24TH ANNUAL REVIEW OF THE FIELD OF NATIONAL SECURITY LAW

CONFERENCE MATERIAL

DAY ONE

SPONSORED BY:

AMERICAN BAR ASSOCIATION
STANDING COMMITTEE ON LAW AND 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

NOVEMBER 6—NOVEMBER 7, 2014

CAPITAL HILTON HOTEL
1001 16TH STREET, NW
WASHINGTON, DC
## Conference Material: Day One

### Panel I

**Executive Branch Updates on Developments in National Security Law**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNI Reveals 2014 National Intelligence Strategy - Office of the Director of National Intelligence</td>
<td>1</td>
</tr>
<tr>
<td>Interim Progress Report on Implementing PPD-28 (Office of the Director of National Intelligence) - Robert Litt and Alexander W. Joel</td>
<td>7</td>
</tr>
<tr>
<td>U.S. National Security Prosecutors Shift Focus from Spies to Cyber - Aruna Viswanatha</td>
<td>15</td>
</tr>
<tr>
<td>Remarks by Assistant Attorney General John P. Carlin on Cybercrime (Carnegie Mellon University)</td>
<td>17</td>
</tr>
<tr>
<td>United States of America v. Wang Dong, et al - U.S. District Court Western District of Pennsylvania</td>
<td>28</td>
</tr>
<tr>
<td>Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? - Remarks by Director of the Federal Bureau of Investigation James B. Comey</td>
<td>56</td>
</tr>
<tr>
<td>Strikes in Syria: The International Law Framework - Jennifer Daskal, Ashley Deeks and Ryan Goodman</td>
<td>65</td>
</tr>
<tr>
<td>The Obama Administration's Legal Justification for Strikes Against the Islamic State in Syria - Jack Goldsmith</td>
<td>67</td>
</tr>
<tr>
<td>Authorization for Use of Military Force Against Iraq Resolution of 2002</td>
<td>71</td>
</tr>
<tr>
<td>Authorization for Use of Military Force, 2001</td>
<td>77</td>
</tr>
<tr>
<td>Letter from the President -- War Powers Resolution Regarding Iraq (September 23, 2014)</td>
<td>79</td>
</tr>
<tr>
<td>Letter to His Excellency Mr. Ban Ki-moon, Secretary-General of the United Nations - Samantha Power</td>
<td>81</td>
</tr>
<tr>
<td>Why Drones Work: The Case for Washington's Weapon of Choice (Brookings) - Daniel L. Byman</td>
<td>97</td>
</tr>
<tr>
<td>Why Drones Fail (Foreign Affairs) - Audrey Kurth Cronin</td>
<td>107</td>
</tr>
<tr>
<td>Projecting Force in the 21st Century - Legitimacy and the Rule of Law - Jeff Mustin &amp; Harvey Rishikof</td>
<td>109</td>
</tr>
<tr>
<td>Demystifying the Title 10 - Title 50 Debate: Distinguishing Military Operations, Intelligence Activities &amp; Covert Action - Andru E. Wall</td>
<td>127</td>
</tr>
</tbody>
</table>

### Panel II

**Role of the Judiciary in National Security**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Security Case Studies: Special Case-Management Challenges - Robert Timothy Reagan</td>
<td>187</td>
</tr>
<tr>
<td>Foreign Intelligence Surveillance Act Litigation - Robert Timothy Reagan</td>
<td>255</td>
</tr>
<tr>
<td>Sealing Court Records and Proceedings: A Pocket Guide - Robert Timothy Reagan</td>
<td>293</td>
</tr>
</tbody>
</table>
# 24th Annual Review of the Field of National Security Law
November 6-7, 2014
Washington, DC

## Conference Material: Day One (Cont’d)

<table>
<thead>
<tr>
<th>Keynote Address</th>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Honorable Suzanne E. Spaulding</td>
<td>Cybersecurity, Terrorism and Beyond: Addressing Evolving Threats to the Homeland - Statement for the Record by The Honorable Suzanne E. Spaulding and The Honorable Francis X. Taylor</td>
<td>383</td>
</tr>
<tr>
<td></td>
<td>Homeland Security Law Institute Looks at Challenges Facing the U.S.</td>
<td>393</td>
</tr>
<tr>
<td></td>
<td>Congress Must Help DHS Combat Rising Cyberattacks (The Hill) - The Honorable Suzanne E. Spaulding</td>
<td>395</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Panel III</th>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Future of Foreign Intelligence</td>
<td>FISA Reform (Georgetown Law) - Laura K. Donohue</td>
<td>399</td>
</tr>
<tr>
<td></td>
<td>High Technology, Consumer Privacy, and U.S. National Security - Remarks by Laura K. Donohue</td>
<td>500</td>
</tr>
<tr>
<td></td>
<td>Bulk Metadata Collection: Statutory and Constitution Considerations (Georgetown Law) - Laura K. Donohue</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Section 702 and the Collection of International Telephone and Internet Content (Georgetown Law) - Laura K. Donohue</td>
<td>500</td>
</tr>
<tr>
<td></td>
<td>Remarks by Robert S. Litt, General Counsel, Office of the Director of National Intelligence (February 28, 2014)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Privacy, Technology &amp; National Security: An Overview of Intelligence Collection - Remarks by Robert S. Litt (July 18, 2013)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Thoughts on a Blue-Sky Overhaul of Surveillance Laws: Introduction - David S. Kris</td>
<td></td>
</tr>
<tr>
<td></td>
<td>On the Bulk Collection of Tangible Things - David S. Kris</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Programmatic Surveillance and FISA: Of Needles in Haystacks (Texas Law Review) - William C. Banks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Remarks by William C. Banks at the 35th Anniversary of the FISC (May 20, 2013)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Guantánamo and Beyond: Exception Courts and Military Commissions in Comparative Perspective - Edited by Fionnuala Ni Aolán &amp; Oren Gross</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Death of FISA - William C. Banks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Basis of the NSA’s Call-Tracking Program Has Disappeared, If It Ever Existed - Jameel Jaffer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Testimony of Jameel Jaffer &amp; Laura W. Murphy before the Senate Judiciary Committee (July 31, 2013)</td>
<td></td>
</tr>
</tbody>
</table>
PANEL I:

EXECUTIVE BRANCH UPDATES ON DEVELOPMENTS IN NATIONAL SECURITY LAW

MEDITATOR: BENJAMIN POWELL
DNI Unveils 2014 National Intelligence Strategy

NEWS RELEASE

FOR IMMEDIATE RELEASE
40-14
September 18 2014

DNI UNVEILS 2014 NATIONAL INTELLIGENCE STRATEGY

Strategy Promotes Integration, Mission Direction and Focuses Resources Across 17 Intelligence Agencies

The Director of National Intelligence James R. Clapper today unveiled the 2014 National Intelligence Strategy - the blueprint that will drive the priorities for the nation's 17 Intelligence Community components over the next four years. The National Intelligence Strategy (NIS) is one of the most important documents for the Intelligence Community (IC) as it sets forth the strategic environment, sets priorities and objectives, and focuses resources on current and future budgets, acquisitions and operations decisions. Most importantly, the strategy builds on the success achieved with integrating intelligence since the previous NIS, as demonstrated by both high-profile operational achievements and significant enterprise improvements.

