, with the aspirational Zero Agreement signed in, say, 2015, and the participants would thereafter press forward with all deliberate speed, reflecting both the urgency of their mission and the criticality of getting the job done right.

Those draft documents do, however, preserve a related point, in carving out a space for the articulation of a new diplomatic infrastructure necessary to goad the world community toward zero. Two new creatures would emerge. First, under the Zero Agreement, a Contact Group would be established. This informal collection of leading countries would steer the rest of the participating states forward, publicizing the ongoing efforts, urging the reluctant to participate, and convening biennial “review conferences” at the head-of-government level that would assess progress and problems. The Contact Group would be small (e.g., fifteen states), led by the P5, and include a representative sampling of diverse, interested and politically effective countries.182

Second, the Zero Treaty would elicit a new, formal multilateral institution, captioned here as the Zero Treaty Organization (ZTO). Like its counterparts established under the Chemical Weapons Convention183 and the Comprehensive Test Ban Treaty,184 this body would be charged with operating the treaty, conducting the inspections and other verification and enforcement operations under it, and resolving issues about compliance. The ZTO could be established by the Zero Treaty, or even before it, to help pave the way for its negotiation and entry into force. A now-common variation is for the negotiators to conclude both the permanent treaty and an associated interim agreement on immediate “provisional application” of key provisions, includ-


183. CWC, supra note 139, art. VIII.

184. CTBT, supra note 129, art. II.
WHAT WOULD ZERO LOOK LIKE?

ing the establishment of a “preparatory commission,” complete with a “provisional secretariat” to facilitate final preparations for entry into force and full operation of the main treaty.185

The ZTO would consist of three organs: an Assembly (responsible for overall policy direction, in which each party to the treaty is a member); an Executive Council (a smaller group—perhaps thirty to forty members—responsible for day-to-day decisions); and a Secretariat (the professional staff). The proposed Zero Treaty largely follows the CWC and CTBT models in this area, suggesting institutional and operational arrangements that are certainly important for the regime, and not very different from those precedents. For the sake of brevity, the full panoply of standard institutional arrangements is not specified in the draft.186

4. Collateral Measures

Finally, there is an array of associated issues that the makers of the draft Zero Agreement and Zero Treaty will have to ponder. Even if ultimately these points are largely invisible in the final texts, they may be the subject of important “side agreements” or intermediate accords that help make the progression toward nuclear elimination seem safer and more feasible.

For example, in many intensely contested regions of the world, incentives for the possession or pursuit of nuclear weapons cannot be divorced from contentious neighbors’ adversarial security postures on a host of longstanding political issues and irritants. It is almost impossible to imagine nuclear abolition in South Asia, the Middle East or Northeast Asia, for example, without some significant amelioration of existing regional tensions. The hope is that the affected states may be able to contextualize today’s embedded problems and recognize that join-


ing the long-term aspirations of the Zero Agreement can facilitate, not conflict with, efforts at regional stability.

Conclusion of a Zero Treaty does not require the lion to lie down with the lamb—severe international problems and military competition are likely to survive forever. Nor does it require the deus ex machina of an all-powerful world government. But getting to zero does require the participants to achieve the important insight that possession of nuclear weapons impedes, rather than assists, reconciliation of their legitimate security interests. Progress toward nuclear abolition, therefore, need not assume that the current array of regional troublespots can all be quickly resolved, but it does require that they at least abate, in the sense that the participants are willing to proceed in their competition without the presence of nuclear weapons—still a tall order. The Zero Agreement will incorporate the participating states’ commitment to address these various regional predicaments, and outside states’ willingness to promote non-nuclear rapprochement.

In the same vein, countries cannot reasonably contemplate abolition of their nuclear weapons without pondering the roles, missions, and capabilities of their non-nuclear forces. For the United States—surrounded by friendly neighbors and ocean buffers, possessing unmatched weapons technology and logistics capabilities, and boasting superb fighting units—the prospect of a world that could resort “only” to conventional warfare would be most welcome. But for other star-crossed countries an imbalance in non-nuclear capabilities may create unwelcome exposure, and international peace and stability cannot long tolerate important security vulnerabilities or asymmetries. Creating the conditions for the elimination of nuclear weapons will therefore require addressing constraints upon general purpose conventional forces as well, even if we cannot today outline what the simultaneous solution may look like or how (if at all) it would be reflected in treaty text.

189. See Perkovich & Acton, supra note 8, at 16 (arguing that the prohibition of nuclear weapons will not “make the world safe for conventional war among major powers.”); Dennis M. Gormley, American Conventional Superiority: The Balancing Act, in Getting to Zero, supra note 3, at 317-43.
WHAT WOULD ZERO LOOK LIKE?

Defenses against nuclear attack—including anti-missile and anti-aircraft systems, as well as civil defense programs—pose a similar puzzle. On one hand, effective defenses could conceivably stabilize nuclear abolition, by raising the threshold for a militarily-successful breakout and helping to ensure that even a successful treaty violator would still face formidable obstacles in making effective use of its illegal, unilateral nuclear capability. Especially if the potential aggressor’s arsenal were small (surely much smaller than the ICBM, SLBM, and bomber fleets maintained by the United States and Russia today) even a modest interception capability could blunt a threatened attack, frustrating the violator’s malign purpose. On the other hand, an efficacious defense before abolition has been accomplished could also provide a shield for aggression, enabling a bad actor to strike a vicious first blow, confident that it could largely protect itself from any disorganized, hasty retaliation.

The question of missile defense is particularly fraught today, as some in the United States pursue anti-missile technology with a fetishist’s zeal, and as the Russian leadership claims, perhaps unreasonably, to find the capabilities inherent in the emerging U.S. programs threatening to it. When both sides dig in their heels so rigidly, the immediate prospects for arms control are dim; even more ambitious undertakings, such as nuclear abolition, will have to deal with (or dodge) this question sooner or later.190

Finally, this succession of treaties may have to address the topic of “sweeteners” in a serious way. The scope of a modern arms control agreement often extends somewhat beyond the specific question of reductions or limitations on weaponry, and this political reality may well apply to several of the steps on the path to nuclear elimination, too. One of the three main pillars of the NPT, for example, concerns each party’s “inalienable right” to pursue nuclear energy for peaceful

190. See Ria Novosti, Russia Skeptical Over Obama’s New Nuclear Reduction Proposal, supra note 116 (Russian officials rebuff U.S. proposal to pursue further bilateral cuts in strategic weapons, while United States is developing a missile defense system); Ria Novosti, Nuclear Arms Reduction Deals to Become Multilateral—Lavrov, ATOMINFO.RU (June 22, 2013), http://www. rianovosti.com/world/20130622/181811968.html (same); PIFER & O’HANLON, supra note 79, at 113-38 (discussing missile defense issues); Christopher A. Ford, Nuclear Weapons Reconstitution and its Discontents: Challenges of “Wapless Deterrence”, in DETERRENCE: ITS PAST AND FUTURE 131, 157-60 (George P. Shultz, Sidney D. Drell & James E. Goodby eds., 2011); John Pike, Ballistic Missile Defense: Enduring Questions, in NUCLEAR WEAPONS: THE ROAD TO ZERO, supra note 14, at 191-212.

2014] 733
purposes, and many NNWS parties vigorously complain that the advanced civil nuclear technology holders have failed to fulfill their end of the bargain about facilitating “the fullest possible exchange of equipment, materials and scientific and technological information”¹⁹¹ for those ends. The Chemical Weapons Convention similarly contains obligations relating to “the fullest possible exchange of chemicals, equipment and scientific and technical information”¹⁹² relating to peaceful applications of chemistry and to the removal of undue restrictions on international trade in chemicals—and, once again, many economically disadvantaged states resent the crabbed implementation of those provisions.

The draft Zero Agreement and Zero Treaty accordingly contemplate that sweeteners of some sort may be necessary to help induce countries to join in the effort to eliminate nuclear weapons. In principle, no state should need to ask, “What’s in it for me?” regarding nuclear abolition—the improved safety and security for the entire planet should be sufficient incentive for all to participate. But some states—who have never possessed or pursued nuclear weapons, but who might nonetheless be required to submit to intrusive and expensive verification procedures—may need more persuasion about the value of joining the instruments. Accordingly, some textual acknowledgement, similar to that of the NPT, about sharing the peaceful benefits of nuclear energy, could be appropriate.

IV. DRAFT ZERO AGREEMENT

This section offers a draft text, with annotations, presenting one picture of what the next or initial step on the road to nuclear disarmament might look like: a non-legally-binding instrument through which the participating states confirm (or, for most of them, re-confirm) their commitment to the ultimate objective and their determination to take immediate steps in pursuit of it. This “framework” document, reifying the concept of getting to zero, could be negotiated and signed relatively soon, perhaps in 2015, in conjunction with the next Review Conference for the NPT.

¹⁹¹. NPT, supra note 44, art. IV. Article V of the NPT likewise promised that the anticipated benefits of “nuclear explosions for peaceful purposes” would be made available to NNWS on a non-discriminatory basis and at a low fee. Feiveson, supra note 102, at 57-76.
¹⁹². CWC, supra note 139, art. XI.
WHAT WOULD ZERO LOOK LIKE?

Zero Agreement\textsuperscript{193}

For the Elimination\textsuperscript{194} of Nuclear Weapons

The Participating States,\textsuperscript{195} (PP1\textsuperscript{196}) \textit{Determined} for the sake of all mankind to create the conditions for a world without nuclear weapons;\textsuperscript{197}

(PP2) \textit{Desiring} to take prompt, effective steps in a joint enterprise in pursuit of that goal;\textsuperscript{198}

193. Some arms control agreements have adopted "neutral" or descriptive titles, which serve well to advertise the contents of the instrument, but forego any effort at retaining a "popular name" or catchy title. For example, the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction is routinely referred to as the "Chemical Weapons Convention," CWC, supra note 139. In contrast, the "Comprehensive Nuclear Test Ban Treaty" avoids a mouthful of words, and adopts the language that has long been associated with CTBT, supra note 128. Alternatively, some treaties are informally named after the city in which they are concluded or signed, such as the Ottawa Convention on land mines, supra note 172. This draft follows the approach of designating a simple, evocative, colloquial title.

194. Again, there is a rhetorical choice here, among words such as "elimination," "prohibition," and "abolition." Some advocates favor the term "abolition," while others avoid the seemingly religious or messianic zeal that might connote. See Holdren, supra note 4; CWC, supra note 139 (using "prohibition"); Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, Apr. 10, 1972, 1015 U.N.T.S. 163, 11 I.L.M. 309 (1972) (entered into force Mar. 26, 1975) (hereinafter BWC) (using "prohibition"). Some might perceive a nuance of content difference, with "prohibition" describing a "legal" action and "elimination" referring to the physical act of destroying the devices; cf. Catherine McArdle Kelleher, \textit{Introduction}, in \textit{GETTING TO ZERO}, supra note 3, at 1, 5 (likening the campaign for nuclear disarmament to the earlier global efforts to eradicate smallpox or slavery).

195. The term "Participating State" is used instead of a term such as "party," reflecting the fact that this document is not legally binding. \textit{See} Guidance on Non-Binding Documents, U.S. DEPT. OF STATE, http://www.state.gov/s/l/treaty/guidance/ (last visited Feb. 23, 2014).

In this iteration of the text, the specific Participating States are not identified by name; the document is drafted as being open for signature by all states. An alternative is to identify (by name or by defining characteristics) a collection of perhaps twenty to forty key states that would be invited to join this Zero Agreement.

196. The preambular paragraphs are provisionally numbered in this draft and in the Zero Treaty, for convenience. In the final version of the documents, numbers would be deleted from the preambles, but retained in the operative paragraphs.

197. Conceptually, this Zero Agreement would be designed to help "create the conditions for" a world free of nuclear weapons; the following Zero Treaty would help effectuate the transition from a world with few nuclear weapons to a world with none.

198. This document contemplates two types of follow-on actions by individual states or groups of states. First, it outlines an anticipated series of interim, legally-binding agreements that would incrementally but definitively reduce nuclear weapons stockpiles around the world and contribute to nuclear disarmament in other ways. Second, it includes an Annex, in which
Anticipating that a systematic series of agreements will be developed, and cooperative reciprocal unilateral actions will be undertaken by many states, in the coming years to approach that goal in a manner that is global, comprehensive, timely, balanced, predictable, secure, verifiable, enforceable, sustainable, irreversible, and legally-binding;200

Fearing that the catastrophic power of nuclear weapons cannot be contained in either space or time, and has the potential to destroy all civilization, to devastate the entire ecosystem of the planet, and to jeopardize the survival of the human race;201

Believing that as long as nuclear weapons exist, the possibility of their proliferation and use cannot be forever precluded, and thus they will continue to pose the most extreme threat to all humanity;202

individual states would offer non-legally-binding unilateral measures (colloquially referred to as "house gifts") that they were prepared to take immediately, to jump start the process. The concept of a "joint enterprise" stresses that many (or all) states will have to play roles in pursuit of nuclear disarmament; the task can be led by, but is not the exclusive responsibility of, the United States, Russia, and the other NWS.

The anticipated unilateral actions undertaken individually by concerned states (such as the proposals suggested in the Annex) would be "cooperative" and "reciprocal," in the sense that each participant would take notice of the offerings of the others, and each would be encouraged to match (or even to leapfrog) the steps of the most progressive. But since individual countries are positioned asymmetrically with respect to current civil and military nuclear programs, the steps would not be identical and could not be exactly uniform. The steps would be "unilateral," in the sense of not being legally binding, and not necessarily being the product of sustained negotiation or dialogue.

This list of defining (and somewhat overlapping) adjectives is the "mantra" of conditions that a durable zero undertaking would have to meet; the ultimate objective is a regime that is: global (or universal) (applicable to all countries and all places on, under, and above Earth); comprehensive (covering all types of nuclear explosive devices and components, regardless of type or status); timely (not indefinitely delayed—although this document does not attempt to identify a specific timetable); balanced (calling for appropriate, corresponding actions from each state); predictable (allowing all states to see where the process is leading at each stage); secure (not jeopardizing any state or group of states at any point in the process); verifiable (to prevent secret cheating); enforceable (to respond effectively to violations); sustainable (not subject to fatal disruptions from temporary perturbations); irreversible (or permanent) (to ensure against the return of nuclear weapons); and legally-binding (to bring the full weight of international law in support of the institution). See supra text accompanying notes 134-38.

This rhetoric is adapted from the ICJ Advisory Opinion on Nuclear Weapons, supra note 59, ¶ 35.

In addition to the possibility of deliberate use of a nuclear weapon, the specter of accidental or mistaken use cannot be ruled out. See Jonathan Granoff, The Process of Zero, 26 WORLD POLICY J. 85, 86-88 (2009), available at http://gsinstitute.s3.amazonaws.com/assets/gsi/docs/WPJ_2009.pdf (recounting examples of accidents and false alarms regarding nuclear weapons).
WHAT WOULD ZERO LOOK LIKE?

(PP6) **Affirming** that all human life is sacred, and that all members of the human family have the equal, inalienable right to life, liberty, peace, security and dignity;203

(PP7) **Underscoring** the legal obligation contained in Article VI of the 1968 Treaty on the Non-Proliferation of Nuclear Weapons “to pursue negotiations in good faith on effective measures relating to cessation of the nuclear arms race at an early date and to nuclear disarmament, and on a Treaty on general and complete disarmament under strict and effective international control”;204

(PP8) **Reaffirming** the statement of “Principles and Objectives for Nuclear Non-Proliferation and Disarmament,” adopted at the 1995 Conference on the Review and Extension of the Non-Proliferation Treaty;205

(PP9) **Commending** the recognition, in the Final Document of the 2000 Review Conference of the Non-Proliferation Treaty, of “an unequivocal undertaking” by the states possessing nuclear weapons to accomplish the total elimination of their nuclear arsenals, through implementation of a series of “practical steps” and of the applicability of the principle of irreversibility in nuclear disarmament;206.

---


204. This Article VI obligation applies to all parties to the NPT—NWS and NNWS alike—but does not apply to non-parties to the NPT (India, Israel, North Korea, and Pakistan). Note that Article VI goes even beyond nuclear disarmament, by including a commitment to pursue “general and complete disarmament.” Some states may object to repetition of this far-distant goal, even in a preamble, while others may insist that this objective not be overlooked, although this instrument deals only with nuclear weapons. See David S. Jonas, *General and Complete Disarmament: Not Just for Nuclear Weapons States Anymore*, 43 GEO. J. INT’L. LAW 587 (2012).


It is possible that the four non-NPT states may object to so many preambular paragraphs referencing and drawing upon the work product of NPT meetings.

206. The Final Document from an NPT Review Conference is not, in itself, legally binding, but it represents a commitment by the NWS to take actions that are necessary to sustain the NPT and the non-proliferation enterprise. This passage is quoted from the Arms Control Association, *2000 NPT Review Conference Final Document, ARMS CONTROL ASSOCIATION* (Apr. 24-May 19, 2000), available at http://www.armscontrol.org/act/2000_06/docjum (discussing Article VI and Preamble, ¶¶ 8-12, 15, regarding "practical steps" in implementation of Article VI, steps #5 and #6).
(PP10) Noting that the Final Document of the 2010 Review Conference of the Non-Proliferation Treaty affirmed that “all States need to make special efforts to establish the necessary framework to achieve and maintain a world without nuclear weapons” and called, inter alia, for discussion of “policies that could prevent the use of nuclear weapons and eventually lead to their elimination.”

(PP11) Recalling Resolution 1(I) of the United Nations General Assembly, adopted unanimously on January 24, 1946, calling for proposals “for the elimination from national armaments of atomic weapons,” and the many subsequent resolutions of the General Assembly also calling for the elimination of nuclear weapons;

(PP12) Recalling also the Final Document of the United Nations General Assembly's First Special Session on Disarmament in 1978, which recognized the imperative of removing the threat of nuclear weapons and halting and reversing the nuclear arms race until the total elimination of nuclear weapons and their delivery systems has been achieved;

(PP13) Emphasizing the determination of the United Nations Security Council, as expressed in its Resolution 1887 of September 24, 2009, “to seek a safer world for all and to create the conditions for a world without nuclear weapons, in accordance with the goals of the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), in a way that promotes international stability, and based on the principle of undiminished security for all”;

(PP14) Recalling the Advisory Opinion of the International Court of Justice of July 8, 1996, in which it affirmed that the threat or use of nuclear weapons would generally be contrary to the rules of interna-


208. Establishment of a Commission to Deal with the Problems Raised by the Discovery of Atomic Energy, supra note 5. There are a great many General Assembly resolutions calling for abolition of nuclear weapons; this citation to the very first such resolution has particular salience, but others could be cited, too.


WHAT WOULD ZERO LOOK LIKE?

tional law applicable in armed conflict, and in particular the principles and rules of humanitarian law;\(^{211}\)

(PP15) Concluding that the financial,\(^{212}\) social, environmental, medical,\(^{213}\) intellectual, and psychological burdens of developing and maintaining nuclear weapons are an intolerable waste of human and material resources;

(PP16) Judging that urgent progress toward nuclear disarmament can facilitate resolution of regional security issues, and conversely that amelioration of those regional tensions can also assist in advancing the progress toward global elimination of nuclear weapons;\(^{214}\)

(PP17) Appreciating the value of nuclear energy for diverse peaceful purposes in electrical power generation, medicine, and other fields, when conducted under appropriate and effective international safeguards;\(^{215}\)

(PP18) Assessing that the creation and operation of additional international diplomatic mechanisms can effectively contribute to the advancement of the pursuit of nuclear disarmament;\(^{216}\) and

(PP19) Applauding the contributions to global peace and stability

---

211. I.C.J. Advisory Opinion on Nuclear Weapons, \textit{supra} note 59, ¶ 105(2)E.


213. \textit{See} supra note 2, at 120-25 (surveying the adverse health and environmental consequences of producing and testing nuclear weapons); John Loretz, International Physicians for the Prevention of Nuclear War, Zero is the Only Option: Four Medical and Environmental Cases for Eradicating Nuclear Weapons (2010), \textit{available at} http://nuclear-zero.org/.

214. \textit{See} supra text accompanying notes 187-88 (regarding the role of regional security issues in getting to zero).

215. This paragraph acknowledges the "dual use" nature of much nuclear material, equipment, facilities, and technology; the task of preserving and enhancing the peaceful applications while eradicating the weapons functions is among the biggest challenges for the regime. \textit{See} supra text accompanying notes 82-86 & 143-54. In contrast, the NWC discourages the use of nuclear power for energy production. NWC, \textit{supra} note 2, at 132-33.