"Intelligence integration is a journey, not an end state, and The National Intelligence Strategy is another way to promote the integration of the 17 Intelligence Community components, which has been my major theme for the past four years. I believe it's the reason my post and office exists, and it's what the 9/11 Commission advocated and IRTPA legislated," said Clapper.

The National Intelligence Strategy lays out the strategic environment and identifies pervasive and emerging threats. While key nation states such as China, Russia, North Korea and Iran will continue to challenge U.S. interests, global power is also becoming more diffuse. New alignments and informal networks, outside of traditional power blocs and national governments, will increasingly have significant impact in global affairs. Competition for scarce resources such as food, water and energy is growing in importance as an intelligence issue as that competition exacerbates instability, and the constant advancements and globalization of technology will bring both benefits and challenges.

"I've often said publicly that the United States is facing the most diverse set of threats I've seen in my 50 years in the intelligence business. We face significant changes in the global and domestic environment and must be ready to meet the 21st century challenges and to recognize emerging opportunities," said Clapper.

The strategic environment also includes factors that Clapper said affect IC capabilities and what
DNI Unveils 2014 National Intelligence Strategy

he referred to as “a perfect storm” that is degrading IC capabilities including: 1) the theft and leak of NSA documents and the associated loss of collection capabilities; 2) the resulting damaged relationships with foreign and corporate stakeholders; 3) the conscious decision to stop collecting on specific targets; and 4) increasingly constrained budget resources.

“The result of that perfect storm,” said Clapper, “is that we—as a nation—are taking more risk.”

“In many cases, we’ve chosen where we’re taking risk, cutting specific programs, stopping specific collections and declassifying specific documents. All of those are good choices, as long as we recognize that we—as a nation—have to manage the attendant risks,” he said.

*The National Intelligence Strategy* identifies and explains the IC’s objectives – what the IC intends to accomplish (mission objectives) and how the IC will accomplish them (enterprise objectives).

The seven “mission objectives” are: 1) strategic intelligence; 2) anticipatory intelligence; 3) current operations; 4) cyber intelligence; 5) counterterrorism; 6) counterproliferation; and 7) counterintelligence.

The six “enterprise objectives” are: 1) integrated mission management; 2) integrated enterprise management; 3) information sharing and safeguarding; 4) innovation; 5) our people; and 6) our partners.

For the first time, *The National Intelligence Strategy* includes the seven “Principles of Professional Ethics for the Intelligence Community,” which were published in September 2012: 1) mission; 2) truth; 3) lawfulness; 4) integrity; 5) stewardship; 6) excellence; and 7) diversity.

“Each of these seven principles has been a part of the IC I’ve known for 50 years. I believe, if we keep these in front of us, we can continue the crucial work in support of our senior policy makers while we also increase transparency and protect privacy and civil liberties,” concluded Clapper.

The Office of the Director of National Intelligence oversees the coordination and integration of the 17 federal organizations that make up the Intelligence Community. The DNI sets the priorities for and manages the implementation of the National Intelligence Program. Additionally, the DNI serves as the principal adviser to the President and the National Security Council on all intelligence issues related to national security.
Interim Progress Report on Implementing PPD-28

By Robert Litt and Alexander W. Joel

As the President said in his speech on January 17, 2014, “the challenges posed by threats like terrorism, proliferation, and cyber-attacks are not going away any time soon, and for our intelligence community to be effective over the long haul, we must maintain the trust of the American people, and people around the world.”

As a part of that effort, the President made clear that the United States is committed to protecting the personal information of all people regardless of nationality. This commitment is reflected in the directions the President gave to the Intelligence Community on that same day, when he issued Presidential Policy Directive/PPD-28, Signals Intelligence Activities.

New Standards for Safeguarding Privacy

PPD-28 reinforces current practices, establishes new principles, and strengthens oversight, to ensure that in conducting signals intelligence 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.

The Intelligence Community already conducts signals intelligence activities in a carefully controlled manner, pursuant to the law and subject to layers of oversight, focusing on important foreign intelligence and national security priorities. But as the President recognized, “[o]ur efforts will only be effective if ordinary citizens in other countries have confidence that the United States respects their privacy too.”

To that end, the Intelligence Community has been working hard to implement PPD-28 within the framework of existing processes, resources, and capabilities, while ensuring that mission needs continue to be met.

In particular, PPD-28 directs intelligence agencies to review and update their policies and processes - and establish new ones as appropriate - to safeguard personal information collected through signals intelligence, regardless of nationality and consistent with our technical capabilities and operational needs.

Released Today - The PPD-28 Interim Report

As we work to meet the January 2015 deadline, PPD-28 called on the Director of National Intelligence to prepare an interim report on the status of our efforts and to evaluate, in
Interim Progress Report on Implementing PPD-28

coordination with the Department of Justice and the rest of the Intelligence Community, additional retention and dissemination safeguards.

The DNI’s interim report is now being made available to the public in line with our pledge to share as much information about sensitive intelligence activities as is possible, consistent with our national security.

The report is the product of many months of work within the Intelligence Community and with our partners in the other parts of the United States Government, and it draws on conversations agencies have held with outside stakeholders.

Key Privacy Principles for the Intelligence Community

We encourage you to read the whole report released today. It articulates key principles for agencies to incorporate in their policies and procedures, including some which afford protections that go beyond those explicitly outlined in PPD-28. These principles include the following:

- Ensuring that privacy and civil liberties are integral considerations in signals intelligence activities.

- Limiting the use of signals intelligence collected in bulk to the specific approved purposes set forth in PPD-28.

- Ensuring that analytic practices and standards appropriately require that queries of collected signals intelligence information are duly authorized and focused.

- Ensuring that retention and dissemination standards for United States person information under Executive Order 12333 are also applied, where feasible, to all personal information in signals intelligence, regardless of nationality.

- Clarifying that the Intelligence Community will not retain or disseminate information as “foreign intelligence” solely because the information relates to a foreign person.
Interim Progress Report on Implementing PPD-28

- Developing procedures to ensure that unevaluated signals intelligence is not retained for more than five years, unless the DNI determines after careful evaluation of appropriate civil liberties and privacy concerns, that continued retention is in the national security interests of the United States.

- Reinforcing and strengthening internal handling of privacy and civil liberties complaints.

- Reviewing training to ensure that the workforce understands the responsibility to protect personal information, regardless of nationality. Successful completion of this training must be a prerequisite for accessing personal information in unevaluated signals intelligence.

- Developing oversight and compliance programs to ensure adherence to PPD-28 and agency procedures, which could include auditing and periodic reviews by appropriate oversight and compliance officials of the practices for protecting personal information contained in signals intelligence and the agencies’ compliance with those procedures.

- Publicly releasing, to the extent consistent with classification requirements, the procedures developed pursuant to PPD-28.

In the coming months, we will continue to work to complete this review. Taken together, these principles make meaningful progress towards the President’s goal of ensuring that ordinary citizens in other countries have confidence that the United States respects their privacy, too.

Robert Litt is the General Counsel for the Office of the Director of National Intelligence.

Alexander W. Joel is the Civil Liberties Protection Officer for the Office of the Director of National Intelligence.
United States

Friday, March 28, 2014

Thank you for that kind introduction – and for inviting me here today. It’s a pleasure to be back at AU, and a privilege to join so many experts, essential partners, and good friends in advancing one of the most important conversations currently facing government and private sector leaders across the country.

At the Justice Department’s National Security Division, there is little we do that is more important than working on how the government can partner with private companies to protect our nation and its people better – from terrorism, from cyber attacks, and from a range of other malicious activities.

This past December, I attended a ceremony marking the twenty-fifth anniversary of the bombing of Pan Am Flight 103 over Lockerbie, Scotland, which claimed the lives of 259 people on the plane and 11 on the ground. 189 were Americans. It was the deadliest act of terror against the United States prior to September 11th.

The families and friends of those who were lost came together that winter day at Arlington National Cemetery to recall the event that changed their lives forever. They spoke movingly of loved ones who had been on board that plane, many of whom were American college students flying home for the holidays.

On December 21, 1988, instead of reuniting with their companions and loved ones, they heard news reports of a catastrophic explosion and wreckage strewn over miles of the Scottish countryside. Shortly thereafter, they learned, as did the rest of the world, that terrorists were to blame.

There was a call for justice – to find the perpetrators and hold them responsible. And there was also a call for new security measures designed to stop another attack from happening.

At the ceremony last winter, former Secretary of Labor Ann McLaughlin Korologos spoke of her experience leading the seven-member Presidential Commission on Aviation Security and Terrorism that was formed a few months after the attack to investigate what went wrong. Eighteen months after Lockerbie, that Commission issued a report calling for national attention to our aviation security system, and identifying a host of specific proposals intended to harden our nation’s airline security and keep all Americans safe – both at airports and in the skies.

Many of these measures did not become reality. Interest faded, attention waned – and so did political and social will. Twelve years later, the horror of 9/11 changed that. It reinvigorated the focus on aviation security – and the 9/11 Commission called for many of the same security measures called for in the wake of Lockerbie. This time, almost all of them were implemented.

Today, national leaders in both government and private industry must apply the lessons we learned from unspeakable tragedies like these, and from decades of effective counterterrorism policy, to business action in cyberspace. It is imperative that we take action promptly, without waiting for a galvanizing tragedy. We can work together to change norms now — not in the wake of an immensely damaging terrorist cyber attack. In doing so, we will have a much better chance of preventing such an attack from ever taking place.
I grew up in New York City, a place where you can experience the anonymity now enjoyed by so many on the Internet. And when I was a kid, the NYPD sent an officer to our school who told us how to conduct ourselves on the streets of New York.

Our version of Officer Friendly told us to look both ways when we crossed the street. Of course, he told us not to make eye contact with people on the street -- which was pretty standard advice back then.

As a kid, that seemed to make total sense. Decades later, New York City is now one of the safest major cities on the planet. And when we look back at that advice, it seems crazy that there was a consensus of blaming the victim for making eye contact. These days, on the internet, we tell our kids to beware of chatting with individuals they don’t know, to avoid certain websites or apps.

When a person’s credit card gets stolen, or their credentials for accessing a social media site or their bank are hacked, we tell them, “You should have known better than to go to that website,” or, “You shouldn’t have used the same 18-character password more than once.” Together, hopefully, we can look back in a few short years and think that that those warnings and the victim-blaming is also strange and that we’ve come a long way with regards to cyber security.

One of the things that’s changed in New York over the years is its social norms – like making eye contact. We need to shape social norms in the cyber area, too. Just as it was in a chaotic urban environment, it’s tricky to cultivate trust in cyberspace. There were streets in New York where the bad guys and the good guys passed each other shoulder to shoulder. The same thing is true in cyberspace. Legitimate businesses and innocent customers use the same Internet that hackers and terrorists use.

As my former boss at the FBI, Bob Mueller, explained, bad actors – specifically terrorists – are using cyberspace for at least three discrete aspects of terrorist activity: (1) to propagandize and recruit; (2) to plot and plan attacks in the physical world; and (3) to launch attacks in the virtual world itself. It’s hard to cultivate trust online amidst such company and to restore a sense of security. But like change in New York, change in cyberspace will be a community effort. When our Officer Friendly came to visit, he told us about Safe Havens – businesses that opened themselves up just a little bit, to be better members of the community, and to provide a place for people to go if they felt threatened. Back then, there were little yellow Safe Haven signs on the doors of stores in New York, and he told us, “If you’re feeling uncomfortable or scared, or are being targeted, don’t be afraid to go into one of these stores and seek help. Your safety should be your first priority.”

Just as those Safe Havens existed as trusted businesses when I was a kid, the government and the corporate community can come together to create safe havens in cyberspace.

We need to work together to prevent terrorists from using networks – using the very websites and apps we use every day – to plot attacks in the physical world. And we need to shore up our security so that devastating attacks cannot be launched in the virtual world. These tasks are not easy, and they are ones we need to undertake with care, to strike a proper balance between security and liberty.

Some businesses, especially those in the communications sectors, may be hesitant to build new partnerships with government – or are drawing back from their current partnerships – because of the national discussion that has taken place over the last year. The President has committed to providing greater transparency about the government’s lawful use of data collection authorities. However, as the President has noted, the nature of some unauthorized disclosures
have shed more heat than light. And that heat has come onto companies as well, often unfairly. We take their concerns seriously, and we are dedicated to increasing transparency as well as protecting civil liberties. That is why many layers of checks and balances are built into the systems — without question some of the best protections provided by any country in the world. Our authorities are rigorously overseen by Congress, and often scrutinized by the courts and independent government watchdogs. And they are aimed at ensuring the safety of the nation and our allies.

Of course, the private sector should not be punished for complying with the law. We are concerned about this issue, and we are dedicated to working with companies to address misconceptions, correct misinformation, and help to rebuild the public's confidence that our partnerships are conducted under the law. We are working with industry to help them be more transparent about what kinds of information they are required to share with the government, and how very few of their customers are ever impacted by government actions.

Yesterday's announcement by the President of a way forward on the handling of telephony metadata indicates just how committed the Government is to ensuring that the public's concerns are addressed, without the Government sacrificing certain operational needs. As you might have heard, the President announced a proposal that will, with the passage of appropriate legislation, allow the government to end bulk collection of telephony metadata records under Section 215, while ensuring that the government has access to the information it needs to meet its national security requirements.

Getting our legal policies right is one thing. But make no mistake: It will lead to tragedy if the ultimate result of these disclosures is to cause businesses to shy away from working with the government to prevent terrorism. The undeniable truth is that our collaboration, and the protections we have put in place together, make us safer from those who would attempt to do us harm — from terrorists to hostile nation-states seeking to capitalize on our vulnerabilities.