216. \textit{See} supra text accompanying notes 182-86 (regarding the creation of a modest new diplomatic infrastructure to promote progress toward nuclear disarmament).
accomplished by numerous treaties in force or pending that deal with nuclear weapons, nuclear weapon free zones, chemical weapons, biological weapons, and other instruments;\footnote{217}

Have agreed as follows:

1. The Participating States confirm that a world without nuclear weapons is desirable and attainable,\footnote{218} and that they are under a moral and legal obligation\footnote{219} to pursue it promptly and vigorously. Participating states will\footnote{220} do everything in their power to cooperate in creating the conditions necessary for the global, comprehensive, timely, balanced, predictable, secure, verifiable, enforceable, sustainable, irreversible, and legally-binding elimination of all nuclear weapons.\footnote{221}

2. All Participating States that have not yet done so should in the near future join the 1972 Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction; the 1993 Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction; and the 1996 Comprehensive Nuclear Test Ban Treaty. All Participating States will promote universal adherence and observance of these instruments.\footnote{222}
WHAT WOULD ZERO LOOK LIKE?

3. The Participating States will support the development, adherence and observance of regional nuclear weapon free zone treaties and their associated protocols and will urge eligible states to participate fully in those regimes.229

4. Each Participating State that possesses nuclear weapons will immediately224 cap225 the total number of its nuclear weapons and undertake additional measures of transparency regarding its nuclear weapons programs.226

5. The Russian Federation and the United States of America will promptly and urgently enter into negotiations and conclude an agreement for the further reduction of their nuclear weapons, with the goal of reducing their current total inventories by approximately fifty percent.227

“ratify,” since the BWC and CWC are no longer open for signature, and any newcomers would join those treaties by accession, rather than ratification. BWC, supra note 193, art. IX.1; CWC, supra note 140, art. XVIII.; CTBT supra note 129, art. XII. The BWC and CWC have attracted wide, but not universal, adherence; the CTBT has not yet entered into force, lacking ratification by the United States, China, and other essential participants.

The Zero Agreement could also endorse the NPT and urge the remaining non-parties to join that treaty, too—but doing so might be politically offensive to India, Israel, North Korea, and Pakistan, who might be inclined against this Zero Agreement, if affiliating with it required them to abandon their longstanding antipathy to the NPT.

223. This paragraph echoes preambular paragraph 19, in supporting the creation and implementation of new and existing regional nuclear weapon free zone arrangements, which are of special interest to nuclear disarmament. See supra text accompanying notes 117-123.

224. Alternatives would be to institute this provision at a (soon) fixed time, at a point when specified other reductions had already occurred, or “as soon as possible.” In particular, the sequencing of events specified in paragraphs 4 and 5 may be problematic—will other states institute caps on their nuclear weapons before, or only after, the United States and Russia have undertaken the next step in their bilateral reductions?

225. This provision is sometimes referred to as a “freeze” on national weapons stockpiles, but the better concept is to impose a “cap” or ceiling on those inventories, which would allow a state to reduce its weapons. This paragraph would also allow a state, for now, to continue to produce new nuclear weapons (for example, to replace defective or obsolete devices) as long as there was at least a one-for-one offsetting elimination of existing devices. Routine maintenance of nuclear weapons would also be permitted for as long as the devices exist.

226. The (unspecified) transparency measures would be designed to enhance other states’ abilities to determine with high confidence the numbers and characteristics of each participating state’s existing nuclear weapons inventories, as a precursor to later verified reductions.

227. This paragraph elicits a successor to the 2010 New START, supra note 78, which imposes a series of limitations upon various categories of U.S. and Russian nuclear weapons, to be effectuated by 2018. The proposal here calls upon those two countries to move forward aggressively with additional limitations now, rather than waiting until 2018 approaches. The target of a fifty percent reduction in weapons is intentionally somewhat vague, in leaving for those two states the potentially difficult and controversial questions of “counting rules” and other provisions...
6. Thereafter, the People’s Republic of China, the French Republic, the Russian Federation, the United Kingdom of Great Britain and Northern Ireland, and the United States of America will enter into five-party negotiations with the goal of achieving deep reductions in their respective nuclear weapons stockpiles in a balanced and progressive fashion. They may implement these agreed reductions in stages. They will seek to achieve as soon as possible the lowest possible levels of nuclear weapons, retaining no more than 100 weapons each.

7. Simultaneously, those five states will enter into negotiations with the Republic of India, the State of Israel, the Democratic People’s Republic of Korea, and the Islamic Republic of Pakistan, to incorporate both deployed and non-deployed weapons, as well as dealing with both strategic and short-range systems. See supra text accompanying notes 104-116; see also David Holloway, in REYKJAVIK REVISITED, supra note 3, at 1-31 (arguing that the process of moving toward nuclear disarmament must begin with Russia and the United States); Pan Zhenqiang, Abolishing Nuclear Weapons: Why Not Outlaw Them First?, in DEBATE, supra note 3, at 249, 253 (asserting that as “[f]irst among unequals, the United States and Russia must lead.”).

Although China, France and the United Kingdom currently possess many fewer nuclear weapons than do the United States and Russia, before long, the current bilateral (U.S.-Russia) structure of nuclear arms control will have to transform into a plurilateral negotiation, incorporating all the P5). See Ria Novosti, Russia Skeptical Over Obama’s New Nuclear Reduction Proposal, supra note 116 (Russian officials insist that other NWS will have to participate in the next round of nuclear weapons reductions); RIA Novosti (Jun. 22, 2013), supra note 189 (same); PIFER & O’HANLON, supra note 79, at 178-81 (multilateralizing arms control).

It is possible that an initial round of negotiations would not provide for equal numbers of nuclear weapons for all five states, but before long, asymmetries would have to be ironed out.

Alternatively, these “stages” could be overtly identified and the numbers and dates could be spelled out in the text, but that would seem to import a level of specificity beyond our current abilities to foresee the acceptable arrangements and timing. Cf. Paine, Cochran, and Norris, International Arrangements, supra note 143, at 149-52 (outlining three stages and fifteen steps toward nuclear elimination); Leonard, supra note 143 (describing four phases).


This paragraph focuses on the four states that are not party to the NPT and that therefore retain a legal right to possess nuclear weapons. (But see the special legal obligations applicable to North Korea, supra notes 55 & 56.) The paragraph does not deal with Iran or any other state that might be thought to be illicitly pursuing a nuclear weapon or the capability to build one; those states are all currently NNWS parties to the NPT.

Under the phrasing of this paragraph, the negotiations do not have to engage India, Israel,
with the goal of capping, reducing and eliminating the respective nuclear weapons stockpiles of those four states.\textsuperscript{233} These negotiations may proceed in stages, including via regional or other groups, as well as bilaterally, plurilaterally, and multilaterally.\textsuperscript{234}

8. Thereafter, the relevant states\textsuperscript{235} will enter negotiations to reduce their nuclear weapons stockpiles to zero. These negotiations will include all nuclear weapons, irrespective of range, type, age, size, mode of delivery, or status as deployed, non-deployed, reserve, retired, stored, awaiting disassembly, or otherwise, and regardless of whether the device is intended for peaceful or military uses.\textsuperscript{236}

9. All Participating States will support and encourage these negotiations and endeavor to promote their success.\textsuperscript{237}

10. Each Participating State possessing nuclear weapons will revise its war plans to eliminate any requirement for a capability to launch weapons on short notice; remove its nuclear weapons from high alert status;\textsuperscript{238} and maintain its missile warheads in peacetime without

---

North Korea, and Pakistan participating around the same table or signing the same instrument. All of the P5 would help facilitate agreements with these four states.

\textsuperscript{233} A special difficulty here is posed by the fact that longstanding Israeli policy is to neither confirm nor deny the existence of the nuclear weapons stockpile that it is widely credited with possessing. See supra note 66.

\textsuperscript{234} These four states might not reduce their holdings of nuclear weapons all the way to zero while the P5 retain as many as 100 weapons each. This Zero Agreement does not have to specify the exact sequence of the respective national cuts.

\textsuperscript{235} It is undetermined who would participate in the negotiation of the Zero Treaty. Surely the P5 and the four non-NPT states would have to be included. Perhaps "all" states would join the negotiation, because they would all have to be part of the Zero Treaty regime. But perhaps a smaller group, led by the states that possess nuclear weapons or the capability to build them relatively quickly (or by some larger, but still not universal group), would conduct the principal negotiations, with the others being pressed to accept the resulting document more or less as drafted. See supra text accompanying notes 169-75.

\textsuperscript{236} Different states may use different categories to describe their nuclear weapons holdings; this provision is intended to ensure that the instrument does not accidentally exclude any weapons just because they are not currently in the "stockpile," or because they are accounted in some arcane non-deployed status. This provision is also intended to cover both military weapons and so-called "peaceful nuclear explosions." See supra text accompanying notes 137 & 222.

\textsuperscript{237} Although only a handful of states will possess nuclear weapons that would be destroyed pursuant to the Zero Treaty, the verification and enforcement provisions would require universal application, so the Zero Treaty will need to have global coverage.

\textsuperscript{238} "De-alerting" means relaxing the stringent requirement for being able to use a weapon (especially an ICBM) on very short notice. This can be accomplished by internal procedures, or can be made more visible and reliable through adoption of measures such as "turning off power to missiles, decoupling warheads from missiles, immobilizing missile silo lids, and discontinuing
targeting coordinates and flight paths inserted into missile guidance computers. Each state will maintain the highest standards of safety and security over its nuclear weapons, components, and facilities. Any nuclear weapons permanently removed from delivery systems will be verifiably disassembled into their constituent elements or stored in conditions and under monitoring arrangements that would preclude them from being quickly or secretly restored to an operational condition.
11. Each Participating State will destroy or convert to other purposes all systems it possesses that were specially designed for the delivery of nuclear weapons.\textsuperscript{242} For systems that are capable of both delivering nuclear weapons and performing other functions, the Participating State will modify the system, to the fullest extent possible, to minimize its capability for delivering nuclear weapons.\textsuperscript{243}

12. Each Participating State will destroy or convert to other purposes any facilities and equipment specially designed or intended for\textsuperscript{244} conducting nuclear weapons tests at all the sites under its jurisdiction or control\textsuperscript{245} that have been used or are primarily intended for the testing of nuclear weapons. It will collapse, permanently fill, or otherwise seal any existing boreholes or tunnels within the boundaries of such sites that could be employed for nuclear weapons tests or that contain radioactive debris from a prior test.\textsuperscript{246}

\textsuperscript{242} This provision posits that the Zero Treaty would require the elimination of all dedicated strategic nuclear delivery systems (such as ICBMs and SLBMs); an alternative would permit a party to retain a small residual arsenal of these devices, in the event that reconstitution of a nuclear weapons capability becomes lawful (as in response to another party's violation of the Zero Treaty). The Zero Agreement contemplates that the elimination or conversion of these dedicated delivery systems would commence promptly, but not necessarily be completed until the Zero Treaty became effective.

\textsuperscript{243} Some bilateral U.S.-Russia nuclear arms control agreements have developed procedures for converting a dual-capable delivery system (such as a long-range bomber) to enable it to perform only a non-nuclear mission, and for reliably tagging it or otherwise making a converted asset observably different from the original. See START I, supra note 110, Protocol on Procedures Governing the Conversion or Elimination of Items Subject to the Treaty; New START, supra note 78, Protocol, Part III. But conversion of a strategic nuclear delivery system to other purposes may not be reliably irrevocable. That is, perhaps a bomber that was adapted to perform a non-nuclear mission could relatively easily and quickly be jury-rigged to deliver a nuclear weapon, too, in an emergency.

\textsuperscript{244} The Zero Agreement would not regulate all items that are "used for" or "necessary for" nuclear weapons testing activities, because such a standard would capture too many pedestrian facilities and equipment of no special interest in this context—e.g., a dormitory at a test site, where technicians sleep while preparing a test explosion, or a bulldozer, shovel or hammer used in routine construction activities there. A standard of "primarily" or "specially designed for" may be more suitable, albeit vague.

\textsuperscript{245} Use of the term "jurisdiction and control" is intended to include all of a country's national territory as well as any other locations outside its territory where it exercises actual authority. See CWC, supra note 139, art. I.2.4.

\textsuperscript{246} The CTBT, which prohibits nuclear weapons test explosions, does not require shuttering or repurposing of the sites where its parties have conducted nuclear tests, but the Zero
13. Each Participating State that possesses nuclear weapons or an advanced civil or military nuclear program will contribute to the cooperative development of the conditions for the elimination of nuclear weapons by undertaking the following actions:

a. ceasing the chemical separation or isotopic enrichment of fissile material intended for use in weapons or in excess of civilian needs;

b. enhancing the effectiveness of international and domestic controls over fissile material;

c. accepting and fully implementing the Additional Protocol with the International Atomic Energy Agency; and

d. exchanging data regarding the past production, consumption, transfer, disposition, loss, and possession of fissile material.

14. The Participating States will negotiate and promptly conclude a comprehensive, legally-binding treaty to regulate the production, possession, transfer, storage, use, handling, and disposal of fissile material. This treaty will include the creation of additional reliable international controls over facilities for the mining, extraction, concentration, conversion, enrichment, fuel fabrication, separation, processing, and use of fissile material, the storage and disposal of spent fuel, and any reprocessing of fuel. The treaty will

Agreement and Zero Treaty should do so, to further constrain a state’s ability to violate the basic prohibitions. NWC, supra note 2, at 114-15.

247. The Zero Agreement or its negotiating history will have to clarify which states are considered to possess “advanced civil or military nuclear programs,” and are therefore subject to more intense monitoring. The roster of such states could grow or shrink over time. See CTBT, supra note 129, Annex 2 (listing 44 states with advanced civil nuclear programs).

248. Again, the Zero Agreement does not specify when these various steps are to be undertaken; presumably the sequencing would be a matter of intense ongoing international bargaining.


250. Many of the commitments in this paragraph would become legally binding pursuant to an FMCT, supra text accompanying note 132.

251. Efforts to negotiate a FMCT have been repeatedly thwarted for more than a decade, but some way around that impasse will have to be developed. See supra text accompanying notes 132-133.
WHAT WOULD ZERO LOOK LIKE?

establish an international nuclear fuel bank to ensure reliable, non-discriminatory access to supplies of nuclear fuel and other materials for peaceful purposes under the auspices of the International Atomic Energy Agency and preclude diversion of those materials for weapons purposes. The treaty will also include an obligation to account for past production, consumption, transfer, disposition, and loss of nuclear materials to the maximum extent possible.  

15. In support of these negotiations and initiatives, the Participating States will meet to discuss, develop, cooperatively test, and implement the key elements of a highly effective worldwide verification system to ensure adequate monitoring of compliance with the ultimate obligation to destroy all nuclear weapons. This verification system will include multiple components such as: national and multilateral technical means of verification; routine on-site inspection; submission of relevant data to a global database; reliable sensors, tags, and seals; societal verification.

252. Some past production of fissile material can no longer be adequately accounted for; some quantities may remain permanently “lost” in various states’ systems, due to poor record-keeping and inventory control. But the FMCT will have to obligate parties to conduct forensic accounting procedures to the maximum extent possible. See Perkovich & Acton, supra note 8, at 53-57 (calling for “nuclear archeology,” to discern past national production of uranium and plutonium); Taubman, supra note 3, at 51 (noting that neither the United States nor Russia can account fully for all the nuclear materials it has produced); Fissile Material Panel, supra note 83, at 82-89 (suggesting nuclear archeology); Paine, Cochran, & Norris, Techniques and Procedures, supra note 160, at 170-71; James M. Acton, Fissile Materials and Disarmament: Long-term Goals, Short-term Steps, in GETTING TO ZERO, supra note 3, at 245, 250.

253. See supra note 159 (discussing national technical means of verification).

254. “Routine on-site inspection” refers to procedures through which inspectors from one state, or from an international organization, are permitted to enter another state and conduct data-gathering operations relevant to an assessment of compliance with an arms control treaty. In some modern arms control arrangements, these occur with great frequency, becoming a systematic, relatively non-problematic feature of the operation of the treaty. See CWC, supra note 139, art. IV.3, 5, Verification Annex; New START, supra note 78, art. XI, Protocol, Part V.

255. Several arms control treaties require parties to declare specified categories of information regarding their holdings of regulated weapons or to contribute on an ongoing basis to an exchange of treaty-relevant data. See, e.g., CWC, supra note 139, art. III (requiring declarations regarding possession of chemical weapons, production facilities and other items); New START, supra note 78, art. VII and Protocol Part Two.

256. Sensors, tags and seals can be used to preclude or detect tampering with inspectors’ equipment or to ensure that observed items are reliably counted. See, e.g., New START, supra note 78, Annex on Inspection Activities, section VI.

2014]  747
and challenge on-site inspection. The verification system will be sufficiently rigorous and intrusive that Participating States will have confidence in its ability to detect, identify, attribute, and substantiate violations within the time required to mount effective responses.

16. In support of these negotiations and initiatives, the Participating States will meet to discuss and develop specific plans and proposals for the international legal and institutional components of a highly effective worldwide enforcement system that would both deter and ensure an adequate response to any violation of the ultimate obligation to destroy all nuclear weapons. This enforcement system will include multiple components such as: diplomatic measures, resort to the institutions of international law, punitive economic measures, criminal prosecution, and military measures. The enforcement system will be sufficiently rigorous and powerful that Participating States will have confidence in its ability to deter violations, punish violators, negate the effects of any violation, and ensure that violations do not result in military or other gains.

257. See Perkovich & Acton, supra note 8, at 65-67 (explaining that societal or civil society monitoring makes the entire community responsible for helping to verify treaty compliance. There could be legal obligations to report treaty violations, and protection for whistleblowers. With modern technology, the possibilities for accurate and timely detection and communications expand; while this process may be most applicable in open, democratic societies, even a small number of dissidents in an authoritarian regime could make a difference). See supra text accompanying note 160.

258. "Challenge on-site inspection" refers to procedures through which a suspicious state or an international organization is authorized to conduct extraordinary, short-notice data-gathering activities inside a target state, when doubts have emerged regarding compliance with the treaty. The procedures for initiation of such an intrusive inspection, and the rights, functions, and equipment to be exercised by the inspectors require painstaking negotiation. See, e.g., CWC, supra note 140, art. IX, Verification Annex, Parts X, XI; CTBT, supra note 129, art. IV.D, Protocol Part II; see also DEBATE, supra note 3, at 65-67.

259. There is admittedly some circularity in this paragraph: It asserts that countries will have confidence in the efficacy of the verification system because the verification system will be constructed in a way that gives countries confidence. But at this point, it may be the best that can be done—the future verification system for the Zero Treaty will depend heavily upon improved monitoring technologies and revised attitudes toward transparency that we cannot today fully specify. One of the primary functions of the Zero Agreement will be to begin the process through which states will develop and negotiate agreements about new verification technologies and political relationships that will give substance to these claims. See supra, text accompanying notes 155-61.

260. Again, an effective enforcement system for the Zero Treaty, enabling it to rise to the rigid standards of success identified here, remains to be conceptualized, developed, negotiated, and instituted. The availability of "military measures" is a key component here—it is far from clear
WHAT WOULD ZERO LOOK LIKE?

17. In support of these negotiations and initiatives, the Participating States will create an international organization competent to operate the verification and enforcement systems, to promote effective implementation of the treaty to destroy their nuclear weapons, and to resolve disputes that might arise under it.\textsuperscript{261}

18. As states dismantle their nuclear weapons, the components will be irreversibly altered in form or content, permanently converted to purposes unrelated to nuclear weapons, or held in secure storage under conditions that preclude their being quickly or secretly reassembled into weapons.\textsuperscript{262} All such operations will be conducted pursuant to verification by the international organization and in accordance with the highest standards for security, safety of people and protection of the environment.\textsuperscript{263}

19. The Participating States will cooperate in the research and development of alternative nuclear fuel cycles that serve peaceful purposes and present stronger barriers to potential exploitation for nuclear weapons. As such technologies become available and economically viable, the Participating States will promote their adoption and use on a non-discriminatory basis.\textsuperscript{264}

\textsuperscript{261} How the parties can empower a reliable, effective military response to a violation in a manner consistent with Article 2(4) of the U.N. Charter and the veto power of the P5 in the Security Council. See supra text accompanying notes 162-67.

261. The new international organization would be similar to the CWC's OPCW and the CTBT's CTBTO; it may have some special relationship to the IAEA. The organization could be created in the Zero Treaty, or could be established prior to conclusion of that accord, in order to help facilitate its negotiation and entry into force. See supra text accompanying notes 183-86.