One example that comes to mind is the case of Khalid Aldawsari, a college student from Saudi Arabia who took chemistry classes at Texas Tech in Lubbock, Texas. When he began placing large and unusual orders for chemicals online, the chemical company reported the order to the FBI, as did the shipping company. Ultimately, he was convicted in federal court and sentenced to life in prison for trying to use those chemicals to make a bomb, potentially to attack a former President. And heading off that threat all began with two companies taking the right step of alerting the FBI to suspicious activity.

Whenever the public faces a threat, whether from terrorists, computer hackers, or pick-pockets on the Metro, people expect the government to protect them. But the government can't do it alone. And that is particularly true in the context of cyber threats, given just how much of our nation's most essential information is found online and, in particular, in the hands of private companies.

You know the threats we face. You've seen them firsthand. Although we often think of the government and our brave men and women serving abroad as a primary focus of terrorist attacks, we must keep in mind that the 9/11 attacks targeted this nation as a whole, and its impact was felt by all of us.

Since then, terrorism is now increasingly diverse and decentralized, from al Qaeda affiliates overseas to homegrown terrorists — such as the Boston Marathon bombers — who may live in the communities they intend to strike. But the cyber threat is growing rapidly, and down the road, may rival or even surpass the threat we face today.
Malicious cyber actors are an increasing risk to our security and prosperity. Last year, BP’s CEO stated that his company sees approximately 50,000 attempted cyber intrusions each day. And he is not alone.

As you know, hackers – in many cases working for foreign states or organized criminal syndicates – break into private businesses’ servers and steal the key intellectual property that gives us a competitive edge in the global marketplace. And malicious cyber actors sometimes target companies’ infrastructure. In 2012, Saudi Arabia’s state oil company, Aramco, suffered an attack that destroyed 30,000 of its computers – nearly 75% of its workstations, a devastating loss for any company.

Many of these same hackers exploit vulnerabilities in software, turning home computers or servers into launch pads for malicious denial-of-service attacks against banks, companies, and government agencies – shutting them down and disrupting their ability to do business. It does not take much imagination to see how these same tools could be used by terrorists, resulting in what has been referred to as a potential “cyber 9/11.”

When these attacks happen, people ask the same two basic questions many asked after the Lockerbie bombing: “What more could have been done to protect me?” And, “are they going to get these guys?” To answer these questions, we need the private sector and the government to work together.

Intrusions by nation-states have gone on longer than acknowledged. Why are so many companies waiting to come to the government for help? This situation is not unlike the way that organized crime was able to intimidate small businesses into paying for so-called “insurance”. For each mom and pop store, individually, it made more sense to pay the insurance rather than face retaliation for speaking up or going to the cops. And as a result, the criminal organizations made big profits. They only took a small amount from each business, but the money added up over the dozens or hundreds of businesses they intimidated. It wasn’t until the cost of doing business with the mafia got too high – or someone was brave enough to stand up to the mob – that law enforcement was able to break up these organized crime rings.

The calculus that many businesses make today is similar to the decisions that the mom and pop stores had to make several decades ago: Does the cost of paying out – that is, failing to tell the authorities about cyber attacks – outweigh the costs of potential retaliation? When faced with the prospect of taking on a nation-state with all of its powers – not to mention the fear of not being able to do business in that’s nation’s marketplace – many companies have made the calculation of remaining silent. But the cost of that silence is increasing. As valuable assets, proprietary information, and research and development investments are repeatedly compromised by increasingly relentless attacks, businesses can no longer afford to stay silent victims. The calculus has changed. Companies are taking action.

Over the last year, we have seen a tipping point. As more and more companies come forward, more and more will feel emboldened. Eventually, these nation-state hackers – just like the mafia – will lose the ability to intimidate victims.

Public-private partnerships are particularly important because of the key role that businesses play in our society. Unlike some countries, where government maintains control over the telecommunications and energy industries, nearly all critical infrastructure in the United States is owned and managed by private companies. The fiber-optic cables that our communications transit; the servers that direct our Internet traffic; the software that allows us to communicate; and the energy we use to power our daily lives – all of these things, and so many more, are created and operated by private companies.
We thrive as a nation because of private innovation, and the creativity that comes with the freedom to innovate. This has been true throughout our history. But these unique strengths also create opportunities for attacks. When attacked, companies are often in the best position to protect themselves and their customers from cyber aggressors. But they may not always be in the best position to know the precise threats they face, which is where we can help.

Take, for example, the Department’s work on cyber threats. On a daily basis, the FBI is working with companies that have been the victims of hacks — many of whom may not even know they have been victimized, or how to protect themselves. The Washington Post reported earlier this week that federal agents notified more than 2,000 U.S. companies last year that their computer systems were hacked — and, as the article explained, even that considerable figure represents only a fraction of the actual number of cyber intrusions into the private sector.

There are many efforts underway across the government to work with private corporations on strengthening public-private cyber cooperation. The Department of Homeland Security, the Department of Energy, and other departments and agencies routinely work closely with companies to protect critical infrastructure.

In driving this work forward, the FBI has long relied on its InfraGard program, which brings together individuals in law enforcement, government, the private sector, and academia to talk about how to protect our critical infrastructure. InfraGard has more than 85 chapters across the country, with more than 47,000 members.

These are all positive and important efforts, but we have to do more.

As we speak, the Department of Justice is working hard to be a more accessible partner to companies. Over the past two years, the National Security Division established a national program to focus on cyber threats to the national security — those posed by terrorist and nation state actors — and we are continuing to grow. We are still a very new Division, but we are evolving quickly to meet new and emerging threats.

The story of NSD’s creation is an interesting one. Although not formally created until 2006, NSD’s story begins, like so many others, with calls for reforms that were first spotted years ago. We trace our origin all the way back to 1978, with the passage of the Foreign Intelligence Surveillance Act. FISA was, in part, a response to public and congressional dissatisfaction with a series of intentional abuses of wiretaps and surveillance for political purposes. The Church Committee’s report set out those problems and made a case for reform. The report emphasized that the Attorney General, as the nation’s chief legal officer, plays an essential role in maintaining the lawfulness of actions by our country’s intelligence agencies. NSD was created, and is proud, to execute that mission decades later on his behalf.

So as we tackle the cyber threat, we build upon our roots. We were created so that prosecutors and law enforcement officials could work smoothly and effectively with intelligence attorneys and the Intelligence Community, to ensure that we most effectively defend our nation’s security while at the same time protecting our vital civil liberties. And I would be remiss in describing the vital work of our Division if I neglected to acknowledge this week’s conviction of Sulaiman Abu Ghayth in New York. Abu Ghayth, described as a senior spokesman for Osama bin Laden and al Qaeda, was convicted by a federal jury on all counts, including conspiring to kill Americans and other terrorism charges.
So, even as we defend our national security through successful counterterrorism prosecutions in federal court, we also defend our security while protecting our civil liberties in cyberspace. In 2012, we established the National Security Cyber Specialists’ Network, with members from across all of our areas of expertise, federal prosecutors from each and every U.S. Attorney’s Office, and partners from the Department’s Computer Crime and Intellectual Property Section, who have had longstanding and continuing success against organized cyber criminals, hacktivists, criminal fraudsters and other bad actors.

Since then, we have hosted extensive training for these network members and for every member of the National Security Division, to ensure we have the skills we need to tackle the threat. Federal prosecutors across the country are reaching out to companies in their districts to let them know about the network and how we can help.

Here in our nation’s capital, we work closely with the FBI’s National Cyber Investigative Joint Task Force to assess cyber issues in real time as they arise. We’ve launched a 24/7 cyber response capacity. We are now a one-stop shop and resource for national security cyber matters across the country.

There are criminal cases to be brought against these actors, but that is just one tool. We are committed to using every tool at our disposal, law enforcement and others, to disrupt adversaries’ activities and prevent damage to U.S. national interests – just as we do in other arenas of counterterrorism, counterespionage, and export control.

We are drawing from our expertise in those areas, and building new capabilities to ensure that we can use all available tools to meet a range of constantly-evolving threats.

Employing this comprehensive, “all-tools” approach means we need to be prepared not only to prosecute cyber intrusions, economic espionage, and export control violations, but also to work with our partners to enforce other civil and regulatory laws.

We cannot do this alone. This “all-tools” approach requires trusted collaboration, including with operational and legal experts in the private sector.

It’s often said, there are only two types of companies: those that have been hacked and those that will be. Now, that’s no longer the case. Today, there is only one category: those that have been hacked, and that will be hacked again.

Going forward, we want to work even more closely with our private sector partners to be ready for whatever may happen in the near future. Of course, private companies will remain our first line of defense, and their legal teams must be prepared to face difficult questions and complex matters, including how to respond to cyber breaches; how to interpret and comply with the cyber Executive Order and the cybersecurity framework recently released by the Administration; and, how to stay on top of the evolving “standard of care” for cyber security.

All of us – including lawyers and operators in the public and private sectors – will need to cooperate closely to address these and associated threats. We all must act on the premise that success requires reporting from, and close relationships with, victims and potential victims who seek indicators of malicious activity.
My colleagues and I have already met with a number of private entities and received a positive response, and we will continue these meetings to keep the dialogue going.

And as we look toward the future, we must continue establishing channels that regularly communicate cyber threat information between the public and private sectors. Information must move in both directions. It is an approach that works in other contexts, and it will succeed here as well.

We have come a long way in our collective approach to counterterrorism. Together, we have improved airline safety, hardened critical infrastructure, developed new technology that can help first responders, and designed a wide range of protective measures. These measures, of course, don’t eliminate the threat of to our national security, which remains very real and very dangerous. But we are safer than we used to be, and better prepared to cope with any potential attack.

We need to achieve this same success in the cyber realm. So the critical question is: What will it take?

We’ve certainly had plenty of attacks that caused real pain, exposed real weaknesses, and suggested real problems for the future. Yet, despite all of these warnings, we don’t seem to have fully turned the corner in addressing this threat. And the reasons for that are understandable.

Confronting cyber threats incurs real economic cost. We appreciate that. But doing nothing will cost us all more in the long run, and may, for some businesses, prove devastating.

The writing is on the wall – our adversaries are getting bolder, more aggressive, and more skilled. They flex their muscle to show us what they can do, but it is only the tip of the iceberg. Without a concerted, collective effort to make the changes needed to protect ourselves in cyberspace, it is only a matter of time before we are really hit – hard. Far better to form partnerships and make the required investments before a large-scale attack takes place.

Indeed, perhaps even more than in the terrorism context, the private sector is critical to our success in the cyber context because of just how much vital information is now held “in corporate trust,” so to speak.

While government holds and protects some of what cyber terrorists want to access, the private sector has much, much more. So, whether it’s about ensuring that our electric grid is safe from attacks – whether physical or cyber – or making sure you can access your bank account information on your smartphone without getting hacked, we urgently need to form the type of public-private partnerships to keep those vital resources safe. These are the type of partnerships we’ve created for counterterrorism. We must build on those partnerships to combat cyber threats – not pull away from each other.

This is the challenge now before us – and this is the cause that everyone in this room, and many beyond it, must come together to confront. Each of us has a unique role to play, and distinct responsibilities to fulfill.

Leaders in government can articulate precisely what we have to offer the private sector. Leaders in the private sector can demonstrate what these partnerships have to offer to their customers. And leaders in academia can survey the legal authorities we have – and take stock of what legal authorities we don’t have but need – to facilitate cooperative, productive cyber partnerships. We can build these partnerships while respecting civil liberties and do it in a transparent and productive way.
We are committed to meeting regularly with critical partners to get your feedback on how we are doing; to solicit suggestions on how we can do better; and to gain the benefit of your views on how the overall landscape is looking. Please reach out to us so that we can talk more about what NSD does, and how we can work together to keep you safer and our nation safer.

I want to close today by calling upon everyone here to continue the important open dialogue we’re holding here at AU today. I urge you to serve as connectors – as bridges – to make private-public partnerships a reality.

We had warnings before 9/11. But we didn’t act – at least not enough. The state of security of the Internet today is a rumbling storm in the distance. We need to be smart and work together, now, before a cyber 9/11 – before there’s an attack or intrusion or exfiltration so big – and so devastating – we are forever changed. Thank you for participating in this important conversation, and thank you for having me here today.

Component:
National Security Division (NSD)
U.S. national security prosecutors shift focus from spies to cyber

6:05am BST

By Aruna Viswanatha

WASHINGTON (Reuters) - The U.S. Justice Department is restructuring its national security prosecution team to deal with cyber attacks and the threat of sensitive technology ending up in the wrong hands, as American business and government agencies face more intrusions.

The revamp, led by Assistant Attorney General John Carlin, also marks a recognition that national security threats have broadened and become more technologically savvy since the 9/11 attacks against the United States.

As part of the shift, the Justice Department has created a new position in the senior ranks of its national security division to focus on cyber security and recruited an experienced prosecutor, Luke Dembosky, to fill the position.

The agency is also renaming its counter-espionage section to reflect its expanding work on cases involving violations of export control laws, Carlin confirmed in an interview.

Such laws prohibit the export without appropriate licenses of products or machinery that could be used in weapons or other defence programs, or goods or services to countries sanctioned by the U.S. government.

"We need to develop the capability and bandwidth to deal with what we can see as an evolving threat," said Carlin, who was confirmed to his post in April.

As Carlin builds his team, he has also recruited a new deputy, Mary McCord, from the U.S. Attorney's office in Washington.

The result, according to experts, could be an uptick in the number of national security-related cases brought in federal court, a shift in focus from the National Security Division's prior mandate to investigate intelligence violations.

"This is not just a reshuffling of the deck," said former national security cyber crime prosecutor Nicholas Oldham, who is now in private practice.