262. See supra text accompanying note 145 (describing the accountable "components" of a nuclear weapon).

263. This provision is similar to that of the CWC, pursuant to which each party "during transportation, sampling, storage and destruction of chemical weapons, shall assign the highest priority to ensuring the safety of people and to protecting the environment." CWC, supra note 199, art. IV.10.

20. The Participating States will develop and implement new and expanded security guaranties or other types of security relationships that might be extended to states potentially jeopardized by future conflicts, to assist in creating the conditions for a world without nuclear weapons.\(^{265}\)

21. The Participating States will devote their energies to the easing of regional tensions and to the resolution of regional conflicts so all states may achieve their legitimate security interests as they create the conditions for a world without nuclear weapons.\(^{266}\)

22. All Participating States will promote this Zero Agreement and the agreements that are developed pursuant to it, and will encourage all states to participate in the relevant negotiations and to accept the obligations of the relevant agreements.

23. Participating States offer the unilateral voluntary undertakings, attached as Annex 1 to this document, as examples of immediate steps they will initiate to facilitate progress toward the elimination of nuclear weapons. The Participating States will encourage all states to continue and expand their contributions to this roster and to fulfill their commitments under it.\(^{267}\)

help induce states to join the process, such as offering them economic assistance, technology sharing, or development aid. Alternatively, perhaps that set of bargaining chips would be deferred to the Zero Treaty. See supra text accompanying notes 192-93 (discussing possible sweeteners).

265. Two types of security guaranties have been contemplated: a “negative security assurance” is a promise by an NWS that it will not use nuclear weapons against an NNWS (provided, for example, that the NNWS fulfills its non-proliferation commitments); a “positive security assurance” is a commitment by an NWS that it will come to the aid of an NNWS that is attacked by another state with nuclear weapons (again, possibly subject to specific conditions or limitations). The NWS have each provided various versions of these assurances; the NNWS have sought stronger statements, subject to fewer caveats. See Negative Security Assurances, REACHING CRITICAL WILL, http://www.reachingcriticalwill.org/resources/factsheets/critical-issues/5442-negative-security-assurances; U.S. “Negative Security Assurances” at a Glance, ARMS CONTROL ASS’N (Sept. 2012), http://www.armscontrol.org/factsheets/negsec; Negative Security Assurance Audiences, CENTER FOR STRATEGIC & INT’L STUDIES (Jan. 2010), http://csis.org/blog/negative-security-assurance-audiences; John Freeman, The Experience of the Chemical Weapons Convention: Lessons for the Elimination of Nuclear Weapons, in ELEMENTS OF A NUCLEAR DISARMAMENT TREATY, supra note 3, at 125 (comparing the assurances offered as part of the Chemical Weapons Convention).

266. See supra text accompanying notes 187-88 (regarding regional security issues).

267. The “house gifts” listed in Annex 1 could include both procedural undertakings (e.g., a commitment to enter into negotiations on future reductions) and unilateral substantive offerings (e.g., a pledge to immediately reduce the country’s numbers of weapons or their alert status, or to increase the transparency of its stockpiles.) Broadly speaking, they constitute
WHAT WOULD ZERO LOOK LIKE?

24. The Participating States will continuously monitor the implementation of this Zero Agreement and will meet at two-year intervals at the head of government level\(^{268}\) to review its progress and to consider additional measures necessary to promote its objectives. Participating States XXX will serve as a Contact Group, to facilitate accomplishment of these objectives.\(^{269}\)

25. This Zero Agreement is not legally binding, but it represents a solemn undertaking by the Participating States on a matter of the greatest international importance and urgency. It is open for signature by all states,\(^{270}\) and will remain open for signature indefinitely.\(^{271}\)

Done, at (place), this (date)

Signatures of Participating States:

"confidence-building measures," or "transparency, security, and confidence-building measures," even without being legally binding.


269. Alternatively, the Zero Agreement could create more "diplomatic infrastructure," to facilitate pursuit of the Zero Treaty, such as a permanent staff, annual meetings, and a research and publication program. In this version, the ongoing "Contact Group" (likely comprising the P5 and a handful of like-minded other leading states) would be charged with continuous responsibilities to promote the objectives on a day-to-day basis.

270. As noted above, an alternative concept would be to specify that only particular states would join this Zero Agreement, or that only particular states would participate in the negotiations, but other states would still be invited to sign. See supra text accompanying notes 195 & 235.

271. Because this document is non-legally-binding, it does not require any of the usual treaty "boilerplate" provisions regarding entry into force, amendment, withdrawal, registration, official languages, etc., that will be included in the Zero Treaty, art. XI, infra, text accompanying notes 379-92.
Annex 1: Immediate Unilateral Undertakings by Individual Participating States

[Examples of cooperative, reciprocal, voluntary “house gifts” that could be offered by one or more states, individually or in collaboration:]272

- A declaration that fissile material removed from newly-dismantled nuclear weapons will not be used in new nuclear weapons; that fissile material from civil nuclear programs will not be used in nuclear weapons; that no newly produced fissile material will be used in nuclear weapons; and that the International Atomic Energy Agency is invited to monitor implementation of these commitments on a permanent basis.

- A declaration of the state’s total inventory of highly enriched uranium and plutonium.

- A declaration of the state’s holdings of nuclear warheads and delivery vehicles.

- A declaration of the state’s nuclear infrastructure facilities.

- A commitment to develop and use an agreed standard format to make public declarations of current and past national fissile material production and holdings.

- Creation of procedures for international monitoring of the secure storage of nuclear weapons designated for dismantlement, to confirm that such weapons and the fissile material they contain are not reintroduced into weapons stockpiles.

- Institution of additional transparency measures at sites where nuclear weapon test explosions have been conducted.

- An invitation, by states that currently conduct inspections of each other’s nuclear forces, to allow third-country officials to join actual or practice inspections as observers.

- Expansion of the monitoring operations established under the Open Skies Treaty, through acceptance of additional types of sensors.

272. See generally FISSILE MATERIAL PANEL, supra note 83, at 28-38, 59-70 (suggesting numerous possible declarations and procedures).
WHAT WOULD ZERO LOOK LIKE?

the institution of overflights in additional geographic areas, the reduction of advance notification of overflights, the reduction or elimination of exclusion zones, and/or the use of repeated or continuous overflights by remotely piloted aircraft.273

- A declaration by a state possessing nuclear weapons that it will not be the first to break the current moratorium on nuclear testing.

- A declaration by a state possessing nuclear weapons that it will not be the first to use a nuclear weapon in combat.274

- A declaration by a state that expands, or makes more legally binding, its offer of security assurances.

- A declaration that a state will cap at current levels its nuclear weapons stockpiles and/or a declaration that it will not build any new nuclear weapons.

- Removal of specified numbers of nuclear warheads from their delivery vehicles.

- Confirmed irreversible dismantlement of specified numbers of nuclear warheads or delivery vehicles.

- A declaration that codes for directing nuclear weapons to specific targets have been (or will be) altered to aim only at unpopulated ocean areas, or removed altogether from missile guidance computers and henceforth will not be stored there in peacetime.

- Revision of war plans to reduce or eliminate any requirement for a capability to launch weapons on short notice.275

273. Treaty on Open Skies, Mar. 24, 1992, S. Treaty Doc. No. 102-37 (1992) [hereinafter Open Skies Treaty]. Under the Open Skies Treaty, parties agree to allow reciprocal aerial overflights of their territories by foreign aircraft equipped with photographic and other sensors that gather military-related data in order to build confidence that no hostile or threatening activities are underway.

274. See Daniel Ellsberg, Roots of the Upcoming Nuclear Crisis, in THE CHALLENGE OF ABOLISHING NUCLEAR WEAPONS 45, 52-53 (David Krieger ed., 2009) (listing 25 occasions from 1948 to 2008 when the United States threatened or considered the first use of nuclear weapons).

Establishment of regional forums to promote security and cooperation for a world without nuclear weapons.

Creation of a national commission to compile a thorough history of the state's nuclear weapons program and collect supporting evidence.

Convening a multilateral group of national experts to develop improved measures for monitoring and verifying the possession and elimination of fissile material and nuclear weapons.

Convening a multilateral group of national experts to develop effective enforcement measures and mechanisms appropriate for a world without nuclear weapons.

Convening a multilateral group of national experts to consider appropriate provisions for a world without nuclear weapons regarding the possible retention of fissile material by the states that currently possess nuclear weapons or by all states, either as a temporary hedge against treaty violations or permanently.

V. Draft Zero Treaty

This section attempts to peer even further into the future, to imagine the political and legal structures that would be suitable for assisting states in making the final ascent from a world with low levels of nuclear weapons held by a few states to the summit of a world free of nuclear weapons altogether. The proposed draft accord is necessarily quite speculative; it would be shaped in important respects by the experience—likely to be protracted over many years—in implementing the goals of the Zero Agreement, and it would depend upon new monitoring technologies or modalities for verification of compliance and new political accommodations to permit robust transparency and enforcement activities that are scarcely conceivable today.

Unlike the preceding Zero Agreement, this Zero Treaty would be legally binding; it would be joined, sooner or later, by all states.

www.whitehouse.gov/the-press-office/2013/06/19/fact-sheet-nuclear-weapons-employment-strategy-united-states (announcing that the United States will "examine and reduce the role of launch under attack in contingency planning").

276. There is no legal significance in the vocabulary of "agreement" versus "treaty." Under the VCLT, supra note 198, art. 2.1, the nomenclature of an instrument does not affect its status.
WHAT WOULD ZERO LOOK LIKE?

Zero Treaty
For the Elimination of Nuclear Weapons

The States Parties to this Treaty,

(PP1) Determined for the sake of all mankind to end forever the scourge of nuclear weapons;

(PP2) Convinced that a global, comprehensive, timely, balanced, predictable, secure, verifiable, enforceable, sustainable, irreversible, and legally-binding treaty constitutes the most effective and reliable mechanism for achieving that objective;

277. The following discussion assumes that by the time the world is ready for negotiation and conclusion of this Zero Treaty, the following crucial conditions will have been satisfied:

(a) the CTBT will be in force;

(b) a comprehensive FMCT will have been negotiated and brought into force;

(c) the United States and Russia will have negotiated and implemented one or more new agreements achieving deep cuts in their respective nuclear weapons arsenals (including strategic and shorter-range weapons, both deployed and non-deployed), reaching very low levels of retained weapons and incorporating new, more intrusive verification mechanisms;

(d) China, France, and the United Kingdom will have joined the reductions process, implementing deep cuts in their respective nuclear weapons arsenals and accepting intrusive verification;

(e) India, Israel, North Korea and Pakistan will have joined the reductions process, eliminating or implementing deep cuts in their respective nuclear weapons arsenals and accepting intrusive verification;

(f) Iran and all other states will have either abandoned their nuclear weapons aspirations and capabilities or agreed to restrict their nuclear weapons arsenals to very low levels and accept intrusive verification;

(g) all other states will have supported the process and no new states will have begun to pursue nuclear weapons; and

(h) regional tensions (in the Middle East, South Asia, Northeast Asia and elsewhere) will have greatly abated, to the extent that affected states accept that possession or possible possession of nuclear weapons does not support their legitimate security objectives. Cf. Paine, Cochran, and Norris, International Arrangements, supra note 144, at 141-42 (listing interim steps that would be assumed to be in place to create the conditions for nuclear weapons elimination).

278. Unlike the non-legally-binding Zero Agreement, this legally-binding document uses the term "party" rather than "participating state."

279. The preamble to a treaty is not generally considered legally operative, as the main text is, but can be instrumental in interpretation of the treaty, as reflecting the parties' "object and purpose."

280. This paragraph repeats the mantra from the Zero Agreement, preambular paragraph 3, supra, text accompanying note 200.
(PP3) Believing that the time is finally ripe for achieving the complete abolition of nuclear weapons, which has for decades been fervently desired by people around the world;

(PP4) Redeeming the pledge contained in Article VI of the 1968 Treaty on the Non-Proliferation of Nuclear Weapons “to pursue negotiations in good faith on effective measures relating to cessation of the nuclear arms race at an early date and to nuclear disarmament, and on a Treaty on general and complete disarmament under strict and effective international control”;281

(PP5) Aware that the use of nuclear weapons would have devastating consequences for mankind282 and that as long as nuclear weapons exist, the possibility of their use cannot be forever precluded;

(PP6) Affirming that all human life is sacred, and that all members of the human family have the equal, inalienable right to life, liberty, peace, security and dignity;283

(PP7) Welcoming the contributions made by a series of agreements and unilateral actions by many countries that have created the conditions for achieving a world without nuclear weapons;284 and

(PP8) Inspired by the vision of a world forever free of nuclear weapons;

Have agreed as follows:285

---

281. In addition to citing Article VI of the NPT, the preamble to the Zero Treaty could also contain quotations from various NPT review conferences. The provisions from the 1995, 2000 and 2010 conferences, as cited in preambular paragraphs 8-10 of the Zero Agreement, will mostly be “old news” by that time.


283. Cf. NWC, supra note 2, at 46 (citing pmbl. ¶ 4).

284. The preamble could include here citations to some of the important interim agreements that created the progression from the initial Zero Agreement to this Zero Treaty, such as the CTBT, FMCT, and nuclear weapon free zone agreements.

285. One or more protocols or annexes (not drafted here) may be appended to the Zero Treaty to provide additional details of the specifications for implementation, inspections, definitions, etc. Cf. CWC, supra note 139; New START, supra note 78.
WHAT WOULD ZERO LOOK LIKE?

Article I
Fundamental Obligations

1. Each Party to this Treaty shall never, under any circumstances:

   a. Develop, test, produce, acquire, possess, retain, stockpile, deploy or transfer nuclear weapons or their components, except as specified in Article II;
   b. Use, threaten to use, or engage in any military or other preparations to use nuclear weapons;
   c. Develop, test, produce, acquire, possess, retain, stockpile, deploy or transfer delivery vehicles for nuclear weapons, except as specified in Article II; or
   d. Assist, encourage, collaborate with, participate with, or induce, in any way, anyone to engage in any activity prohibited to a Party under this Treaty.

---

286. Cf. NWC, supra note 2, at 48 (citing article I); CTBT, supra note 129, art. I ("Basic Obligations"); CWC, supra note 139, art. I ("General Obligations").

287. Unlike the Zero Agreement, the Zero Treaty, as a legally-binding document, uses the mandatory verb "shall," instead of "will" or "should," and it refers to "Parties" instead of "Participating States."

288. The language of "never, under any circumstances" is subject to the qualification that reconstitution of a nuclear weapon inventory could in some circumstances be a key, allowable response to an illegal "breakout" attempt by another Party.

   In contrast, the CWC, which uses similar language, was intended "to bind states parties not to acquire and use chemical weapons even if attacked by hostile states with such weapons." THOMAS GRAHAM, JR. AND DAMIEN J. LAVERA, CORNERSTONES OF SECURITY 1168 (2003) (also interpreting the BWC in the same absolutist fashion).

289. As with prior arms control agreements, this provision does not attempt to regulate "research," defined as activity that occurs in a library or laboratory, where the capabilities for verification of compliance would be too difficult, and where the problem of dual capability is most pronounced. In contrast, the NWC does ban nuclear weapons related research. NWC, supra note 2, at 48 (citing article I(1)(g)).

290. This string of prohibitory verbs combines terms from CWC, supra note 139, art. I; CTBT, supra note 129, art. I; and elsewhere.

291. The language of "engage in any military preparations to use" comes from the CWC, supra note 139, art. I.1(c); this text adds a prohibition on "other" types of preparations. See NWC, supra note 2, at 48 (citing article I(1)(a)(b)). The negotiating history of the treaty would have to make clear that activities such as the continued possession of components of disassembled nuclear weapons, as permitted by the Zero Treaty, would not constitute prohibited "preparations to use."

292. Prior treaties prohibit actions that would "assist, encourage, or induce" behavior incompatible with the agreement; this proposed text adds "collaborate with" and "participate
2. Each Party shall destroy all the nuclear weapons that it owns or
possesses, or that are located at any place under its jurisdiction
or control.298

3. Each Party shall destroy or convert to permitted purposes294 all
the delivery vehicles for nuclear weapons that it owns or pos-
sesses, or that are located at any place under its jurisdiction or
control.

4. Each Party shall destroy or convert to permitted purposes all
the facilities and equipment that it owns or possesses, or that
are located at any place under its jurisdiction or control,
that have been used or principally designed or intended for
use in the research, testing, manufacturing, storage, process-
ing, maintenance, or elimination of nuclear weapons or com-
ponents.295 The following designated facilities and locations
shall be subject to special monitoring: [list, by country, particu-
larly important sites or buildings that have performed signifi-
cant nuclear weapon-related work and will be verifiably de-
stroyed or converted to other purposes; specialized monitoring
arrangements will be developed for each and described in an
annex.]296

with" to capture coordinated planning and operational activities that might not otherwise be
covered. See CWC, supra note 139, art. I.1(d); Ottawa Convention, supra note 172, art. 1.1(c);
Oslo CMC, supra note 173, art. 1.1(c). The CTBT prohibits "causing, encouraging, or in any way
participating in" the conduct of a nuclear explosion, CTBT, supra note 129, art. I.2.

299. The Chemical Weapons Convention also deals with weapons that are "abandoned" on
the territory of another state; that scenario seems unlikely with nuclear weapons. CWC, supra note
139, art. I.3. The CTBT requires parties to "prohibit and prevent" nuclear weapons tests at
locations under their jurisdiction and control; following that model, the Zero Treaty could
prohibit and prevent possession of nuclear weapons, but since this draft requires destruction of
nuclear weapons at all locations under a party’s jurisdiction and control, the "prohibit and
prevent" language would seem redundant. CTBT, supra note 129, art. I.1.

294. Some prior agreements use the term "activities not prohibited"; the term "permitted
purposes" here aims at the same concept, but avoids a double negative. But it is noteworthy that
under international law, treaties do not usually "permit" activities—a state is considered inher-
ently free to undertake any activities that are not specifically prohibited by law. See CWC, supra
note 139, art. II.9, VI.

295. At some suitable point in the negotiation process, each state would be required to
declare or list all its relevant facilities, and other states could contest whether additional sites
should be added to the roster, to ensure that all appropriate locations were covered.

296. The Treaty could list here particular sites or installations that would require special
monitoring. See, e.g., the Savannah River Site and Y-12 National Security Complex (used for
producing radioactive materials for nuclear weapons), Pantex Plant (for assembling and refurbish-
ing nuclear weapons), and Kansas City Plant (for producing or procuring non-nuclear compo-
nents). See Our Locations, NAT’L NUCLEAR SEC. ADMIN. (NNSA), http://nnsa.energy.gov/aboutus/
WHAT WOULD ZERO LOOK LIKE?

5. All destruction, closure, conversion, maintenance, storage, transportation, and other operations required by the Treaty shall be monitored by the Organization.\(^{297}\) In conducting these operations, each Party shall assign the highest priority to ensuring security, safety of people and protection of the environment.\(^{298}\) Destruction and conversion operations shall be completed no later than seven years after the entry into force of this Treaty.\(^{299}\)
6. Each Party shall, in accordance with its constitutional processes, adopt the necessary measures to implement its obligations under this Treaty, including:

a. Prohibiting natural and legal persons anywhere on its territory or at any other place under its jurisdiction or control from undertaking any activity prohibited to a Party under this Treaty, including by enacting or expanding penal legislation;

b. Prohibiting natural and legal persons having its nationality from undertaking any activity prohibited to a Party under this Treaty anywhere, including by enacting or expanding penal legislation;

c. Concluding appropriate agreements to extradite to another Party persons to be prosecuted for actions inconsistent with this Treaty, and

The timetable for converting or destroying delivery vehicles and the buildings and other facilities that constitute the nuclear weapons infrastructure could be set to match the seven-year period for elimination of nuclear weapons; alternatively, it could be extended, depending on how many such items and sites remain at the time the Zero Treaty is concluded and on whether parties wish to convert or to destroy them. The Treaty could specify a date, or could leave that to case-by-case determination through the Organization.