CYBER THREATS

The changes come amid reports that hackers in Russia and elsewhere are targeting everyone from the North Atlantic Treaty Organisation and the European Union, to JPMorgan Chase & Co and other financial institutions.

The counter espionage section, which deals less with on-the-ground spies than it used to, will now be called the Counter Intelligence and Export Controls Section. A network of terrorism prosecutors around the country called the Anti-Terrorism Advisory Council, or ATAC, will also be renamed the National Security/ATAC network to make clear its broader responsibilities, Carlin said.

In 2012, Carlin helped create a similar network of national security cyber specialists in each U.S. Attorney's office around the country. That was the first of his efforts to start building cyber expertise within the group of prosecutors that had access to national security intelligence information.

In the first public case to come out of the effort, the agency charged five Chinese military officers in May, accusing them of hacking into U.S. nuclear, metal and solar companies to steal trade secrets. The move ratcheted up tensions between the two countries.

"This prosecution raises the risk that other countries are going to go after our employees ... it's a risky strategy, but a bold one," said Amy Jeffress, a former national security prosecutor who is now in private practices at Arnold & Porter.

While the Chinese officers are not expected to be extradited to face charges in the United States, Carlin said his team is busy with similar cases that would likely be litigated in court.

"I think you will more regularly see the use of the criminal justice system ... We are now actively investigating a variety of nation-state cases. Not all, but some, will result in prosecutions," he said.

In addition to Dembosky, who was coordinating litigation within the criminal division's computer crime section and will serve as one of four deputy assistant attorney generals, Carlin has also brought on board others with cyber expertise. He expects to bring in several more cyber lawyers soon. His chief of staff, Anita Singh, also spent time as a prosecutor in the computer crime section.

(Reporting by Aruna Viswanatha. Editing by Karey Van Hall and Andre Grenon)
REMARKS BY ASSISTANT ATTORNEY GENERAL JOHN P. CARLIN ON CYBER-CRIME AT CARNEGIE MELLON UNIVERSITY

As Prepared for Delivery

PITTSBURGH, PA

Thanks for that kind introduction. I’m grateful to be with you today to discuss emerging national security threats.

In particular, I’ll discuss cyber threats linked to a diverse range of dangerous cyber actors. And I’ll tell you what we in the National Security Division, at the Department of Justice, are doing to counter those threats.

I should note at the outset that this week marks a busy time for national security law. There is a lot going on in the world, all of which we are tracking closely. But I’m going to focus today on the threats associated with national security cyber issues.

Just last week, the 9/11 Commission published its reflections on the tenth anniversary of the Commission’s original report. And it specifically pointed to the growing significance of cyber threats to our Government and private sector.

In its report, the Commission noted that: “We are at September 10th levels in terms of cyber preparedness.” They added that “American companies’ most-sensitive patented technologies and intellectual property, U.S. universities’ research and development, and the nation’s defense capabilities and critical infrastructure, are all under cyber attack.”

I could not agree more.

As the Commission concluded, “One lesson of the 9/11 story is that, as a nation, Americans did not awaken to the gravity of the terrorist threat until it was too late. History may be repeating itself in the cyber realm.”

Returning to Pittsburgh

I’m particularly glad to talk about these important issues here in Pittsburgh. In a way, this brings me back to earlier days of my cybersecurity work.

I began my career as a prosecutor handling a wide range of crimes, but I have spent nearly a decade focusing on cyber issues – including as the National Coordinator of the Justice Department’s Computer Hacking and Intellectual Property, or “CHIP,” program.

Then, I had the honor of joining FBI Director Mueller as he led a critical shift. Even back then, he understood just how significant cyber threats would soon become.

Soon after arriving I was asked to prepare a speech on the FBI’s role in tackling national security cyber threats. We saw this as an important opportunity to underscore how serious the national security cyber threat was—at a time when not many people were talking about it.

It was his first major FBI speech on the national security cyber threat. Much of what the Director said that day remains true today. We warned of the particular dangers lurking in the intersection between cyber and terrorism.

But we also emphasized that terrorists are not the only ones seeking to harm us online—there are other dangerous actors out there, including nation-states. We pointed to the growing use of botnets as a way to attack networks, infect computers, and inject spyware.

We talked about the dangers of cyber espionage, including economic espionage. And we explained that the FBI was mobilizing to address these threats by collaborating with partners across the Federal Government and in the private sector.

That speech, a significant moment in the FBI’s cyber history, was delivered just a few hours east of here, at Penn State. Not just because of the balmy November weather it’s known for. But rather, as explained then, because “[m]uch of our collaboration begins in Pittsburgh—at the FBI’s Cyber Fusion Center.”

The Director said to think of that fusion center as a hub, with spokes emanating out to federal agencies, software companies, Internet service providers, merchants, and members of the financial sector.

That model was right then and it is right now.

The fusion center, and Pittsburgh generally, is the center of so much of our cybersecurity collaboration, which is critical to our efforts to disrupt cyber threats.

That is why a key theme from our time near Pittsburgh nearly seven years ago was collaboration. Back then we talked about the cooperation underway as part of Operation Bot Roast.

Through that project, the Justice Department, the FBI, the CERT Coordination Center at Carnegie Mellon, and private companies were working to identify infected computers and shut down bot-herders.
Also on that trip, we visited the National Cyber-Forensics and Training Alliance, right here in Pittsburgh. Today I came full circle. Now I am delivering a speech about cyber in Pittsburgh. And I spent this morning with the current FBI Director, Jim Comey, visiting NCFTA again.

I could scarcely have guessed back in 2007 that by today the NCFTA would have aided in successful prosecutions of more than 300 cyber criminals worldwide. Or that it would be specifically called out by the recent 9/11 Commission Report, as “a promising example of the type of cross-sector collaboration that will be needed to combat this threat.”

Returning to Pittsburgh, I am struck by just how much progress we have made in seven short years. But there is more that must be done. Our recognition of the magnitude of the cyber threat has grown over that same time.

Director Comey recently said, as the torch was passed, that Director Mueller told him he believed cyber issues would come to dominate Director Comey’s tenure just as counterterrorism had dominated his. Director Comey has continued to express FBI’s steadfast commitment to tackling cyber threats.

Just this morning as the FBI Director and I toured the NCFTA, he reiterated what he has said before, “John Dillinger couldn’t do a thousand robberies in the same day in all 50 states in his pajamas halfway around the world. That’s the challenge we now face with the Internet.”

So the threat is real, it is here, and it is not going away. But today, seven years later, our ability to detect, disrupt and deter has also improved.

Our most recent successes can be traced to the visionaries who predicted the threat years ago and laid the foundation to meet the challenge.

The Pittsburgh Case

Take as just one example, another Pittsburgh story. A historic indictment that came right out of the Western District of Pennsylvania.

Earlier this summer, we announced unprecedented charges against five members of the Chinese military for computer hacking, economic espionage, and other offenses directed at six American victims in the U.S. nuclear power, metals and solar products industries.