300. Paragraphs 6a and 6b are adapted from CWC, supra note 139, art. VII.1, to prevent circumvention of the treaty obligations imposed upon states, by requiring the states to extend similar obligations, in the form of penal legislation, to their nationals and throughout their territories. The treaty could go further and declare that actions inconsistent with the treaty constituted international crimes (suitable for prosecution in an international tribunal) or crimes of universal jurisdiction (suitable for prosecution by any state, regardless of the location of the act or the nationality of the actor). These prohibitions could apply both to persons and to corporations and other entities. See NWC, supra note 2, at 49, 66-68 (citing articles I(5), VI, VII(1)-(2)); Rome Statute of the International Criminal Court art. 1, Jul. 17, 1998, UN Doc. A/CONF. 183/9, 2187 UN.T.S. 90; 37 I.L.M. 1002 (1998) (entered into force Jul. 1, 2002) [hereinafter Rome Statute] (treaty creating the International Criminal Court, with jurisdiction to prosecute “the most serious crimes of international concern.”). For a discussion regarding universality jurisdiction, see Restatement (Third) of Foreign Relations Law of the United States § 404 (1987) (discussing the small category of offenses “recognized by the community of nations as of universal concern,” enabling any state to assert jurisdiction).

The Zero Treaty could also require each party to designate a National Authority, to serve as the focal point for domestic implementation measures and for communications and liaison with the Organization. See CWC, supra note 139, art. VII.4; CTBT, supra note 129, art. III.4.

301. See NWC, supra note 2, at 68 (citing article VII(2)).
d. Adopting appropriate measures to protect persons providing to the Organization information regarding actions related to or inconsistent with this Treaty.302

Article II
Permitted Activities

1. A Party303 may retain304 and maintain305 components306 for a limited number307 of nuclear weapons, provided that:

---

302. This provision is designed to promote adequate protection for whistleblowers, who alert the Organization to prohibited actions, and who might otherwise be subject to retaliation by governments, employers or others. See NWC, supra note 2, at 66, 72 (citing articles VI(1)(b), VII(C)).

303. In this draft, “any” Party would be allowed to hold these components of nuclear weapons; an alternative would confine that right to only those countries that had previously (and legally) possessed nuclear weapons (i.e., the P5 and the four non-NPT states). As drafted, the provision might allow and encourage some “proliferation” of nuclear weapons components, as some current NNWS might decide to build small stockpiles of weapons components for the first time as a hedge against another country’s violation of the Zero Treaty. On the other hand, the alternative concept would perpetuate an unpopular “discriminatory” aspect of the NPT.

304. The Zero Treaty could further restrict a party’s right to retain components of nuclear weapons by limiting the maximum quantity of such items that could be held and/or by establishing a progressive timetable under which the party must reduce or eliminate its holdings.

The concept of “retaining” these components implies that a party would be allowed to “extract” them from intact nuclear weapons that it was destroying but perhaps not be allowed to “create” new components from scratch. The drafters of the Zero Treaty could be explicit about this by allowing or prohibiting new manufacturing of components.

The provisions of this article would have to apply, mutatis mutandis, to the components of nuclear weapons that were dismantled prior to the entry into force of the Zero Treaty as well as to those disassembled under it.

305. The Zero Treaty could include a definition of the sorts of “maintenance” activities a party would be permitted to undertake regarding these components. If so, it could define a distinction between maintenance, testing, repair, refurbishment, remanufacturing, etc.

306. The Zero Treaty will need to define the critical “components” being regulated. Notionally, these could include: (a) the fissile material (extracted from the uranium or plutonium “pit” or “physics package”); (b) the shaped chemical high explosive; and (c) the “electronics package” of detonator charges. Different types of weapons might include different critical components. See supra text accompanying note 145.

307. The Zero Treaty could specify here the specific quantities of various components that parties would be allowed to retain.

2014] 761
a. All components shall be held in safe and secure conditions in declared storage facilities;\(^{308}\)
b. All components shall be permanently tagged and continuously monitored;\(^{309}\)
c. No storage facility shall contain all the components necessary to create a nuclear weapon;\(^{310}\)
d. Any movement or reassembly of components shall not be conducted quickly or secretly, and not for more than one weapon at a time;\(^{311}\) and
e. Ten years after this Treaty enters into force, the Parties shall evaluate whether the right to hold components shall be further restricted or prohibited.\(^{312}\)

2. A Party may withdraw components from a storage facility for destruction or for use in applications unrelated to nuclear weapons,\(^{313}\) provided that:

\(^{308}\) The Zero Treaty, or decisions of the Organization implementing it, will need to establish standards for the safety and security of the storage facilities and the procedures for making the required national declarations. The Zero Treaty could require the storage sites to be publicly declared, or they could be disclosed in confidence to the Organization.

\(^{309}\) A critical challenge for the Zero Treaty’s verification arrangements will be to design a system allowing reliable monitoring of these components without providing the monitors with too much information about the party’s design of nuclear weapons.

\(^{310}\) In addition, the Zero Treaty could require that facilities storing the components of nuclear weapons should be located at some substantial distance apart to further reduce the possibility for quick, secret reconstitution. *Cf.* START I Treaty, *supra* note 110, art. IV.11 (requiring at least 100 km separation between certain ICBMs, launchers, and other related equipment). For “two-stage” nuclear weapons, the Zero Treaty could specify a degree of physical separation of the two types of explosive devices.

\(^{311}\) The Zero Treaty or its implementing procedures could specify how rapid and transparent the potential reconstitution process could be by defining, for example, how many subcomponents each nuclear weapon must be broken down into, how far apart the components must be held, what physical impediments might block access to the storage facilities, whether the party would have to announce publicly whenever it was handling, moving, or reassembling components, whether permission would be required from the Organization prior to any movement of components, and whether the party would need to invite observers from the Organization to monitor the process. Perhaps the timetable required for reconstituting weapons could be gradually further stretched out over the life of the Zero Treaty.

\(^{312}\) The parties could decide—such as at a review conference for the Zero Treaty—to amend the Treaty to restrict or prohibit the right to hold components. Alternatively, the Treaty could specify at the outset that a party’s rights in this regard should automatically expire after a set period of time.

\(^{313}\) Probably, the main component that a party might be interested in converting to peaceful purposes would be the fissile material. It is possible that by the time the world gets close
WHAT WOULD ZERO LOOK LIKE?

a. The component shall be destroyed or irreversibly converted into a form unsuitable for use in a nuclear weapon; or
b. The component shall remain tagged and subject to continuous monitoring.

3. A Party may retain delivery systems for nuclear weapons, provided that:

a. No inter-continental ballistic missiles or submarine-launched ballistic missiles shall be retained;

b. All retained delivery systems shall be dedicated exclusively to purposes other than the delivery of nuclear weapons; any features specially related to the delivery of nuclear weapons shall be removed or converted to other purposes; and the delivery system shall remain subject to inspection;

and to concluding a Zero Treaty, countries will already have extracted sufficient quantities of any components from nuclear weapons that were disassembled and destroyed in prior years, so they would have little need to re-use any further components from the last remaining nuclear devices, and those items could be consigned to permanent storage or destruction.

314. In some applications, perhaps, periodic, rather than continuous, monitoring, or monitoring of a statistical sampling would be sufficient and less burdensome.

315. This provision is grounded on the proposition that the short flight times of ICBMs and SLBMs make them uniquely threatening and on the fact that they have been traditionally allocated almost exclusively to nuclear missions, with little if any role in conventional warfare.

An alternative would be to allow the retention of a limited number of ICBMs or SLBMs and making them available for delivery of nuclear or conventional weapons in response to another state’s illegal breakout activity. This limited number could be reduced over time. If any ICBMs or SLBMs may be retained, the Treaty will also need to address the extent to which those weapons may be maintained, refurbished, remanufactured, etc. The Zero Treaty could also allow a party to convert these missiles to peaceful purposes, such as in launching space vehicles.

Another alternative would be to require elimination of ballistic (and cruise) missiles of shorter ranges, too—at least any such systems that had ever been tested or deployed with nuclear weapons. Cf. NWC, supra note 2, at 84 (citing article XII requiring destruction of heavy bombers, ballistic missile submarines, and ground-launched cruise missiles as well as ICBMs and SLBMs).

316. Prior U.S.-U.S.S.R. (and Russia) treaties have included provisions for the conversion of nuclear delivery systems such as long-range bombers, to non-nuclear missions. See START I, supra note 110, Protocol on Procedures Governing the Conversion or Elimination of Items Subject to the Treaty; New START, supra note 78, Protocol, Part III. In the absence of frequent inspection, however, such conversion may not be reliably irreversible.

Again, an alternative would be to allow the retention of a limited number of nuclear-capable bombers and other delivery systems, making them available for delivery of nuclear weapons if another state has illegally reconstituted its nuclear weapons. This limited number could be reduced over time.
c. No new systems designed for the delivery of nuclear weapons shall be developed, tested or deployed, and no system designed for purposes other than delivery of nuclear weapons shall be tested in a nuclear weapons mode.

Article III
Definitions

1. "Nuclear weapon" means any device that is capable of releasing nuclear energy in an essentially uncontrolled manner and that has a group of characteristics that are largely appropriate for use for warlike purposes, regardless of whether the device is intended for warlike or peaceful purposes. The term includes weapons that are deployed, non-deployed, inactive, on reserve, retired, awaiting destruction, and in any other status.


3. "Destroy" means to disassemble, denature, deform, disable, incapacitate, or render in an essentially irreversible way into a form unsuitable for weapons purposes.

317. This provision would require a definition of what counts as a "new" system as opposed to a modification of an existing type. Cf. SALT II, supra note 107, at art. IV.9 (associated Agreed Statements and Common Understandings) (allowing each side to deploy one new type of ICBM, and defining "new" for this purpose).


319. Cf. NWC, supra note 2, at 50 (citing article II presenting eighty definitions).

320. The first sentence of this definition is adapted from the Treaty of Tlatelolco, supra note 117, art. 5. This definition is designed to capture so-called "peaceful nuclear explosion" devices, as well as weapons, and to capture all nuclear weapons regardless of their status. See supra text accompanying notes 78-81, 137, 222 & 307.

321. For this purpose, the main components of a nuclear weapon would be the fissile material, the high explosive detonator, and the electronics, although numerous other items are relevant. See supra text accompanying notes 145 & 306 (regarding components of a nuclear weapon).

322. This definition is based on the CWC's definition of "destruction of chemical weapons." CWC, supra note 139, Verification Annex, Part IV(A), ¶ 12. The notion is that an actor who was attempting to construct a new nuclear weapon would not be materially advantaged by having access to destroyed components of a previous weapon; the task would be essentially as difficult, expensive, and time-consuming as starting from scratch. See Gronlund et al., supra note 296,
WHAT WOULD ZERO LOOK LIKE?

4. "Delivery system" means any mechanism that has been developed, tested, or deployed for, or is capable of, transporting a nuclear weapon to a target.

Article IV
Nuclear Weapons and Delivery Systems

1. Each Party shall declare, upon entry into force of the Treaty for it, and annually thereafter, all the nuclear weapons and components it owns or possesses or that are located at any place under its jurisdiction or control, and shall provide to the Organization its plan for destroying or converting them.\(^{323}\)

2. Each Party shall declare, upon entry into force of the Treaty for it, and annually thereafter, all the delivery systems for nuclear weapons it owns or possesses or that are located at any place under its jurisdiction and control, and shall provide to the Organization its plan for destroying or converting them.

3. The declaration shall specify the location, characteristics, condition, storage procedures, and destruction or conversion method and timetable for each item, on a standard form developed by the Organization.\(^{324}\)

---

\(^{323}\) For most states, this provision would require simply a declaration that it possessed no nuclear weapons, but even a state that had allowed another state to base nuclear weapons on its territory would be required to declare that fact. \textit{Cf.} NWC, \textit{supra} note 2, at 58 (citing article III collecting into one article all the required declarations).

\(^{324}\) The Organization— or a provisional precursor to it—will have to be operational even before the Zero Treaty enters into force to accomplish the preparation of suitable standardized forms for reporting required data.
Article V
Nuclear Weapon Test Sites

1. Each Party shall declare, upon entry into force of the Treaty for it, all sites at which it has conducted nuclear weapon test explosions, and provide to the Organization its plan for completing the actions required by this article.

2. Each Party shall close or convert to purposes unrelated to nuclear weapons all its declared nuclear weapon test sites and submit them to continuous monitoring.

3. Each Party shall collapse, fill, or permanently seal all emplacement boreholes and tunnels at such sites.

4. Each Party shall destroy or convert to other purposes and submit to continuous monitoring all equipment or facilities specially designed for purposes of conducting nuclear weapon tests.

325. Some countries have conducted nuclear tests outside their own national territory; in those instances, two states would have to collaborate to fulfill the obligations of this article. Similar collaboration was required to implement provisions of the INF Treaty, supra note 79, Memorandum of Understanding Regarding the Establishment of the Data Base for the Treaty Between the Union of Soviet Socialist Republics and the United States of America on the Elimination of Their Intermediate Range and Shorter-Range Missiles, U.S.-U.S.S.R. (Dec. 8, 1987), available at http://www.fas.org/nuke/control/inf/text/inf3.htm [hereinafter INF MOU] (identifying U.S. bases in Germany, the Netherlands, Italy and elsewhere subject to inspection by the Soviet Union) and the CWC, supra note 139, Verification Annex, Part II, ¶¶ 19-21 (establishing procedures for conducting an inspection of a chemical facility owned by one state but located in the territory of another state).

326. The Treaty could specify a required deadline for completing the various actions required by this article. Some (such as collapsing any remaining emplacement tunnels) could probably be accomplished quickly, while others (such as converting sites and equipment to permitted purposes) could require quite a bit of time, at least for some locations.

327. True "closure" of a large area, such as the Nevada National Security Site, may not be practical; more likely, such locations would be "converted" to other purposes, which could include military activities not connected to nuclear weapons. See Nevada National Security Site, supra note 150 (regarding Nevada National Security Site).

328. This text would require that a country could not conduct even "permitted" nuclear weapons-related activities at a test site. It may be more "efficient" to allow such activities to be conducted at a former test site, but perhaps the history of that location should override efficiency.

329. This provision would effectively lengthen the time required before a party could conduct a nuclear weapon test.

330. Alternatively, the text could list the specific items of equipment and facilities that would be subject to intense regulation.

331. The monitoring could be accomplished by cameras and other mechanical sensors, by roving or permanent observers, or otherwise, according to the characteristics of the particular site.
WHAT WOULD ZERO LOOK LIKE?

5. Each Party shall remove from the site or render unrecoverable or unusable any residual fissile material that has remained from previous testing.\textsuperscript{332}

Article VI

Nuclear Weapon Laboratories, Facilities and Personnel\textsuperscript{338}

1. Each Party shall declare, upon entry into force of the Treaty for it, all laboratories and related facilities or sites at which it has conducted nuclear weapon-related research, development, fabrication, production, maintenance, or testing activities,\textsuperscript{334} and provide to the Organization its plan for completing the actions required by this article.\textsuperscript{335}

2. Each Party shall close or convert to purposes unrelated to nuclear weapons all such laboratories, facilities and sites and submit them to continuous monitoring.\textsuperscript{336} A converted laboratory, facility or site shall be rendered no more capable of being re-converted to nuclear weapons purposes than is any other comparable laboratory, facility or site used for peaceful purposes.\textsuperscript{337}

3. No Party shall construct new laboratories, facilities or sites for purposes of nuclear weapon-related research, development, fabrication, production, maintenance, or testing.\textsuperscript{338}


\textsuperscript{333} Cf. NWC, supra note 2, at 82 (citing article XI).

\textsuperscript{334} Most such locations are well-known, so making the declaration would not be burdensome, but there might be a need to specify more precisely which types of locations are to be included in the declaration and to create procedures for challenging another party's omission of a location that should have been listed.

\textsuperscript{335} Again, the Treaty could specify deadlines for completing each of these types of actions.

\textsuperscript{336} Continuous monitoring of national weapons laboratories is likely to pose special problems, since they will continue to conduct sensitive national security work unconnected to nuclear weapons; intrusive monitoring risks revealing national security and proprietary information.

\textsuperscript{337} This provision is adapted from CWC, supra note 139, art. V.14, designed to ensure that a party does not retain any special advantage from a converted nuclear weapons asset.

\textsuperscript{338} This provision includes a prohibition even on undeclared "defensive" nuclear weapons-related research and other functions. In contrast, some other treaties do not categorically prohibit activities that are not directed at producing offensive weapons. See CWC, supra note 139, art. II.9(b) (permitting chemical weapons activities that are related to protection against chemical
4. Each Party shall destroy or convert to other purposes and submit to continuous monitoring all equipment specially designed for purposes of nuclear weapon-related research, development, fabrication, production, maintenance, or testing.

5. The following designated facilities and locations shall be subject to special monitoring: [list, by country, particularly important laboratory buildings or items of equipment that have performed significant nuclear weapon-related work and will be eliminated or converted to other purposes; specialized monitoring arrangements will be developed for each and described in an annex.]339

6. Each Party shall declare all individual scientists, technicians and researchers who participated in nuclear weapon-related research, development, fabrication, production, maintenance, or testing activities at any time in the previous ten years, and shall report annually on a standardized form the professional activities of each.340 For any declared person who has been involved

weapons), and the BWC, supra note 194 art. I.1 (allowing biological weapons related actions undertaken for “prophylactic, protective or other peaceful purposes”).


340. The concept here is to monitor the professional activities (the whereabouts and “whatabouts”) of anyone who, in the previous ten years, had participated in nuclear weapon-related activities (perhaps confined to those who had devoted a substantial percentage of their professional activity to that sort of enterprise). The content and level of detail of the reports
WHAT WOULD ZERO LOOK LIKE?

in any way in nuclear weapon-related activities in the previous year, the reporting shall be particularly detailed. 341

Article VII
The Organization 342

1. The Parties hereby establish the Zero Treaty Organization, to assist them in achieving the object and purpose of this Treaty, to ensure effective implementation of its provisions, including those for international verification and enforcement of compliance with it, and to provide a forum for consultation and cooperation.

2. The Organization shall consist of the Assembly, the Executive Council, and the Secretariat.

3. The costs of the Organization's activities shall be paid annually by Parties in accordance with the United Nations scale of assessments, adjusted to take into account differences in membership between the United Nations and the Organization. 348

4. The Organization shall establish procedures for cooperation, consultation, fact-finding, and resolution of disputes. 344

remain to be worked out; a standard reporting format would be developed. The results of the reporting might be held as confidential information within the Organization. There might be a procedure through which the Organization or a party could suggest that another party should also report on additional specified individuals.

341. This provision would not prohibit or regulate the person's activities or livelihood, but would require reporting about them.

342. This draft is based upon the models of the CWC, supra note 139, art. VIII, and the CTBT, supra note 129, art. II. It would eventually have to be greatly expanded, to deal with numerous critical structural and administrative questions, such as the powers, procedures, and functions of each organ; the composition of the Executive Council; and the privileges and immunities of the organization and its staff members. These matters are not specified in this draft because they are lengthy and—although important—they are not unique to the functioning of the Zero Treaty. Cf. NWC, supra note 2, at 70, 86 (citing articles VIII, XIV).

343. This provision is comparable to CWC, supra note 199, art. VIII.7, and CTBT, supra note 129, art. II.9.

344. The Zero Treaty will probably include a lengthy section regarding procedures for enabling and requiring the parties to cooperate through the Organization in resolving ambiguous situations and settling disagreements. Again, these are not specified here because of their length and familiarity. See CWC, supra note 139, arts. IX, XII, XIV; CTBT, supra note 129, arts. V, VI; see also NWC, supra note 2, at 86 (citing article XIV).

2014] 769
Article VIII
Verification\textsuperscript{345}

1. The verification system for this Treaty shall include:
   
   a. Declarations of relevant past and present data by each Party;\textsuperscript{346}
   
   b. National and multinational technical means of verification;\textsuperscript{347}
   
   c. Installation of tamper-proof tags and seals or other inventory-control devices on nuclear weapon-related components, items, canisters and facilities;\textsuperscript{348}
   
   d. Installation of remote and on-site radioactivity and other sensors providing high-quality, authenticated, real time data to the Organization;\textsuperscript{349}

---

\textsuperscript{345} The verification mechanisms will have to be a major portion of the eventual Zero Treaty. At present, the CWC, CTBT, and New START represent the "state of the art" in arms control verification; they include provisions that are as robust, diverse, and effective as countries have to date been willing and able to negotiate. But the Zero Treaty will demand much more far-reaching inspection powers, running well beyond current experiences and capabilities; it will require new monitoring, communications, and data processing technologies and new political relationships to tolerate a higher degree of intrusions than have yet been contemplated. It is therefore premature to offer detailed drafting suggestions here. See supra text accompanying notes 155-61; cf. NWC, supra note 2, at 63 (citing article V).

\textsuperscript{346} Cf. CWC, supra note 139, art. III; New START, supra note 78, art. III.8; INF Treaty, supra note 79, art. IX; INF MOU, supra note 325; see Paine, Cochran & Norris, Techniques and Procedures, in CANBERRA COMMISSION ON THE ELIMINATION OF NUCLEAR WEAPONS, BACKGROUND PAPERS, supra note 56, at 168-71 (use of verified data declarations and exchanges in treaty monitoring).