What these charges allege is stealing from America’s heartland, literally and figuratively.

The charges allege that cyber thieves grabbed the hard work of companies right here in Pennsylvania. And they allege that the thieves targeted key American economic sectors, like metals and energy.

This is the true face of cyber economic espionage and of those it targets. This type of theft hurts American competitiveness by stealing what we work so hard for.

These charges against uniformed members of the Chinese military were the first of their kind. Some said they could not be brought. But this indictment alleging, with particularity, specific actions on specific days by specific actors to use their computers to steal valuable information from across our economy.

It alleges that while the men and women of our businesses spent their work-days innovating, creating, and developing strategies to compete in the global marketplace, these members of Unit 61398 spent their work days in Shanghai stealing the fruits of our labor.

It alleges that they stole information particularly beneficial to Chinese companies, and took communications that would provide competitors with key insight into the strategy and vulnerabilities of the victims.

We should not and will not stand idly by, tacitly giving permission to anyone to steal from us. We will hold accountable those who steal—no matter who they are, where they are, or whether they steal in person or through the Internet.

Because cyber crime affects us all, including those here in Pennsylvania who have suffered at the hands of cyber thieves.

While cases like the one brought here in Pittsburgh are extremely challenging, we proved that they are possible. The criminal justice system is a critical component of our nation’s cyber security strategy.

Following the Evidence

At the Justice Department, we follow the facts and evidence where they lead. Sometimes, the facts and evidence lead us to a lone hacker in the United States, or a sophisticated organized crime syndicate in Russia. And sometimes, they lead us to a uniformed member of the Chinese military.

Other times, as we recently saw, they may lead us to a foreign businessman alleged to have conspired to hack in and steal information from Boeing and other defense contractors.

Information that included more than six hundred thousand data files of sensitive information related to U.S. military aircraft and other defense matters.

And yet other times, they may lead to other types of criminals, like those investigated and prosecuted by DOJ’s Criminal Division for spyware, botnets, and similar conduct.

But, no matter where they lead, there can be no free passes because the stakes are too high. The list of threats out there is significant and it is expanding.

We have all seen the harms inflicted by state actors and criminals, and we have
responded. But we know they are not the only ones interested in cyber activity.

Terrorists are also using cyberspace to further their goals. They are using it to communicate and plan. They are using it for propaganda and recruitment. And they are intent on getting to the point where they can conduct cyber attacks themselves.

That last category is a relatively new one. But we know that terrorists are looking to launch cyber attacks. They have that intent now.

Over the past few years, we have seen al-Qaeda issue calls for cyberattacks against networks such as the electric grid, comparing vulnerabilities in the United States' critical cyber networks to the vulnerabilities in the country's aviation system before 9/11.

If successful, terrorists could use cyber attacks to bring about economic or physical damage, or even, in extreme cases, serious injury or death.

The National Security Division

These are serious threats. To disrupt them, we take an all-tools approach, deeply rooted in our Division's history.

While the Pittsburgh case was the first of its kind in some ways, it was not the first charges we have brought against individuals who steal from Americans to benefit state-owned enterprises.

As just one example, in March, we successfully obtained a significant conviction against Walter Liew for economic espionage.

What Liew stole was something Americans see and use daily. Something that does not have a national security implication. Something that simply brings a profit.

Liew stole the formula for the color white from DuPont and passed it to a large Chinese state-owned company. Just this month, he was brought to justice -- sentenced to 180 months' incarceration and ordered to pay restitution of about half a million dollars.

Our success in the cyber arena builds upon a solid foundation. But its roots go back even farther, and extend well beyond the economic espionage context.

NSD was created in response to the grave threat of terrorism.

After the devastating attacks of September 11, it became clear that the Justice Department needed to reorganize to tackle terrorism and national security threats more effectively.

We needed a single Division to integrate the work of prosecutors and law enforcement officials with intelligence officers and the Intelligence Community.

So, in 2006, Congress created the Department's first new litigating division in almost a century: NSD.

NSD works closely with partners throughout the government to ensure we leverage all available tools to combat the terrorism threat. And we've proven, in that context, that the criminal justice system is a vital part of our nation's counterterrorism strategy.

Just this spring, Abu Hamza al-Masri was convicted by a jury in New York on eleven counts. He was involved in an attack in Yemen in December 1998 that resulted in the deaths of four hostages.

And he provided material support to terrorists, including al Qaeda and the Taliban.

In March, Sulaiman Abu Ghaith was convicted of conspiring to kill Americans and other terrorism charges. Abu Ghaith was the son-in-law of Osama bin Laden and a senior member of al Qaeda. He was the face and voice of al Qaeda in the days and weeks after the 9/11 attacks.

In both of these cases, it took more than a decade; but, as a result of our integrated approach to combating terrorism, we brought these men to justice.

These cases are the two most recent in a long line of successful terrorism prosecutions.

At NSD, we took the lessons we learned from counterterrorism and applied them to our work on national security cyber threats. In the face of escalating threats, we recognized the need to reorganize. To integrate.

When I was chief of staff for Director Mueller, the FBI undertook a transformation to meet the growing cyber threat—a transformation built around the type of collaboration, coordination, and cooperation that the Director described in his speech right here in Pennsylvania. In 2011, NSD did the same.

In late fall of 2011, ten years after 9/11, we established a review group to evaluate NSD’s existing work on national security threats and chart a plan for the future.

Six months later, that team issued recommendations that shaped what NSD’s national security cyber program looks like today.

Most significantly, in 2012, we created and trained the National Security Cyber Specialists' Network to focus on combating cyber threats to the national security.

This Network—known as NSCS—includes prosecutors from every U.S. Attorney's Office around the country, along with experts from the Department’s Computer Crime and Intellectual Property Section (or "CCIPS") and attorneys from across all parts of NSD.

Adopting the successful counterterrorism model, we now have prosecutors nationwide routinely meeting with the FBI to review intelligence and investigative files.
The creation of the NSCS Network was motivated by a desire to increase the Department's contribution to U.S. cybersecurity efforts through criminal investigation and prosecution.

By December 2012, we made public predictions that with the establishment of the NSCS—by empowering more than a hundred prosecutors in the field working with the FBI on these cases—one would be brought.

And, in May, we made good on that promise. It is this new, integrated approach that made the Pittsburgh case possible.

As part of the creation of the NSCS, we brought prosecutors from around the country—Wisconsin, New York, and Georgia—to help NSD build this case.

We partnered with colleagues across the government, like U.S. Attorney David Hickton here in the Western District of Pennsylvania, where entities were repeatedly hit. And we worked with offices across the FBI—from California, to Oregon, to Oklahoma, and back in D.C.

Our team thought creatively. They worked collaboratively. They explored all available options for stopping this activity.

That's how we were able to indict five members of the Third Department of the People's Liberation Army. And now these men stand accused of cyber intrusions targeting a range of U.S. industries.

All-Tools

But we recognize that charges are just one tool—albeit a very effective one—in our toolbox. We are committed to working with our colleagues throughout the government to ensure we bring all tools to bear to disrupt cyber threats—both criminal and national security.