\textsuperscript{347} See supra note 159 (explaining NTM and MTM); cf. CTBT, supra note 129, art. IV.5.6; New START, supra note 78, art. X; ABM Treaty, supra note 105, art. XII. See Paine, Cochran & Norris, Techniques and Procedures, in CANBERRA COMMISSION ON THE ELIMINATION OF NUCLEAR WEAPONS, BACKGROUND PAPERS, supra note 56, at 167-68 (role of NTM in verifying compliance with nuclear elimination requirements).


\textsuperscript{348} See, e.g., New START, supra note 78, at Fourth Agreed Statement (authorizing the use of tamper-proof seals on the weapons bays of certain deployed heavy bombers).

\textsuperscript{349} For comparison, the CTBT specifies that a variety of types of automated, high quality internationally-controlled monitoring stations shall be established in the territories of its parties,
WHAT WOULD ZERO LOOK LIKE?

e. Routine or continuous monitoring overflights by aircraft of the Organization; 350
f. Interdiction of traffic (on road, rail, sea and air) by the Organization to inspect for and seize contraband; 351
g. Unimpeded, systematic, routine on-site inspection; 352
h. Taking and analysis of samples 353
i. Public sources and societal verification, including via social media; 354
j. The right of the Organization to interview any person confidentially, to take sworn testimony, to mandate the production of documents and materials, and to provide protection to cooperating individuals; 355 and
k. Challenge on-site inspection, including full, immediate access to confirm compliance with the Treaty. 356

350. This type of monitoring could be similar to that undertaken pursuant to the Open Skies Treaty, supra note 273, but could provide broader geographic coverage, additional suites of sensors, and more frequent overflights, including perhaps continuous observation by drone aircraft. The aircraft might be owned and operated by the Organization or by individual parties.

351. This type of monitoring could be similar to that undertaken pursuant to the Proliferation Security Initiative. See Proliferation Security Initiative, DEPT. OF STATE, http://www.state.gov/t/isn/c10390.htm (last visited Mar. 20, 2014). The parties to the Zero Treaty would provide their consent, pursuant to designated procedures, allowing the Organization to intercept suspicious traffic.

352. Many arms control treaties have provided different types of programs for routine on-site inspection, with varying kinds of powers for the inspectors. See, e.g., INF Treaty, supra note 79, art. IX, Protocol on Inspections (permitting up to twenty inspections per year and continuous monitoring at the portals of key facilities for thirteen years); CWC, supra note 139, Verification Annex, Part X, ¶¶ 46-52 (presenting the procedures for "managed access," to balance the interests of inspectors and the inspected state and facility); New START, supra note 78, art. XI, Protocol, Part V (specifying two different types of inspections, totaling eighteen inspections per year). The inspections under the Zero Treaty would be much more demanding and intrusive; inspectors would need much more than the current exercise of managed access.

353. Inspectors could seek environmental samples of air, soil, water, flora, and fauna, as well as materials or wipes from facilities of interest and biological samples from humans. Cf. CWC, supra note 139, Verification Annex, Part II, ¶¶ 52-58; CTBT, supra note 129, Protocol, ¶ 69.d, h.

354. See supra note 160 (regarding societal verification).

355. The Organization should have quasi-judicial legal power to exercise jurisdiction inside the territory of parties and to protect and reward whistleblowers. Cf. NWC, supra note 2, at 66, 68-69 (citing articles VI(1)(b), VII(C)); see also Perkovich & Acton, supra note 8, at 64 (under-scoring the value of interviews of key personnel).

356. "Routine" inspection is undertaken on a regular basis, such as to confirm the accuracy of a state's declared data, without any suspicion of violation; in contrast, a "challenge" inspection would be initiated when concerns have arisen about non-compliance. Provisions for requesting
2. The Organization shall sponsor collaborative research into improved and additional sensors and verification techniques. As these become available, they shall be considered for implementation by the Organization on an expedited basis.  

3. The Organization shall promptly make available to each Party all the information collected through the Treaty’s verification system, together with suitable analysis.  

4. Each Party shall fully cooperate with the Organization in all verification activities.  

5. All verification activities shall be limited to the subject matter of this Treaty and shall be carried out with full respect for the sovereignty of states and in the least intrusive manner possible, consistent with the effective and timely accomplishment of their objectives. Each Party and the Organization shall refrain from any abuse of the right of verification.  

6. No Party shall interfere with the verification operations of the Treaty or with national or multinational technical means of verification of any Party operating in accordance with international law. No Party shall engage in concealment activities that impede verification of compliance with the Treaty.  

and conducting a challenge inspection may require detailed elaboration in the negotiations and treaty text. See CWC, supra note 139, art. IX.8-25, Verification Annex, Part X; CTBT, supra note 129, art. IV.D, Protocol Part II.  

357. Verification is never a "finished" product; the parties will have to continuously seek to refine and upgrade their capabilities. This provision is based on CTBT, supra note 129, art. IV.11.  

358. Prompt circulation of data collected by the verification system will enable each party to make its own judgments about others’ compliance; analysis by the Organization will assist in interpretation of the data. CTBT, supra note 129, art. IV.9.  

The Treaty would also need provisions regarding the possibility that parties may provide to and receive from the Organization sensitive information that should not be made public. See CWC, supra note 139, Annex on the Protection of Confidential Information; CTBT, supra note 129, art. II.7.  

359. This provision is based on CTBT, supra note 129, art. IV.3.  

360. This provision is based on CTBT, supra note 129, art. IV.2. Although the content of the paragraph is correct, alternatively, it could be deleted, in recognition of the fact that the Zero Treaty will require a transformation in states’ attitudes regarding secrecy, such that they would no longer be as protective against intrusive inspections.  

361. Provisions of this sort have become standard for arms control agreements, with slight variations. See, e.g., CTBT, supra note 129, art. IV.5,6; New START, supra note 78, art. X.
WHAT WOULD ZERO LOOK LIKE?

Article IX

Enforcement

1. The enforcement system for this Treaty shall include:
   a. Diplomatic measures;
   b. Legal measures;
   c. Economic measures;
   d. Law enforcement measures; and
   e. Military measures.

2. If a Party believes that another Party may have violated the Treaty, it may:

362. As with verification, the Zero Treaty will have to be path-breaking regarding enforcement provisions. Existing arms control treaties provide a variety of mechanisms for consultations, exchanges of information, and discussions in treaty organs to resolve concerns about compliance. See, e.g., CWC, supra note 139, arts. XII, XIV; CTBT, supra note 129, arts. V, VI. But the Zero Treaty will require the creation of much more vigorous and powerful mechanisms for response to treaty violations. These will have to be the most demanding and innovative portions of the Zero Treaty, eclipsing the accomplishments of current negotiators, in ways we cannot currently discern. See supra text accompanying notes 162-67.

363. Diplomatic measures could include unilateral and collective political pressure, as well as actions through regional organizations and the United Nations General Assembly.

364. Legal measures could include exercise of rights under the VCLT, supra note 139, and resort to the International Court of Justice and the United Nations Security Council, as well as to the organs of the Zero Treaty Organization. See Rebecca Bornstein, Enforcement Scenario: Iran, in ELEMENTS OF A NUCLEAR DISARMAMENT TREATY, supra note 3, at 156-58.

365. Economic sanctions and related restrictions could be imposed by one or several countries, by the United Nations Security Council, or by the organs of international economics, such as the World Bank or International Monetary Fund. See Rebecca Bornstein, Enforcement Scenario: Iran, in ELEMENTS OF A NUCLEAR DISARMAMENT TREATY, supra note 3, at 158-60.

366. The Zero Treaty requires each party to enact penal legislation prohibiting its nationals and other real and legal persons from engaging in activities that would be prohibited to the state. See supra note 301; Rebecca Bornstein, Enforcement Scenario: Iran, in ELEMENTS OF A NUCLEAR DISARMAMENT TREATY, supra note 3, at 157. The International Criminal Court, supra note 300, could also play a role in law enforcement operations.

367. The single most vexing point regarding enforcement of the Zero Treaty concerns the question of what, if any military measures may be applicable in response to a serious violation. The United Nations Security Council, of course, has the power to authorize or require the exercise of force in response to a threat to the peace, UN Charter, supra note 58, art. 39. But the Security Council may be blocked by the exercise or threat of a P5 veto. An individual state or group of states may conclude that another party's illegal effort to break out of the Zero Treaty justified action (such as a military strike against the sites at which the violating country was re-assembling or storing its illicit nuclear weapons) as an exercise of national self-defense, even without Security Council endorsement, but this judgment could be legally and factually problematic. See supra text accompanying notes 162-64; Rebecca Bornstein, Enforcement Scenario: Iran, in ELEMENTS OF A NUCLEAR DISARMAMENT TREATY, supra note 3, at 160-62.
a. Exercise the Treaty’s provisions for consultations and dispute resolution; 368
b. Use the good offices of the Secretariat to facilitate a resolution; 369
c. Bring the matter to the attention of the Executive Council and the Assembly, which may impose sanctions under the Treaty; 370
d. Bring the matter to the attention of the United Nations Security Council, the United Nations General Assembly, or the International Court of Justice; 371 and
e. Terminate or suspend, in whole or in part, its performance of its obligations under this Treaty, in proportional response to the violation. 372

368. See, e.g., CWC, supra note 139, arts. IX, XIV; CTBT, supra note 129, arts. IV.C, V, VI.
369. See, e.g., CWC, supra note 139, art. IX.3; CTBT, supra note 129, art. IV.31, V.2.
370. See, e.g., CTBT, supra note 129, art. IV.32. This draft contemplates that the Organization itself, as well as individual parties acting on their own, could reach an official judgment about whether a party had violated the treaty, and the Executive Council or Assembly could respond to the breach with collective sanctions or other penalties. Alternatively, the treaty could reserve those powers exclusively for the individual states.
371. See, e.g., CTBT, supra note 129, art. VI.2, VI.4; CWC, supra note 139, arts. XII, XIV.
372. The idea here is that if Country X perceives that Country Y is violating the obligation not to re-assemble or otherwise possess a nuclear weapon, then Country X may likewise disregard the constraint—without obtaining any consensus or approval from the Treaty bodies or the UN Security Council. This “self-help” mechanism may be an appropriate and necessary component of the enforcement regime, pursuant to traditional international law standards regarding an innocent party’s response to another party’s material breach, VCLT, supra note 138, art. 60. But it does pose additional problems here: (a) It is in some tension with the bold commitment in Article I “never, under any circumstances” to possess a nuclear weapon; (b) It is a remedy that would not be equally available to all parties—the former NWS would be in a much better position to reconstitute their former nuclear weapons—so this avenue perpetuates some of the discriminatory character of the NPT; and (c) It retains in the Zero Treaty a measure of the current practice of nuclear deterrence, perhaps in an even more precarious form. See supra text accompanying notes 165-67.

An additional quandary is whether Country X would have to publicly and immediately declare its termination or suspension. That is, in some circumstances it might be advantageous to conceal the fact that X has detected Y’s violation and is moving to counteract it. But that approach would implicate X in its own secret breach of the Zero Treaty.

This draft of the Zero Treaty contains two “escape hatches” from the obligation not to possess nuclear weapons: this provision for suspension or termination in the case of another party’s breach, and the later provision in art. XI.7 for withdrawal due to supreme national interests. See infra, text accompanying notes 384-86. The withdrawal option is even broader than the current article, because it contemplates a party’s ability to escape the Treaty for reasons unconnected to another party’s breach (such as the possession of a nuclear weapon by a non-state actor, or other
WHAT WOULD ZERO LOOK LIKE?

Article X
Security Relationships

1. The Parties shall develop and implement comprehensive, legally binding security assurances as safeguards against the threat or use of nuclear weapons. 373

2. The Parties shall develop procedures, institutions, and additional measures to assist in the resolution of regional security problems in a manner that promotes the legitimate security interests of all participants, without recourse to the possession, threat or use of nuclear weapons. 374

3. The Parties shall cooperate and provide assistance in the development of defenses against nuclear weapons. 375

4. The Parties shall develop procedures, institutions, and additional measures to reduce conventional weaponry and military budgets. 376

---

conditions that might be thought to jeopardize the party’s supreme security interests.) But the withdrawal clause requires ninety days advance notice before the action is effective.

373. The traditional topic of “security assurances”—both “negative” and “positive”—may play a useful role in creating the conditions for nuclear disarmament. These assurances will have less salience in a world free of nuclear weapons, but may have some continuing relevance. See supra, text accompanying notes 265. Cf. BWC, supra note 194, art. VII (parties undertake to assist a party endangered by another state’s violation of the treaty); CWC, supra note 139, art. X (establishing provisions for assistance and protection against chemical weapons); John Freeman, The Experience of the Chemical Weapons Convention: Lessons for the Elimination of Nuclear Weapons, in ELEMENTS OF A NUCLEAR DISARMAMENT TREATY, supra note 3, at 125-26; Rebecca Bornstein, Enforcement Scenario: Iran, in ELEMENTS OF A NUCLEAR DISARMAMENT TREATY, supra note 3, at 155; Frank Blackaby, Introduction and Summary, in NUCLEAR WEAPONS: THE ROAD TO ZERO, supra note 14, at 10-11 (arguing that the NWS “speak with forked tongues” when they offer non-legally-binding security assurances). The new security assurances might be included in the Zero Treaty; alternatively, they might be concluded before or after it enters into force.

374. Construction of a world free of nuclear weapons does not require the complete “resolution” of intractable regional problems, but it does require the various protagonists to agree that possession or pursuit of nuclear weapons would be unnecessary (indeed, harmful) to advancement of their respective legitimate national security goals. See supra, text accompanying notes 187-88.

375. The question of defenses against nuclear weapons (including missile defense, air defense, and civil defense) will have to be addressed long before the Zero Treaty is concluded, but some provision dealing with those topics may be in order. New START acknowledges that the relationship between offenses and defenses becomes even more important as offenses are reduced. New START, supra note 78, pmbl ¶ 8. See supra text accompanying note 190.

376. As nuclear weapons are eliminated, the question of conventional forces will rise to even greater prominence. See supra text accompanying notes 187-89.
5. The Parties shall cooperate and provide assistance, as necessary, to improve the safety and security of any retained nuclear weapons components.  

6. Each Party shall cooperate in, facilitate, provide assistance in, and have the right to participate in, the fullest possible exchange of equipment, material, and scientific and technological information concerning the development of nuclear energy for peaceful purposes. The Parties shall not maintain any restrictions incompatible with the obligations undertaken in this Treaty that would restrict or impede trade and the development and promotion of scientific and technological knowledge concerning the development of nuclear energy for peaceful purposes. Each Party shall review its existing national regulations in the field of trade to ensure that they are consistent with the object and purpose of the Treaty.

Article XI

Final Provisions

1. This Treaty shall be open for signature by all states indefinitely.

2. This Treaty shall be subject to ratification by signatory states according to their respective constitutional processes.

3. This Treaty shall enter into force 180 days after the deposit of instruments of ratification by all states possessing nuclear weapons and fifty other states. For any state depositing an
WHAT WOULD ZERO LOOK LIKE?

instrument of ratification thereafter, the Treaty shall enter into force thirty days after the deposit.

4. This Treaty shall not be subject to reservations.384

5. This Treaty shall be of unlimited duration.385

6. This Treaty shall be subject to amendments and changes as follows:386

a. Any Party may propose an amendment, which shall be submitted to the Secretariat for prompt circulation to all Parties. If one-third or more of the Parties notify the Secretariat within sixty days after its circulation that they support further consideration of the proposal, it shall be considered at an Amendment Conference. The Amendment Conference shall be held immediately following a regular session of the Assembly. If the proposed amendment is adopted at the Amendment Conference by a majority vote of all Parties, with no Party casting a negative vote, the amendment shall enter into force for all Parties ninety days after the deposit of instruments of ratification by a majority of all Parties.

b. A change may be related only to technical, administrative or procedural matters. Any Party may propose a change, which shall be submitted to the Secretariat for prompt circulation to all Parties. The Executive Council shall evalu-
ate the proposed change and make a recommendation, which shall be circulated to all Parties within ninety days. If the Executive Council recommends that the proposed change be adopted, it shall be considered adopted if no Party objects within ninety days. If the Executive Council recommends that the proposed change be rejected, it shall be considered rejected if no Party objects within ninety days. If any Party objects to the recommendation of the Executive Council, the proposed change shall be considered as a matter of substance by the Assembly at its next session. Any adopted change shall enter into force for all Parties 180 days after adoption.

7. Each Party shall, in exercising its national sovereignty, have the right to withdraw from this Treaty if it decides that extraordinary events related to the subject matter of the Treaty have jeopardized its supreme interests.\textsuperscript{384} It shall give ninety days' advance notice\textsuperscript{385} of such withdrawal, including a statement of the extraordinary events it regards as having jeopardized its supreme interests.\textsuperscript{386}

8. Nothing in this Treaty shall be interpreted as in any way limiting or deterring from the obligations of the Parties under other international law. A Party's withdrawal from this Treaty shall not in any way affect its obligations under other

---

\textsuperscript{384} This is the standard "supreme interests withdrawal" clause, common to arms control treaties. It provides an "escape hatch" from the obligations, making it safer for states to enter the agreement in the first place. See CWC, supra note 139, art. XVI; CTBT, supra note 129, art. IX; New START, supra note 78, art. XIV.3. Withdrawal from an arms control treaty has been rare, with only the 2002 U.S. withdrawal from the ABM Treaty and the 2003 North Korean withdrawal from the NPT as precedents. Christer Ahlström, \textit{Withdrawal from Arms Control Treaties}, in \textbf{STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE 2004 YEARBOOK}, available at \url{http://www.sipri.org/yearbook/2004/files/SIPRIYBO419.pdf}.

\textsuperscript{385} Alternatively, the time period specified for withdrawal could be shorter or longer. See CTBT, supra note 129, art. IX.3 (six months' notice); CWC, supra note 139, art. XVI.2 (ninety days' notice). A longer notification period provides other parties additional time to react to the impending withdrawal, but in the case of nuclear disarmament, parties may feel the need for an ability to respond very quickly to the most severe challenges.

\textsuperscript{386} Alternatively, the Zero Treaty could depart from precedent and prohibit withdrawal (except, perhaps, in the case of material breach of the treaty by another party). Cf. NWC, supra note 2, at 96 (citing article XVIII(5), prohibiting withdrawal); Perkovich and Acton, supra note 8, at 95-97.
international law, including other arms control or disarmament treaties.\footnote{Cf. CWC, supra note 139, art. XVI.3 (specifying that withdrawal from the CWC would not affect a party’s status under the 1925 Geneva Protocol).}

9. The Protocol is an integral part of this Treaty. Any references to the Treaty include the Protocol.\footnote{Cf. CTBT, supra note 129, art. X; CWC, supra note 139, art. XVII.}

10. Five years after the entry into force of this Treaty, and at five year intervals thereafter, the Parties shall assemble in a Review Conference to assess the operation and effectiveness of the Treaty, with a view to ensuring that the object and purpose of the Treaty are being realized.\footnote{See, e.g., CTBT, supra note 129, art. VIII (providing for review conferences every ten years); CWC, supra note 139, art. VIII.22 (providing for review conferences at five-year intervals).}

11. The Secretary-General of the United Nations is hereby designated as the Depositary of this Treaty, and shall perform all appropriate duties, including registering this Treaty pursuant to Article 102 of the Charter of the United Nations.\footnote{Cf. CTBT, supra note 129, art. XVI.1; CWC, supra note 139, art. XXIII.}

12. The Arabic, Chinese, English, French, Russian and Spanish texts of this Treaty are equally authentic.\footnote{Cf. CTBT, supra note 129, art. XVII; CWC, supra note 139, art. XXIV.}

In Witness Whereof, the undersigned, being duly authorized to that effect, have signed this Treaty.

Done at (place) on (date).\footnote{The Zero Treaty would probably be accompanied by an agreement to apply provisionally some of the key provisions of the Treaty and to establish a Preparatory Commission that would help pave the way for entry into force. See Resolution Establishing CTBT Preparatory Commission, supra note 185; Paris Resolution, supra note 185; New START, supra note 78, Protocol, Part VIII.}

VI. CONCLUSION

What are the prospects for this nuclear disarmament enterprise? Is the world now ready—after decades of contemplation—to initiate, and to pursue with the necessary vigor, the vision of abolishing all nuclear weapons?

It is hard to be optimistic about escaping the nearly seventy-year addiction to nuclear strategy, armaments and institutions. Even with the zealous advocacy from today’s Gang of Four—echoing the judgments and sentiments from Baruch, Reagan, Gorbachev, and Gandhi—it is still difficult to summon the global commitment to ascend that mist-covered mountain. The concept of nuclear arms control—reducing...
and limiting the mass destruction inventories of the United States, Russia, and others—is difficult enough, but it at least remains a credible “action item” on the contemporary political agenda; the concept of true nuclear disarmament, on the other hand, may seem almost as remote as ever.

Still, the goal of getting to zero remains persistent. It has been endorsed by world leaders and the general public; it has been adopted by the United Nations Security Council and General Assembly; and it stands as a binding legal obligation under the essential Nuclear Non-Proliferation Treaty. Perhaps its time is finally coming.

As the draft Zero Agreement and Zero Treaty indicate, there are a great many moving parts in this proposal, and several of them strain credulity. To conceptualize a world free of nuclear weapons, we have to presume a global readiness to effectuate the Comprehensive Nuclear Test Ban Treaty, a Fissile Material Cutoff Treaty, and sequential deep cuts in nuclear arsenals by the nine states currently possessing them; we need a resolution or at least mitigation of seemingly perpetual regional tensions in the Middle East, South Asia and elsewhere; and we have to assume that revolutionary new technologies for air-tight verification and enforcement of compliance can be crafted and accepted by mutually suspicious sovereigns. That’s asking a lot of the public imagination.

On the other hand, the risks of sustaining the nuclearized status quo beggar belief, too. It cannot realistically be argued that a heavily-armed—and perhaps increasingly proliferating—world can perpetually dodge the specter of the use of nuclear weapons, by hostile forces or terrorists, by design, accident, or horrific miscalculation. No one can imagine that the world’s current course will continue to escape forever a cataclysm beyond history.

Alice in Wonderland’s White Queen, who claimed to be able to believe six impossible things before breakfast, would therefore enjoy a rich smorgasbord of competing non-credible choices here: both the option of an unprecedented exploration up the mountain and the option of nervously remaining at our current base camp seem implausibly hazardous and unsustainable.

The hardest part of nuclear disarmament, of course, is dealing with the potential for cheating. What can we do to deter, detect and defeat the potential bad actors, who might well perceive a powerful incentive for secretly violating the disarmament norm in pursuit of an awesome one-sided advantage? Where the stakes are so high—where the world is proceeding well beyond the relatively modest accomplishments of New START and a plethora of other incremental measures—the
WHAT WOULD ZERO LOOK LIKE?

standards for acceptable confidence in verification and enforcement must rise, too. Louis Henkin’s famous aphorism about states’ pattern of compliance with international law—“almost all nations observe almost all principles of international law and almost all of their obligations almost all of the time”393—may be comforting in many applications and environments, but it would be a woefully inadequate measure of success in the realm of nuclear weapons abolition.

In the effort to illuminate a path toward greater confidence in compliance, legal draftsmanship may be of assistance. The enterprise here to craft a pair of prototype instruments—the short-term, non-legally-binding Zero Agreement and the eventual legally-binding Zero Treaty—can highlight, if not conclude or finesse, a variety of confounding questions. Resolution of these “in the weeds” details will require additional engagement of diplomatic, political, military, and technical expertise, but the drafting exercise can contribute by raising the visibility of the outstanding puzzles. Sometimes, it’s helpful just to imagine what the ultimate goal might actually look like.

PANEL X:

THE MODEL RULES IN THE NATIONAL SECURITY CONTEXT

DISCUSSANTS:
JUDGE JAMES E. BAKER
HARVEY RISHIKOF
ABA MODEL RULES OF PROFESSIONAL CONDUCT

Client-Lawyer Relationship

RULE 1.1: COMPETENCE

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Comment

Legal Knowledge and Skill

[1] In determining whether a lawyer employs the requisite knowledge and skill in a particular matter, relevant factors include the relative complexity and specialized nature of the matter, the lawyer's general experience, the lawyer's training and experience in the field in question, the preparation and study the lawyer is able to give the matter and whether it is feasible to refer the matter to, or associate or consult with, a lawyer of established competence in the field in question. In many instances, the required proficiency is that of a general practitioner. Expertise in a particular field of law may be required in some circumstances.

[2] A lawyer need not necessarily have special training or prior experience to handle legal problems of a type with which the lawyer is unfamiliar. A newly admitted lawyer can be as competent as a practitioner with long experience. Some important legal skills, such as the analysis of precedent, the evaluation of evidence and legal drafting, are required in all legal problems. Perhaps the most fundamental legal skill consists of determining what kind of legal problems a situation may involve, a skill that necessarily transcends any particular specialized knowledge. A lawyer can provide adequate representation in a wholly novel field through necessary study. Competent representation can also be provided through the association of a lawyer of established competence in the field in question.

[3] In an emergency a lawyer may give advice or assistance in a matter in which the lawyer does not have the skill ordinarily required where referral to or consultation or association with another lawyer would be impractical. Even in an emergency, however, assistance should be limited to that reasonably necessary in the circumstances, for ill-considered action under emergency conditions can jeopardize the client's interest.

[4] A lawyer may accept representation where the requisite level of competence can be achieved by reasonable preparation. This applies as well to a lawyer who is appointed as counsel for an unrepresented person. See also Rule 6.2.

Thoroughness and Preparation

[5] Competent handling of a particular matter includes inquiry into and analysis of the factual and legal elements of the problem, and use of methods and procedures meeting the standards of competent practitioners. It also includes adequate preparation. The required attention and preparation are determined in part by what is at stake; major litigation and complex transactions ordinarily require more extensive treatment than matters of lesser complexity and consequence. An agreement between the lawyer and the client regarding the scope of the representation may limit the matters for which the lawyer is responsible. See Rule 1.2(c).
Retaining or Contracting With Other Lawyers

[6] Before a lawyer retains or contracts with other lawyers outside the lawyer’s own firm to provide or assist in the provision of legal services to a client, the lawyer should ordinarily obtain informed consent from the client and must reasonably believe that the other lawyers’ services will contribute to the competent and ethical representation of the client. See also Rules 1.2 (allocation of authority), 1.4 (communication with client), 1.5(e) (fee sharing), 1.6 (confidentiality), and 5.5(a) (unauthorized practice of law). The reasonableness of the decision to retain or contract with other lawyers outside the lawyer’s own firm will depend upon the circumstances, including the education, experience and reputation of the nonfirm lawyers; the nature of the services assigned to the nonfirm lawyers; and the legal protections, professional conduct rules, and ethical environments of the jurisdictions in which the services will be performed, particularly relating to confidential information.

[7] When lawyers from more than one law firm are providing legal services to the client on a particular matter, the lawyers ordinarily should consult with each other and the client about the scope of their respective representations and the allocation of responsibility among them. See Rule 1.2. When making allocations of responsibility in a matter pending before a tribunal, lawyers and parties may have additional obligations that are a matter of law beyond the scope of these Rules.

Maintaining Competence

[8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

Definitional Cross-References
“Reasonably” See Rule 1.0(h)
RULE 1.2: SCOPE OF REPRESENTATION AND ALLOCATION OF AUTHORITY BETWEEN CLIENT AND LAWYER

(a) Subject to paragraphs (c) and (d), a lawyer shall abide by a client's decisions concerning the objectives of representation and, as required by Rule 1.4, shall consult with the client as to the means by which they are to be pursued. A lawyer may take such action on behalf of the client as is impliedly authorized to carry out the representation. A lawyer shall abide by a client's decision whether to settle a matter. In a criminal case, the lawyer shall abide by the client's decision, after consultation with the lawyer, as to a plea to be entered, whether to waive jury trial and whether the client will testify.

(b) A lawyer's representation of a client, including representation by appointment, does not constitute an endorsement of the client's political, economic, social or moral views or activities.

(c) A lawyer may limit the scope of the representation if the limitation is reasonable under the circumstances and the client gives informed consent.

(d) A lawyer shall not counsel a client to engage, or assist a client, in conduct that the lawyer knows is criminal or fraudulent, but a lawyer may discuss the legal consequences of any proposed course of conduct with a client and may counsel or assist a client to make a good faith effort to determine the validity, scope, meaning or application of the law.

Comment

Allocation of Authority between Client and Lawyer

[1] Paragraph (a) confers upon the client the ultimate authority to determine the purposes to be served by legal representation, within the limits imposed by law and the lawyer's professional obligations. The decisions specified in paragraph (a), such as whether to settle a civil matter, must also be made by the client. See Rule 1.4(a)(1) for the lawyer's duty to communicate with the client about such decisions. With respect to the means by which the client's objectives are to be pursued, the lawyer shall consult with the client as required by Rule 1.4(a)(2) and may take such action as is impliedly authorized to carry out the representation.

[2] On occasion, however, a lawyer and a client may disagree about the means to be used to accomplish the client's objectives. Clients normally defer to the special knowledge and skill of their lawyer with respect to the means to be used to accomplish their objectives, particularly with respect to technical, legal and tactical matters. Conversely, lawyers usually defer to the client regarding such questions as the expense to be incurred and concern for third persons who might be adversely affected. Because of the varied nature of the matters about which a lawyer and client might disagree and because the actions in question may implicate the interests of a tribunal or other persons, this Rule does not prescribe how such disagreements are to be resolved. Other law, however, may be applicable and should be consulted by the lawyer. The lawyer should also consult with the client and seek a mutually acceptable resolution of the disagreement. If such efforts are unavailing and the lawyer has a fundamental disagreement with the client, the lawyer may withdraw from the representation. See Rule 1.16(b)(4). Conversely, the client may resolve the disagreement by discharging the lawyer. See Rule 1.16(a)(3).

[3] At the outset of a representation, the client may authorize the lawyer to take specific action on the client's behalf without further consultation. Absent a material change in
circumstances and subject to Rule 1.4, a lawyer may rely on such an advance authorization. The client may, however, revoke such authority at any time.

[4] In a case in which the client appears to be suffering diminished capacity, the lawyer's duty to abide by the client's decisions is to be guided by reference to Rule 1.14.

Independence from Client's Views or Activities

[5] Legal representation should not be denied to people who are unable to afford legal services, or whose cause is controversial or the subject of popular disapproval. By the same token, representing a client does not constitute approval of the client's views or activities.

Agreements Limiting Scope of Representation

[6] The scope of services to be provided by a lawyer may be limited by agreement with the client or by the terms under which the lawyer's services are made available to the client. When a lawyer has been retained by an insurer to represent an insured, for example, the representation may be limited to matters related to the insurance coverage. A limited representation may be appropriate because the client has limited objectives for the representation. In addition, the terms upon which representation is undertaken may exclude specific means that might otherwise be used to accomplish the client's objectives. Such limitations may exclude actions that the client thinks are too costly or that the lawyer regards as repugnant or imprudent.

[7] Although this Rule affords the lawyer and client substantial latitude to limit the representation, the limitation must be reasonable under the circumstances. If, for example, a client's objective is limited to securing general information about the law the client needs in order to handle a common and typically uncomplicated legal problem, the lawyer and client may agree that the lawyer's services will be limited to a brief telephone consultation. Such a limitation, however, would not be reasonable if the time allotted was not sufficient to yield advice upon which the client could rely. Although an agreement for a limited representation does not exempt a lawyer from the duty to provide competent representation, the limitation is a factor to be considered when determining the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation. See Rule 1.1.


Criminal, Fraudulent and Prohibited Transactions

[9] Paragraph (d) prohibits a lawyer from knowingly counseling or assisting a client to commit a crime or fraud. This prohibition, however, does not preclude the lawyer from giving an honest opinion about the actual consequences that appear likely to result from a client's conduct. Nor does the fact that a client uses advice in a course of action that is criminal or fraudulent of itself make a lawyer a party to the course of action. There is a critical distinction between presenting an analysis of legal aspects of questionable conduct and recommending the means by which a crime or fraud might be committed with impunity.

[10] When the client's course of action has already begun and is continuing, the lawyer's responsibility is especially delicate. The lawyer is required to avoid assisting the client, for example, by drafting or delivering documents that the lawyer knows are fraudulent or by suggesting how the wrongdoing might be concealed. A lawyer may not continue assisting a client in conduct that the lawyer originally supposed was legally proper but then discovers is criminal or fraudulent. The lawyer must, therefore, withdraw from the representation of the client in the matter. See Rule 1.16(a). In some cases, withdrawal alone might be insufficient. It may be necessary for the lawyer to give notice of the fact of withdrawal and to disaffirm any opinion,
[11] Where the client is a fiduciary, the lawyer may be charged with special obligations in dealings with a beneficiary.

[12] Paragraph (d) applies whether or not the defrauded party is a party to the transaction. Hence, a lawyer must not participate in a transaction to effectuate criminal or fraudulent avoidance of tax liability. Paragraph (d) does not preclude undertaking a criminal defense incident to a general retainer for legal services to a lawful enterprise. The last clause of paragraph (d) recognizes that determining the validity or interpretation of a statute or regulation may require a course of action involving disobedience of the statute or regulation or of the interpretation placed upon it by governmental authorities.

[13] If a lawyer comes to know or reasonably should know that a client expects assistance not permitted by the Rules of Professional Conduct or other law or if the lawyer intends to act contrary to the client's instructions, the lawyer must consult with the client regarding the limitations on the lawyer's conduct. See Rule 1.4(a)(5).

**Definitional Cross-References**

“Fraudulent” See Rule 1.0(d)
“Informed consent” See Rule 1.0(e)
“Knows” See Rule 1.0(f)
“Reasonable” See Rule 1.0(h)

**RULE 1.3: DILIGENCE**

A lawyer shall act with reasonable diligence and promptness in representing a client.

**Comment**

[1] A lawyer should pursue a matter on behalf of a client despite opposition, obstruction or personal inconvenience to the lawyer, and take whatever lawful and ethical measures are required to vindicate a client's cause or endeavor. A lawyer must also act with commitment and dedication to the interests of the client and with zeal in advocacy upon the client's behalf. A lawyer is not bound, however, to press for every advantage that might be realized for a client. For example, a lawyer may have authority to exercise professional discretion in determining the means by which a matter should be pursued. See Rule 1.2. The lawyer's duty to act with reasonable diligence does not require the use of offensive tactics or preclude the treating of all persons involved in the legal process with courtesy and respect.

[2] A lawyer's work load must be controlled so that each matter can be handled competently.

[3] Perhaps no professional shortcoming is more widely resented than procrastination. A client's interests often can be adversely affected by the passage of time or the change of conditions; in extreme instances, as when a lawyer overlooks a statute of limitations, the client's legal position may be destroyed. Even when the client's interests are not affected in substance, however, unreasonable delay can cause a client needless anxiety and undermine confidence in the lawyer's trustworthiness. A lawyer's duty to act with reasonable promptness, however, does not preclude the lawyer from agreeing to a reasonable request for a postponement that will not prejudice the lawyer's client.

[4] Unless the relationship is terminated as provided in Rule 1.16, a lawyer should carry through to conclusion all matters undertaken for a client. If a lawyer's employment is
limited to a specific matter, the relationship terminates when the matter has been resolved. If a lawyer has served a client over a substantial period in a variety of matters, the client sometimes may assume that the lawyer will continue to serve on a continuing basis unless the lawyer gives notice of withdrawal. Doubt about whether a client-lawyer relationship still exists should be clarified by the lawyer, preferably in writing, so that the client will not mistakenly suppose the lawyer is looking after the client's affairs when the lawyer has ceased to do so. For example, if a lawyer has handled a judicial or administrative proceeding that produced a result adverse to the client and the lawyer and the client have not agreed that the lawyer will handle the matter on appeal, the lawyer must consult with the client about the possibility of appeal before relinquishing responsibility for the matter. See Rule 1.4(a)(2). Whether the lawyer is obligated to prosecute the appeal for the client depends on the scope of the representation the lawyer has agreed to provide to the client. See Rule 1.2.

[5] To prevent neglect of client matters in the event of a sole practitioner's death or disability, the duty of diligence may require that each sole practitioner prepare a plan, in conformity with applicable rules, that designates another competent lawyer to review client files, notify each client of the lawyer's death or disability, and determine whether there is a need for immediate protective action. Cf. Rule 28 of the American Bar Association Model Rules for Lawyer Disciplinary Enforcement (providing for court appointment of a lawyer to inventory files and take other protective action in absence of a plan providing for another lawyer to protect the interests of the clients of a deceased or disabled lawyer).

**Definitional Cross-References**

“Reasonable” See Rule 1.0(h)
RULE 1.4: COMMUNICATION

(a) A lawyer shall:

(1) promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(e), is required by these Rules;

(2) reasonably consult with the client about the means by which the client's objectives are to be accomplished;

(3) keep the client reasonably informed about the status of the matter;

(4) promptly comply with reasonable requests for information; and

(5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law.

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

Comment

[1] Reasonable communication between the lawyer and the client is necessary for the client effectively to participate in the representation.

Communicating with Client

[2] If these Rules require that a particular decision about the representation be made by the client, paragraph (a)(1) requires that the lawyer promptly consult with and secure the client's consent prior to taking action unless prior discussions with the client have resolved what action the client wants the lawyer to take. For example, a lawyer who receives from opposing counsel an offer of settlement in a civil controversy or a proffered plea bargain in a criminal case must promptly inform the client of its substance unless the client has previously indicated that the proposal will be acceptable or unacceptable or has authorized the lawyer to accept or to reject the offer. See Rule 1.2(a).

[3] Paragraph (a)(2) requires the lawyer to reasonably consult with the client about the means to be used to accomplish the client's objectives. In some situations — depending on both the importance of the action under consideration and the feasibility of consulting with the client — this duty will require consultation prior to taking action. In other circumstances, such as during a trial when an immediate decision must be made, the exigency of the situation may require the lawyer to act without prior consultation. In such cases the lawyer must nonetheless act reasonably to inform the client of actions the lawyer has taken on the client's behalf. Additionally, paragraph (a)(3) requires that the lawyer keep the client reasonably informed about the status of the matter, such as significant developments affecting the timing or the substance of the representation.

[4] A lawyer's regular communication with clients will minimize the occasions on which a client will need to request information concerning the representation. When a client makes a reasonable request for information, however, paragraph (a)(4) requires prompt compliance with the request, or if a prompt response is not feasible, that the lawyer, or a member...
of the lawyer's staff, acknowledge receipt of the request and advise the client when a response may be expected. A lawyer should promptly respond to or acknowledge client communications.

Explaining Matters

[5] The client should have sufficient information to participate intelligently in decisions concerning the objectives of the representation and the means by which they are to be pursued, to the extent the client is willing and able to do so. Adequacy of communication depends in part on the kind of advice or assistance that is involved. For example, when there is time to explain a proposal made in a negotiation, the lawyer should review all important provisions with the client before proceeding to an agreement. In litigation a lawyer should explain the general strategy and prospects of success and ordinarily should consult the client on tactics that are likely to result in significant expense or to injure or coerce others. On the other hand, a lawyer ordinarily will not be expected to describe trial or negotiation strategy in detail. The guiding principle is that the lawyer should fulfill reasonable client expectations for information consistent with the duty to act in the client's best interests, and the client's overall requirements as to the character of representation. In certain circumstances, such as when a lawyer asks a client to consent to a representation affected by a conflict of interest, the client must give informed consent, as defined in Rule 1.0(e).

[6] Ordinarily, the information to be provided is that appropriate for a client who is a comprehending and responsible adult. However, fully informing the client according to this standard may be impracticable, for example, where the client is a child or suffers from diminished capacity. See Rule 1.14. When the client is an organization or group, it is often impossible or inappropriate to inform every one of its members about its legal affairs; ordinarily, the lawyer should address communications to the appropriate officials of the organization. See Rule 1.13. Where many routine matters are involved, a system of limited or occasional reporting may be arranged with the client.

Withholding Information

[7] In some circumstances, a lawyer may be justified in delaying transmission of information when the client would be likely to react imprudently to an immediate communication. Thus, a lawyer might withhold a psychiatric diagnosis of a client when the examining psychiatrist indicates that disclosure would harm the client. A lawyer may not withhold information to serve the lawyer's own interest or convenience or the interests or convenience of another person. Rules or court orders governing litigation may provide that information supplied to a lawyer may not be disclosed to the client. Rule 3.4(c) directs compliance with such rules or orders.

Definitional Cross-References

“Informed consent” See Rule 1.0(e)
“Knows” See Rule 1.0(f)
“Reasonably” See Rule 1.0(h)
RULE 1.6: CONFIDENTIALITY OF INFORMATION

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

(b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

(1) to prevent reasonably certain death or substantial bodily harm;

(2) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services;

(3) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;

(4) to secure legal advice about the lawyer's compliance with these Rules;

(5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client;

(6) to comply with other law or a court order; or

(7) to detect and resolve conflicts of interest arising from the lawyer’s change of employment or from changes in the composition or ownership of a firm, but only if the revealed information would not compromise the attorney-client privilege or otherwise prejudice the client.

(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

Comment

[1] This Rule governs the disclosure by a lawyer of information relating to the representation of a client during the lawyer's representation of the client. See Rule 1.18 for the lawyer's duties with respect to information provided to the lawyer by a prospective client, Rule 1.9(c)(2) for the lawyer's duty not to reveal information relating to the lawyer's prior representation of a former client and Rules 1.8(b) and 1.9(c)(1) for the lawyer's duties with respect to the use of such information to the disadvantage of clients and former clients.

[2] A fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information relating to the representation. See Rule 1.0(e) for the definition of informed consent. This contributes to the trust that is the hallmark of the client-lawyer relationship. The client is thereby encouraged to
seek legal assistance and to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter. The lawyer needs this information to represent the client effectively and, if necessary, to advise the client to refrain from wrongful conduct. Almost without exception, clients come to lawyers in order to determine their rights and what is, in the complex of laws and regulations, deemed to be legal and correct. Based upon experience, lawyers know that almost all clients follow the advice given, and the law is upheld.

[3] The principle of client-lawyer confidentiality is given effect by related bodies of law: the attorney-client privilege, the work product doctrine and the rule of confidentiality established in professional ethics. The attorney-client privilege and work product doctrine apply in judicial and other proceedings in which a lawyer may be called as a witness or otherwise required to produce evidence concerning a client. The rule of client-lawyer confidentiality applies in situations other than those where evidence is sought from the lawyer through compulsion of law. The confidentiality rule, for example, applies not only to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source. A lawyer may not disclose such information except as authorized or required by the Rules of Professional Conduct or other law. See also Scope.

[4] Paragraph (a) prohibits a lawyer from revealing information relating to the representation of a client. This prohibition also applies to disclosures by a lawyer that do not in themselves reveal protected information but could reasonably lead to the discovery of such information by a third person. A lawyer's use of a hypothetical to discuss issues relating to the representation is permissible so long as there is no reasonable likelihood that the listener will be able to ascertain the identity of the client or the situation involved.

**Authorized Disclosure**

[5] Except to the extent that the client's instructions or special circumstances limit that authority, a lawyer is impliedly authorized to make disclosures about a client when appropriate in carrying out the representation. In some situations, for example, a lawyer may be impliedly authorized to admit a fact that cannot properly be disputed or to make a disclosure that facilitates a satisfactory conclusion to a matter. Lawyers in a firm may, in the course of the firm's practice, disclose to each other information relating to a client of the firm, unless the client has instructed that particular information be confined to specified lawyers.

**Disclosure Adverse to Client**

[6] Although the public interest is usually best served by a strict rule requiring lawyers to preserve the confidentiality of information relating to the representation of their clients, the confidentiality rule is subject to limited exceptions. Paragraph (b)(1) recognizes the overriding value of life and physical integrity and permits disclosure reasonably necessary to prevent reasonably certain death or substantial bodily harm. Such harm is reasonably certain to occur if it will be suffered imminently or if there is a present and substantial threat that a person will suffer such harm at a later date if the lawyer fails to take action necessary to eliminate the threat. Thus, a lawyer who knows that a client has accidentally discharged toxic waste into a town's water supply may reveal this information to the authorities if there is a present and substantial risk that a person who drinks the water will contract a life-threatening or debilitating disease and the lawyer's disclosure is necessary to eliminate the threat or reduce the number of victims.

[7] Paragraph (b)(2) is a limited exception to the rule of confidentiality that permits the lawyer to reveal information to the extent necessary to enable affected persons or appropriate authorities to prevent the client from committing a crime or fraud, as defined in Rule 1.0(d), that is reasonably certain to result in substantial injury to the financial or property interests of another
and in furtherance of which the client has used or is using the lawyer’s services. Such a serious abuse of the client-lawyer relationship by the client forfeits the protection of this Rule. The client can, of course, prevent such disclosure by refraining from the wrongful conduct. Although paragraph (b)(2) does not require the lawyer to reveal the client’s misconduct, the lawyer may not counsel or assist the client in conduct the lawyer knows is criminal or fraudulent. See Rule 1.2(d). See also Rule 1.16 with respect to the lawyer’s obligation or right to withdraw from the representation of the client in such circumstances, and Rule 1.13(c), which permits the lawyer, where the client is an organization, to reveal information relating to the representation in limited circumstances.

[8] Paragraph (b)(3) addresses the situation in which the lawyer does not learn of the client’s crime or fraud until after it has been consummated. Although the client no longer has the option of preventing disclosure by refraining from the wrongful conduct, there will be situations in which the loss suffered by the affected person can be prevented, rectified or mitigated. In such situations, the lawyer may disclose information relating to the representation to the extent necessary to enable the affected persons to prevent or mitigate reasonably certain losses or to attempt to recoup their losses. Paragraph (b)(3) does not apply when a person who has committed a crime or fraud thereafter employs a lawyer for representation concerning that offense.

[9] A lawyer's confidentiality obligations do not preclude a lawyer from securing confidential legal advice about the lawyer's personal responsibility to comply with these Rules. In most situations, disclosing information to secure such advice will be impliedly authorized for the lawyer to carry out the representation. Even when the disclosure is not impliedly authorized, paragraph (b)(4) permits such disclosure because of the importance of a lawyer's compliance with the Rules of Professional Conduct.

[10] Where a legal claim or disciplinary charge alleges complicity of the lawyer in a client's conduct or other misconduct of the lawyer involving representation of the client, the lawyer may respond to the extent the lawyer reasonably believes necessary to establish a defense. The same is true with respect to a claim involving the conduct or representation of a former client. Such a charge can arise in a civil, criminal, disciplinary or other proceeding and can be based on a wrong allegedly committed by the lawyer against the client or on a wrong alleged by a third person, for example, a person claiming to have been defrauded by the lawyer and client acting together. The lawyer's right to respond arises when an assertion of such complicity has been made. Paragraph (b)(5) does not require the lawyer to await the commencement of an action or proceeding that charges such complicity, so that the defense may be established by responding directly to a third party who has made such an assertion. The right to defend also applies, of course, where a proceeding has been commenced.

[11] A lawyer entitled to a fee is permitted by paragraph (b)(5) to prove the services rendered in an action to collect it. This aspect of the rule expresses the principle that the beneficiary of a fiduciary relationship may not exploit it to the detriment of the fiduciary.

[12] Other law may require that a lawyer disclose information about a client. Whether such a law supersedes Rule 1.6 is a question of law beyond the scope of these Rules. When disclosure of information relating to the representation appears to be required by other law, the lawyer must discuss the matter with the client to the extent required by Rule 1.4. If, however, the other law supersedes this Rule and requires disclosure, paragraph (b)(6) permits the lawyer to make such disclosures as are necessary to comply with the law.

Detection of Conflicts of Interest

[13] Paragraph (b)(7) recognizes that lawyers in different firms may need to disclose limited information to each other to detect and resolve conflicts of interest, such as when a lawyer is considering an association with another firm, two or more firms are considering a
merger, or a lawyer is considering the purchase of a law practice. See Rule 1.17, Comment [7]. Under these circumstances, lawyers and law firms are permitted to disclose limited information, but only once substantive discussions regarding the new relationship have occurred. Any such disclosure should ordinarily include no more than the identity of the persons and entities involved in a matter, a brief summary of the general issues involved, and information about whether the matter has terminated. Even this limited information, however, should be disclosed only to the extent reasonably necessary to detect and resolve conflicts of interest that might arise from the possible new relationship. Moreover, the disclosure of any information is prohibited if it would compromise the attorney-client privilege or otherwise prejudice the client (e.g., the fact that a corporate client is seeking advice on a corporate takeover that has not been publicly announced; that a person has consulted a lawyer about the possibility of divorce before the person's intentions are known to the person's spouse; or that a person has consulted a lawyer about a criminal investigation that has not led to a public charge). Under those circumstances, paragraph (a) prohibits disclosure unless the client or former client gives informed consent. A lawyer’s fiduciary duty to the lawyer’s firm may also govern a lawyer’s conduct when exploring an association with another firm and is beyond the scope of these Rules.

[14] Any information disclosed pursuant to paragraph (b)(7) may be used or further disclosed only to the extent necessary to detect and resolve conflicts of interest. Paragraph (b)(7) does not restrict the use of information acquired by means independent of any disclosure pursuant to paragraph (b)(7). Paragraph (b)(7) also does not affect the disclosure of information within a law firm when the disclosure is otherwise authorized, see Comment [5], such as when a lawyer in a firm discloses information to another lawyer in the same firm to detect and resolve conflicts of interest that could arise in connection with undertaking a new representation.

[15] A lawyer may be ordered to reveal information relating to the representation of a client by a court or by another tribunal or governmental entity claiming authority pursuant to other law to compel the disclosure. Absent informed consent of the client to do otherwise, the lawyer should assert on behalf of the client all nonfrivolous claims that the order is not authorized by other law or that the information sought is protected against disclosure by the attorney-client privilege or other applicable law. In the event of an adverse ruling, the lawyer must consult with the client about the possibility of appeal to the extent required by Rule 1.4. Unless review is sought, however, paragraph (b)(6) permits the lawyer to comply with the court's order.

[16] Paragraph (b) permits disclosure only to the extent the lawyer reasonably believes the disclosure is necessary to accomplish one of the purposes specified. Where practicable, the lawyer should first seek to persuade the client to take suitable action to obviate the need for disclosure. In any case, a disclosure adverse to the client's interest should be no greater than the lawyer reasonably believes necessary to accomplish the purpose. If the disclosure will be made in connection with a judicial proceeding, the disclosure should be made in a manner that limits access to the information to the tribunal or other persons having a need to know it and appropriate protective orders or other arrangements should be sought by the lawyer to the fullest extent practicable.

[17] Paragraph (b) permits but does not require the disclosure of information relating to a client's representation to accomplish the purposes specified in paragraphs (b)(1) through (b)(6). In exercising the discretion conferred by this Rule, the lawyer may consider such factors as the nature of the lawyer's relationship with the client and with those who might be injured by the client, the lawyer's own involvement in the transaction and factors that may extenuate the conduct in question. A lawyer's decision not to disclose as permitted by paragraph (b) does not violate this Rule. Disclosure may be required, however, by other Rules. Some Rules require disclosure only if such disclosure would be permitted by paragraph (b). See Rules 1.2(d), 4.1(b), 8.1 and 8.3. Rule 3.3, on the other hand, requires disclosure in some circumstances regardless of whether such disclosure is permitted by this Rule. See Rule 3.3(c).
Acting Competently to Preserve Confidentiality

[18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer’s efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client’s information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer’s duties when sharing information with nonlawyers outside the lawyer’s own firm, see Rule 5.3, Comments [3]-[4].

[19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer’s expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

Former Client

[20] The duty of confidentiality continues after the client-lawyer relationship has terminated. See Rule 1.9(c)(2). See Rule 1.9(c)(1) for the prohibition against using such information to the disadvantage of the former client.

Definitional Cross-References
“Firm” See Rule 1.0(c)
“Fraud” See Rule 1.0(d)
“Informed consent” See Rule 1.0(e)
“Reasonably” See Rule 1.0(h)
“Reasonably believes” See Rule 1.0(i)
“Substantial” See Rule 1.0(l)
RULE 1.13: ORGANIZATION AS CLIENT

(a) A lawyer employed or retained by an organization represents the organization acting through its duly authorized constituents.

(b) If a lawyer for an organization knows that an officer, employee or other person associated with the organization is engaged in action, intends to act or refuses to act in a matter related to the representation that is a violation of a legal obligation to the organization, or a violation of law that reasonably might be imputed to the organization, and that is likely to result in substantial injury to the organization, then the lawyer shall proceed as is reasonably necessary in the best interest of the organization. Unless the lawyer reasonably believes that it is not necessary in the best interest of the organization to do so, the lawyer shall refer the matter to higher authority in the organization, including, if warranted by the circumstances, to the highest authority that can act on behalf of the organization as determined by applicable law.

(c) Except as provided in paragraph (d), if

(1) despite the lawyer's efforts in accordance with paragraph (b) the highest authority that can act on behalf of the organization insists upon or fails to address in a timely and appropriate manner an action or a refusal to act, that is clearly a violation of law; and

(2) the lawyer reasonably believes that the violation is reasonably certain to result in substantial injury to the organization,

then the lawyer may reveal information relating to the representation whether or not Rule 1.6 permits such disclosure, but only if and to the extent the lawyer reasonably believes necessary to prevent substantial injury to the organization.

(d) Paragraph (c) shall not apply with respect to information relating to a lawyer's representation of an organization to investigate an alleged violation of law, or to defend the organization or an officer, employee or other constituent associated with the organization against a claim arising out of an alleged violation of law.

(e) A lawyer who reasonably believes that he or she has been discharged because of the lawyer's actions taken pursuant to paragraphs (b) or (c), or who withdraws under circumstances that require or permit the lawyer to take action under either of those paragraphs, shall proceed as the lawyer reasonably believes necessary to assure that the organization's highest authority is informed of the lawyer's discharge or withdrawal.

(f) In dealing with an organization's directors, officers, employees, members, shareholders or other constituents, a lawyer shall explain the identity of the client when the lawyer knows or reasonably should know that the organization's interests are adverse to those of the constituents with whom the lawyer is dealing.

(g) A lawyer representing an organization may also represent any of its directors, officers, employees, members, shareholders or other constituents, subject to the provisions of Rule 1.7. If the organization's consent to the dual representation is required by Rule 1.7, the consent shall be given by an appropriate official of the organization other than the
individual who is to be represented, or by the shareholders.

Comment

The Entity as the Client

[1] An organizational client is a legal entity, but it cannot act except through its officers, directors, employees, shareholders and other constituents. Officers, directors, employees and shareholders are the constituents of the corporate organizational client. The duties defined in this Comment apply equally to unincorporated associations. "Other constituents" as used in this Comment means the positions equivalent to officers, directors, employees and shareholders held by persons acting for organizational clients that are not corporations.

[2] When one of the constituents of an organizational client communicates with the organization's lawyer in that person's organizational capacity, the communication is protected by Rule 1.6. Thus, by way of example, if an organizational client requests its lawyer to investigate allegations of wrongdoing, interviews made in the course of that investigation between the lawyer and the client's employees or other constituents are covered by Rule 1.6. This does not mean, however, that constituents of an organizational client are the clients of the lawyer. The lawyer may not disclose to such constituents information relating to the representation except for disclosures explicitly or impliedly authorized by the organizational client in order to carry out the representation or as otherwise permitted by Rule 1.6.

[3] When constituents of the organization make decisions for it, the decisions ordinarily must be accepted by the lawyer even if their utility or prudence is doubtful. Decisions concerning policy and operations, including ones entailing serious risk, are not as such in the lawyer's province. Paragraph (b) makes clear, however, that when the lawyer knows that the organization is likely to be substantially injured by action of an officer or other constituent that violates a legal obligation to the organization or is in violation of law that might be imputed to the organization, the lawyer must proceed as is reasonably necessary in the best interest of the organization. As defined in Rule 1.0(f), knowledge can be inferred from circumstances, and a lawyer cannot ignore the obvious.

[4] In determining how to proceed under paragraph (b), the lawyer should give due consideration to the seriousness of the violation and its consequences, the responsibility in the organization and the apparent motivation of the person involved, the policies of the organization concerning such matters, and any other relevant considerations. Ordinarily, referral to a higher authority would be necessary. In some circumstances, however, it may be appropriate for the lawyer to ask the constituent to reconsider the matter; for example, if the circumstances involve a constituent’s innocent misunderstanding of law and subsequent acceptance of the lawyer’s advice, the lawyer may reasonably conclude that the best interest of the organization does not require that the matter be referred to higher authority. If a constituent persists in conduct contrary to the lawyer’s advice, it will be necessary for the lawyer to take steps to have the matter reviewed by a higher authority in the organization. If the matter is of sufficient seriousness and importance or urgency to the organization, referral to higher authority in the organization may be necessary even if the lawyer has not communicated with the constituent. Any measures taken should, to the extent practicable, minimize the risk of revealing information relating to the representation to persons outside the organization. Even in circumstances where a lawyer is not obligated by Rule 1.13 to proceed, a lawyer may bring to the attention of an organizational client, including its highest authority, matters that the lawyer reasonably believes to be of sufficient importance to warrant doing so in the best interest of the organization.

[5] Paragraph (b) also makes clear that when it is reasonably necessary to enable the organization to address the matter in a timely and appropriate manner, the lawyer must refer the matter to higher authority, including, if warranted by the circumstances, the highest authority that
can act on behalf of the organization under applicable law. The organization's highest authority
to whom a matter may be referred ordinarily will be the board of directors or similar governing
body. However, applicable law may prescribe that under certain conditions the highest authority
reposes elsewhere, for example, in the independent directors of a corporation.

Relation to Other Rules

[6] The authority and responsibility provided in this Rule are concurrent with the
authority and responsibility provided in other Rules. In particular, this Rule does not limit or
expand the lawyer's responsibility under Rules 1.8, 1.16, 3.3 or 4.1. Paragraph (c) of this Rule
supplements Rule 1.6(b) by providing an additional basis upon which the lawyer may reveal
information relating to the representation, but does not modify, restrict, or limit the provisions of
Rule 1.6(b)(1) – (6). Under paragraph (c) the lawyer may reveal such information only when the
organization’s highest authority insists upon or fails to address threatened or ongoing action that
is clearly a violation of law, and then only to the extent the lawyer reasonably believes necessary
to prevent reasonably certain substantial injury to the organization. It is not necessary that the
lawyer’s services be used in furtherance of the violation, but it is required that the matter be
related to the lawyer’s representation of the organization. If the lawyer's services are being used
by an organization to further a crime or fraud by the organization, Rules 1.6(b)(2) and 1.6(b)(3)
may permit the lawyer to disclose confidential information. In such circumstances Rule 1.16(a)(3)
may also be applicable, in which event, withdrawal from the representation under Rule
1.16(a)(1) may be required.

[7] Paragraph (d) makes clear that the authority of a lawyer to disclose information
relating to a representation in circumstances described in paragraph (c) does not apply with
respect to information relating to a lawyer’s engagement by an organization to investigate an
alleged violation of law or to defend the organization or an officer, employee or other person
associated with the organization against a claim arising out of an alleged violation of law. This is
necessary in order to enable organizational clients to enjoy the full benefits of legal counsel in
cconducting an investigation or defending against a claim.

[8] A lawyer who reasonably believes that he or she has been discharged because of
the lawyer’s actions taken pursuant to paragraph (b) or (c), or who withdraws in circumstances
that require or permit the lawyer to take action under either of these paragraphs, must proceed as
the lawyer reasonably believes necessary to assure that the organization’s highest authority is
informed of the lawyer’s discharge or withdrawal.

Government Agency

[9] The duty defined in this Rule applies to governmental organizations. Defining
precisely the identity of the client and prescribing the resulting obligations of such lawyers may
be more difficult in the government context and is a matter beyond the scope of these Rules. See
Scope [18]. Although in some circumstances the client may be a specific agency, it may also be a
branch of government, such as the executive branch, or the government as a whole. For example,
if the action or failure to act involves the head of a bureau, either the department of which the
bureau is a part or the relevant branch of government may be the client for purposes of this Rule.
Moreover, in a matter involving the conduct of government officials, a government lawyer may
have authority under applicable law to question such conduct more extensively than that of a
lawyer for a private organization in similar circumstances. Thus, when the client is a
governmental organization, a different balance may be appropriate between maintaining
confidentiality and assuring that the wrongful act is prevented or rectified, for public business is
involved. In addition, duties of lawyers employed by the government or lawyers in military
service may be defined by statutes and regulation. This Rule does not limit that authority. See
Scope.

**Clarifying the Lawyer's Role**

[10] There are times when the organization's interest may be or become adverse to those of one or more of its constituents. In such circumstances the lawyer should advise any constituent, whose interest the lawyer finds adverse to that of the organization of the conflict or potential conflict of interest, that the lawyer cannot represent such constituent, and that such person may wish to obtain independent representation. Care must be taken to assure that the individual understands that, when there is such adversity of interest, the lawyer for the organization cannot provide legal representation for that constituent individual, and that discussions between the lawyer for the organization and the individual may not be privileged.

[11] Whether such a warning should be given by the lawyer for the organization to any constituent individual may turn on the facts of each case.

**Dual Representation**

[12] Paragraph (g) recognizes that a lawyer for an organization may also represent a principal officer or major shareholder.

**Derivative Actions**

[13] Under generally prevailing law, the shareholders or members of a corporation may bring suit to compel the directors to perform their legal obligations in the supervision of the organization. Members of unincorporated associations have essentially the same right. Such an action may be brought nominally by the organization, but usually is, in fact, a legal controversy over management of the organization.

[14] The question can arise whether counsel for the organization may defend such an action. The proposition that the organization is the lawyer's client does not alone resolve the issue. Most derivative actions are a normal incident of an organization's affairs, to be defended by the organization's lawyer like any other suit. However, if the claim involves serious charges of wrongdoing by those in control of the organization, a conflict may arise between the lawyer's duty to the organization and the lawyer's relationship with the board. In those circumstances, Rule 1.7 governs who should represent the directors and the organization.

**Definitional Cross-References**

“Knows” *See* Rule 1.0(f)
“Reasonably” *See* Rule 1.0(h)
“Reasonably believes” *See* Rule 1.0(i)
“Reasonably should know” *See* Rule 1.0(j)
“Substantial” *See* Rule 1.0(l)
RULE 3.3: CANDOR TOWARD THE TRIBUNAL

(a) A lawyer shall not knowingly:

(1) make a false statement of fact or law to a tribunal or fail to correct a false statement of material fact or law previously made to the tribunal by the lawyer;

(2) fail to disclose to the tribunal legal authority in the controlling jurisdiction known to the lawyer to be directly adverse to the position of the client and not disclosed by opposing counsel; or

(3) offer evidence that the lawyer knows to be false. If a lawyer, the lawyer’s client, or a witness called by the lawyer, has offered material evidence and the lawyer comes to know of its falsity, the lawyer shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal. A lawyer may refuse to offer evidence, other than the testimony of a defendant in a criminal matter, that the lawyer reasonably believes is false.

(b) A lawyer who represents a client in an adjudicative proceeding and who knows that a person intends to engage, is engaging or has engaged in criminal or fraudulent conduct related to the proceeding shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal.

(c) The duties stated in paragraphs (a) and (b) continue to the conclusion of the proceeding, and apply even if compliance requires disclosure of information otherwise protected by Rule 1.6.

(d) In an ex parte proceeding, a lawyer shall inform the tribunal of all material facts known to the lawyer that will enable the tribunal to make an informed decision, whether or not the facts are adverse.

Comment

[1] This Rule governs the conduct of a lawyer who is representing a client in the proceedings of a tribunal. See Rule 1.0(m) for the definition of "tribunal." It also applies when the lawyer is representing a client in an ancillary proceeding conducted pursuant to the tribunal’s adjudicative authority, such as a deposition. Thus, for example, paragraph (a)(3) requires a lawyer to take reasonable remedial measures if the lawyer comes to know that a client who is testifying in a deposition has offered evidence that is false.

[2] This Rule sets forth the special duties of lawyers as officers of the court to avoid conduct that undermines the integrity of the adjudicative process. A lawyer acting as an advocate in an adjudicative proceeding has an obligation to present the client's case with persuasive force. Performance of that duty while maintaining confidences of the client, however, is qualified by the advocate's duty of candor to the tribunal. Consequently, although a lawyer in an adversary proceeding is not required to present an impartial exposition of the law or to vouch for the evidence submitted in a cause, the lawyer must not allow the tribunal to be misled by false
statements of law or fact or evidence that the lawyer knows to be false.

**Representations by a Lawyer**

[3] An advocate is responsible for pleadings and other documents prepared for litigation, but is usually not required to have personal knowledge of matters asserted therein, for litigation documents ordinarily present assertions by the client, or by someone on the client's behalf, and not assertions by the lawyer. Compare Rule 3.1. However, an assertion purporting to be on the lawyer's own knowledge, as in an affidavit by the lawyer or in a statement in open court, may properly be made only when the lawyer knows the assertion is true or believes it to be true on the basis of a reasonably diligent inquiry. There are circumstances where failure to make a disclosure is the equivalent of an affirmative misrepresentation. The obligation prescribed in Rule 1.2(d) not to counsel a client to commit or assist the client in committing a fraud applies in litigation. Regarding compliance with Rule 1.2(d), see the Comment to that Rule. See also the Comment to Rule 8.4(b).

**Legal Argument**

[4] Legal argument based on a knowingly false representation of law constitutes dishonesty toward the tribunal. A lawyer is not required to make a disinterested exposition of the law, but must recognize the existence of pertinent legal authorities. Furthermore, as stated in paragraph (a)(2), an advocate has a duty to disclose directly adverse authority in the controlling jurisdiction that has not been disclosed by the opposing party. The underlying concept is that legal argument is a discussion seeking to determine the legal premises properly applicable to the case.

**Offering Evidence**

[5] Paragraph (a)(3) requires that the lawyer refuse to offer evidence that the lawyer knows to be false, regardless of the client’s wishes. This duty is premised on the lawyer’s obligation as an officer of the court to prevent the trier of fact from being misled by false evidence. A lawyer does not violate this Rule if the lawyer offers the evidence for the purpose of establishing its falsity.

[6] If a lawyer knows that the client intends to testify falsely or wants the lawyer to introduce false evidence, the lawyer should seek to persuade the client that the evidence should not be offered. If the persuasion is ineffective and the lawyer continues to represent the client, the lawyer must refuse to offer the false evidence. If only a portion of a witness's testimony will be false, the lawyer may call the witness to testify but may not elicit or otherwise permit the witness to present the testimony that the lawyer knows is false.

[7] The duties stated in paragraphs (a) and (b) apply to all lawyers, including defense counsel in criminal cases. In some jurisdictions, however, courts have required counsel to present the accused as a witness or to give a narrative statement if the accused so desires, even if counsel knows that the testimony or statement will be false. The obligation of the advocate under the Rules of Professional Conduct is subordinate to such requirements. See also Comment [9].

[8] The prohibition against offering false evidence only applies if the lawyer knows that the evidence is false. A lawyer’s reasonable belief that evidence is false does not preclude its presentation to the trier of fact. A lawyer’s knowledge that evidence is false, however, can be inferred from the circumstances. See Rule 1.0(f). Thus, although a lawyer should resolve doubts about the veracity of testimony or other evidence in favor of the client, the lawyer cannot ignore an obvious falsehood.

[9] Although paragraph (a)(3) only prohibits a lawyer from offering evidence the
lawyer knows to be false, it permits the lawyer to refuse to offer testimony or other proof that the lawyer reasonably believes is false. Offering such proof may reflect adversely on the lawyer's ability to discriminate in the quality of evidence and thus impair the lawyer's effectiveness as an advocate. Because of the special protections historically provided criminal defendants, however, this Rule does not permit a lawyer to refuse to offer the testimony of such a client where the lawyer reasonably believes but does not know that the testimony will be false. Unless the lawyer knows the testimony will be false, the lawyer must honor the client’s decision to testify. See also Comment [7].

Remedial Measures

[10] Having offered material evidence in the belief that it was true, a lawyer may subsequently come to know that the evidence is false. Or, a lawyer may be surprised when the lawyer’s client, or another witness called by the lawyer, offers testimony the lawyer knows to be false, either during the lawyer’s direct examination or in response to cross-examination by the opposing lawyer. In such situations or if the lawyer knows of the falsity of testimony elicited from the client during a deposition, the lawyer must take reasonable remedial measures. In such situations, the advocate’s proper course is to remonstrate with the client confidentially, advise the client of the lawyer’s duty of candor to the tribunal and seek the client’s cooperation with respect to the withdrawal or correction of the false statements or evidence. If that fails, the advocate must take further remedial action. If withdrawal from the representation is not permitted or will not undo the effect of the false evidence, the advocate must make such disclosure to the tribunal as is reasonably necessary to remedy the situation, even if doing so requires the lawyer to reveal information that otherwise would be protected by Rule 1.6. It is for the tribunal then to determine what should be done — making a statement about the matter to the trier of fact, ordering a mistrial or perhaps nothing.

[11] The disclosure of a client’s false testimony can result in grave consequences to the client, including not only a sense of betrayal but also loss of the case and perhaps a prosecution for perjury. But the alternative is that the lawyer cooperate in deceiving the court, thereby subverting the truth-finding process which the adversary system is designed to implement. See Rule 1.2(d). Furthermore, unless it is clearly understood that the lawyer will act upon the duty to disclose the existence of false evidence, the client can simply reject the lawyer's advice to reveal the false evidence and insist that the lawyer keep silent. Thus the client could in effect coerce the lawyer into being a party to fraud on the court.

Preserving Integrity of Adjudicative Process

[12] Lawyers have a special obligation to protect a tribunal against criminal or fraudulent conduct that undermines the integrity of the adjudicative process, such as bribing, intimidating or otherwise unlawfully communicating with a witness, juror, court official or other participant in the proceeding, unlawfully destroying or concealing documents or other evidence or failing to disclose information to the tribunal when required by law to do so. Thus, paragraph (b) requires a lawyer to take reasonable remedial measures, including disclosure if necessary, whenever the lawyer knows that a person, including the lawyer’s client, intends to engage, is engaging or has engaged in criminal or fraudulent conduct related to the proceeding.

Duration of Obligation

[13] A practical time limit on the obligation to rectify false evidence or false statements of law and fact has to be established. The conclusion of the proceeding is a reasonably definite point for the termination of the obligation. A proceeding has concluded within the meaning of
this Rule when a final judgment in the proceeding has been affirmed on appeal or the time for review has passed.

**Ex Parte Proceedings**

[14] Ordinarily, an advocate has the limited responsibility of presenting one side of the matters that a tribunal should consider in reaching a decision; the conflicting position is expected to be presented by the opposing party. However, in any ex parte proceeding, such as an application for a temporary restraining order, there is no balance of presentation by opposing advocates. The object of an ex parte proceeding is nevertheless to yield a substantially just result. The judge has an affirmative responsibility to accord the absent party just consideration. The lawyer for the represented party has the correlative duty to make disclosures of material facts known to the lawyer and that the lawyer reasonably believes are necessary to an informed decision.

**Withdrawal**

[15] Normally, a lawyer’s compliance with the duty of candor imposed by this Rule does not require that the lawyer withdraw from the representation of a client whose interests will be or have been adversely affected by the lawyer’s disclosure. The lawyer may, however, be required by Rule 1.16(a) to seek permission of the tribunal to withdraw if the lawyer’s compliance with this Rule’s duty of candor results in such an extreme deterioration of the client-lawyer relationship that the lawyer can no longer competently represent the client. Also see Rule 1.16(b) for the circumstances in which a lawyer will be permitted to seek a tribunal’s permission to withdraw. In connection with a request for permission to withdraw that is premised on a client’s misconduct, a lawyer may reveal information relating to the representation only to the extent reasonably necessary to comply with this Rule or as otherwise permitted by Rule 1.6.

**Definitional Cross-References**

“Fraudulent” See Rule 1.0(d)
“Knowingly” and “Known” and “Knows” See Rule 1.0(f)
“Reasonable” See Rule 1.0(h)
“Reasonably believes” See Rule 1.0(i)
“Tribunal” See Rule 1.0(m)
RUL 5.2: RESPONSIBILITIES OF A SUBORDINATE LAWYER

(a) A lawyer is bound by the Rules of Professional Conduct notwithstanding that the lawyer acted at the direction of another person.

(b) A subordinate lawyer does not violate the Rules of Professional Conduct if that lawyer acts in accordance with a supervisory lawyer's reasonable resolution of an arguable question of professional duty.

Comment

[1] Although a lawyer is not relieved of responsibility for a violation by the fact that the lawyer acted at the direction of a supervisor, that fact may be relevant in determining whether a lawyer had the knowledge required to render conduct a violation of the Rules. For example, if a subordinate filed a frivolous pleading at the direction of a supervisor, the subordinate would not be guilty of a professional violation unless the subordinate knew of the document's frivolous character.

[2] When lawyers in a supervisor-subordinate relationship encounter a matter involving professional judgment as to ethical duty, the supervisor may assume responsibility for making the judgment. Otherwise a consistent course of action or position could not be taken. If the question can reasonably be answered only one way, the duty of both lawyers is clear and they are equally responsible for fulfilling it. However, if the question is reasonably arguable, someone has to decide upon the course of action. That authority ordinarily reposes in the supervisor, and a subordinate may be guided accordingly. For example, if a question arises whether the interests of two clients conflict under Rule 1.7, the supervisor's reasonable resolution of the question should protect the subordinate professionally if the resolution is subsequently challenged.

Definitional Cross-References

“Reasonable” See Rule 1.0(h)
Leaders and Lawyers
Think more deeply about your role as an SJA and the Commander-Judge Advocate relationship as well as the role of the lawyer as a senior counselor and leader. Why care?

• The more effective the command-law partnership the better the result.

• If well-crafted and implemented:
  – The law provides authority to act.
  – The law provides for essential process.
  – The Law also provides essential Security as well as Legal values.

• Most security challenges today have a significant, if not controlling, substantive legal component, in addition to the ordinary legal questions that arise regarding operations, personnel, finances.

• Most Government challenges are leadership/personality challenges, then process, and only in the third instance legal. Counselor
We will start by listing some of the challenges of working with Commanders.

As well as working with lawyers.

We will then consider some of the solutions.

So we end up with ...
This!
What do you find most challenging about serving as a Judge Advocate?
(Some of) The Lawyer’s Challenges: My List

- Commanders who do not understand the law
- Judgment in the absence of experience
- Endurance
- Grade differentials
- Obnoxious personality (yours and the client’s)
- Role playing
- Clients who do not seek or follow advice
- Doing the right thing the right way
- Too little time
- Incomplete facts
- The Pressure to “Get to Yes”
- Confidence: Too much and too little
- Different Policy Views
- Work-Life “Balance”
- The substance of the law – Which area?
- The Challenge you didn’t expect
- Your job is to keep me out of trouble; get me to yes; and otherwise stay out of the way.
The Other Side of the Coin: What do Commanders find most challenging or Frustrating about working with lawyers?
(Some of the) Things Commanders May find frustrating about working with Lawyers: My List

- They take too long
- They talk too much
- They write too much
- They are too nervous
- They always say no
- They change their position
- They do not understand context
- They think they are the commander
- They don’t stay in their lane
- Unrealistic advice
- They are never available
- They always want to meet
- Too many caveats
- Finishing
- Lawyers as enablers
1. Understand What the Commander Needs as well as Wants

- Tell the Commander what he or she needs to know, not what you know.
- Solve the problem rather than answer the question.
- Distinguish between law, legal policy, and policy
- Objective analysis
- At the right time and in the right form
- Articulate the why and not just the whether
- Yes, No, and nuance
- Meet all deadlines that are real
- Finish – Take the Ball to the Hoop
2. Commanders and Lawyers Need to Understand the three Purposes Law Plays:

(A) The Law Provides Authority to Act in Response to Substantive Challenges as well as Defines the left and right boundaries of that Action

MJ Cases – MJ law and policy
Targeting/ROE -- The War Power
Tactical Intelligence/DOD Regulation -- Title 50 Authorities; FISA
Title 10 -- Article II
The Law [Can] Provide for Essential Process

Good Process = Better Results:

Get the Process You Demand or Tolerate

- Unity of Command
- Dissent and Mitigation
- Minimization of Mistake
- Fusion
- Accountability
- Importance of Role Playing
- Capacity to Cope
- Meaningful Application of the Law
- Minimizes Pathologies of Decision-Making
  - Secrecy
  - Speed
  - Cognitive Bias
  - NS Imperative

National Process – Interagency; Joint; Combined; PSI; MOTR
Remember Good Process is not one size fits all...

It is:

- Timely
- Contextual
- Meaningful

And:

- Engine
- Informal
- Visibility – External, Internal
- Consequence
- In-box
- Less sooner/more later
(C) The Law Provides Essential Security as well as Legal Values

Think Big
Teach/Guide
Why, not just What

This:

This is too late:
3. Understand the Role of the Lawyer and What He or She Brings to the Table

A. The Lawyer as Counselor & Teacher

Message: Help Decision-makers make conscious and purposeful choices aware of law, ethics, policy, context, and history that will stand the test of time.

“The hallmark of a successful national security lawyer is “to move forward with honor, under the law, and to approach the job from the perspective of always leaving the law and Constitution intact, with the nation well taken care of.” - Leon Fuerth

“The tendency is strong to emphasize transient results upon policies—such as wages or stabilization—and lose sight of enduring consequences upon the balanced power structure of our Republic.” Youngstown Sheet & Tube Co. et al. v. Sawyer, 343 U.S. 579, 634 (1952) (Jackson, J., concurring).

In representing a client, a lawyer shall exercise independent professional judgment and render candid advice. In rendering advice, a lawyer may refer not only to law but to other considerations such as moral, economic, social and political factors, that may be relevant to the client's situation. 2.1
“[M]ilitary lawyers were true combat multipliers in Iraq. They were not only invaluable in dealing with a host of operational law issues, they also made enormous contributions in helping resolve a host of issues that were more than a bit out of the normal legal lanes. In essence, we ‘threw’ lawyers at very difficult problems and they produced solutions in virtually every case—often under very challenging circumstances and in an uncertain security environment . . . . I tried to get all the lawyers we could get our hands on—and then sought more.”  - General David Petraeus
C. Critical Tools: Legal Tools and Playbooks

**Personality**
- Pile-driver
- Rope-a-doper
- Nervous Nelly
- Diplomat
- Good cop
- Bad cop

**Mechanisms**
- Constitution
- Statute
- Presidential Decision
- Presidential Order, Memo, Directive
- Presidential Statement
- Summary of Conclusions
- MOU/MOA
- Interagency Transfer
- Reserves
- Drawdowns

**Process Menu**
- POTUS
- Small Group
- Principals Committee
- Deputies Committee
- Interagency Working Group
- Biweekly
- Lunch, breakfast
- Hallway
- Rollout

**Substance**
- LOAC
- NIAC/IAC
- DPH
- Interrogation
- Detention
- Intelligence
- Criminal Law
- Cyber
- Ethics
And, 4.

Lawyers and Leadership – Skills and Traits

Compassion, Kindness, Teamwork, Humor
Humility, Grace, Control, Candor, Perspective

“HUMILITY IS NOT THINKING LESS OF YOURSELF, IT IS THINKING OF YOURSELF LESS.”

- C S LEWIS

Pocket Full of Liberty

www.pocketfullofliberty.com

© Chris Hasson/Supplied
Focus, Determination, Grit, Endurance
## Some Skills

### Specific Skills
- Mentorship
- Spontaneous/Public speaking
- Hiring
- Firing
- Promoting
- Rewarding and awarding
- Evaluating subordinates
- Counseling a subordinate who is also a friend
- Evaluating oneself
- Providing constructive feedback
- Teaching
- Guidance
- Press contacts and releases/media communications
- Investigations x 2
- Writing a memo
- Testimony
- In-brief
- Out-brief
- Getting time
- Knowing which modality to use and when
- Managing the in-box
- Managing email

### Know Hows
- Trust/delegation to subordinates
- Mission/life balance
- How deal with not knowing something
- When do you express/hold on to your own values
- Judgment
- Calm and patience
- Defining and holding to standards
- Subordinating ego
- Serving with or subject to an incompetent or unethical leader
- Being asked to do borderline tasks
- Dealing with a difficult subordinate
- When to stay within your lane and when not to
- Coping
- Making time for strategic thinking and vision
- Identifying/dealing with informational bias
- Interoffice friendships and romance
- Real and perceived sexual and racial bias
- Time constraints and knowing when enough is enough and when it is not
- When to speak up and when not to
Seven Final Observations

• Bridge the Gaps
  – Between cultures
  – Between HQ and the Field
• If it doesn’t work change it
• Appraise your work – substance, process, outcome
• Lean in
• Officers Eat Last
• The Allen Rule
• The DPM Rule
Moral Courage and Role Models
“The ideals we cherish, our fondest dreams and fervent hopes may not be realized in our lifetime. But that is beside the point. The knowledge that in your day you did your duty, and lived up to the expectations of your fellow men is in itself a rewarding experience and magnificent achievement.”
Nelson Mandela

Self-respect cannot be hunted. It cannot be purchased. It is never for sale. It cannot be fabricated out of public relations. It comes to us when we are alone, in quiet moments, in quiet places, when we suddenly realize that, knowing the good, we have done it; knowing the beautiful, we have served it; knowing the truth, we have spoken it.”
A. Whitney Griswold
Conclusion
Lawyers are Leaders