A great example is yet another Pittsburgh story. Back in June, our colleagues in the Criminal Division, the Western District of Pennsylvania, and the Bureau undertook an operation that disrupted the GameOver Zeus botnet.

This criminal threat was significant—losses attributable to the botnet were estimated to be more than $100 million. But disruption involved more than just criminal charges—it also involved civil court orders, significant information sharing, and seizures of servers in many foreign countries.

This is just one example. In the national security context, we look to the viability of sanctions, designations, diplomatic options, and other enforcement mechanisms. Through collaboration and creative thinking, our toolset continues to grow.

Importance of Defense

But we at NSD recognize that stopping attacks before they ever take place is the ultimate goal. That we will succeed when there are no more criminal charges to bring.

To that end, we also worked hard to improve cyber defenses, both in Government and with the private sector. We've emphasized precisely the type of collaboration that Director Mueller discussed here in Pennsylvania seven years ago.

Through the FBI's InfraGard, the FBI works closely with companies that have been the victims of hackers.

That program, which has grown to more than 25,000 active members, continues to bring together individuals in law enforcement, government, the private sector, and academia to talk about how to protect our critical infrastructure.

Likewise, the Department of Homeland Security, the Department of Energy, and other departments and agencies routinely work closely with companies to protect critical infrastructure.

We at the Justice Department heard from such companies. And we are taking steps to respond to the concerns of the private sector.

In April, we teamed up with the Federal Trade Commission to issue a policy statement making it clear that antitrust law is not and should not be a bar to legitimate cyber security information sharing.

And in May, the Justice Department issued a white paper, which clarifies that the Stored Communications Act doesn't ordinarily restrict network operators from sharing certain data with the Government to guard information.

This guidance will help the private sector collaborate more freely to protect itself.

All of this is just a start. Going forward, we need legislation to facilitate greater information sharing between the private sector and the government.

Conclusion

In conclusion, we've come a long way in seven years.

In Pennsylvania seven years ago, we warned that "cyber criminals and terrorists seek to harm our economy, our infrastructure, and our way of life." That was true then, and it's even more true now.

We noted that "our capabilities are strong, but they rely on key partnerships with other federal agencies, law enforcement, private industry, academia, and citizens alike." That was true then, and it's even more true now.

Finally, the Director of the FBI issued an imperative: "we must continue to work closely
with all of you—members of the privacy sector and the academic community.”

I’m here today with a new FBI Director to reaffirm that call. Because it was true then, and, as the 9/11 Commission’s recent report makes clear, it’s even more true now.

Through charges like the ones announced in the Pittsburgh case, we at the Justice Department continue to protect Americans from being victimized through cyberspace as they were here in Pittsburgh. We need your support. Talk with us; share with us; work with us. Build trust.

Together, we can ensure that, here in America’s heartland and throughout this country, the hard work of Americans doesn’t fall prey to cyber criminals. Together, we can stay connected, and also stay safe.

Thank you for your attention. I look forward to your questions.

###

Department of Justice
Office of Public Affairs

FOR IMMEDIATE RELEASE

Monday, May 19, 2014


First Time Criminal Charges Are Filed Against Known State Actors for Hacking

A grand jury in the Western District of Pennsylvania (WDPA) indicted five Chinese military hackers for computer hacking, economic espionage and other offenses directed at six American victims in the U.S. nuclear power, metals and solar products industries.

The indictment alleges that the defendants conspired to hack into American entities, to maintain unauthorized access to their computers and to steal information from those entities that would be useful to their competitors in China, including state-owned enterprises (SOEs). In some cases, it alleges, the conspirators stole trade secrets that would have been particularly beneficial to Chinese companies at the time they were stolen. In other cases, it alleges, the conspirators also stole sensitive, internal communications that would provide a competitor, or an adversary in litigation, with insight into the strategy and vulnerabilities of the American entity.

“This is a case alleging economic espionage by members of the Chinese military and represents the first ever charges against a state actor for this type of hacking,” U.S. Attorney General Eric Holder said. “The range of trade secrets and other sensitive business information stolen in this case is significant and demands an aggressive response. Success in the global market place should be based solely on a company’s ability to innovate and compete, not on a sponsor government’s ability to spy and steal business secrets. This Administration will not tolerate actions by any nation that seeks to illegally sabotage American companies and undermine the integrity of fair competition in the operation of the free market.”

“For too long, the Chinese government has blatantly sought to use cyber espionage to obtain economic advantage for its state-owned industries,” said FBI Director James B. Comey. “The indictment announced today is an important step. But there are many more victims, and there is much more to be done. With our unique criminal and national security authorities, we will continue to use all legal tools at our disposal to counter cyber espionage from all sources.”

“State actors engaged in cyber espionage for economic advantage are not immune from the law just because they hack under the shadow of their country’s flag,” said John Carlin, Assistant Attorney General for National Security. “Cyber theft is real theft and we will hold state
sponsored cyber thieves accountable as we would any other transnational criminal organization
that steals our goods and breaks our laws.”

“This 21st century burglary has to stop,” said David Hickton, U.S. Attorney for the Western
District of Pennsylvania. “This prosecution vindicates hard working men and women in Western
Pennsylvania and around the world who play by the rules and deserve a fair shot and a level
playing field.”

Summary of the Indictment

Defendants: Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui, who
were officers in Unit 61398 of the Third Department of the Chinese People’s Liberation Army
(PLA). The indictment alleges that Wang, Sun, and Wen, among others known and unknown to
the grand jury, hacked or attempted to hack into U.S. entities named in the indictment, while
Huang and Gu supported their conspiracy by, among other things, managing infrastructure (e.g.,
domain accounts) used for hacking.

Victims: Westinghouse Electric Co. (Westinghouse), U.S. subsidiaries of SolarWorld AG
(SolarWorld), United States Steel Corp. (U.S. Steel), Allegheny Technologies Inc. (ATTI), the
United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service
Workers International Union (USW) and Alcoa Inc.


Crimes: Thirty-one counts as follows (all defendants are charged in all counts).

<table>
<thead>
<tr>
<th>Count(s)</th>
<th>Charge</th>
<th>Statute</th>
<th>Maximum Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Conspiring to commit computer fraud and abuse</td>
<td>18 U.S.C. § 1030(b).</td>
<td>10 years.</td>
</tr>
<tr>
<td>2-9</td>
<td>Accessing (or attempting to access) a protected computer without authorization to obtain information for the purpose of commercial advantage and private financial gain.</td>
<td>18 U.S.C. §§ 1030(a)(2)(C), 1030(e)(2)(B)(i)-(iii), and 2.</td>
<td>5 years (each count).</td>
</tr>
<tr>
<td>10-23</td>
<td>Transmitting a program, information, code, or command with the intent to cause damage to protected computers.</td>
<td>18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(B), and 2.</td>
<td>10 years (each count).</td>
</tr>
<tr>
<td>24-29</td>
<td>Aggravated identity theft.</td>
<td>18 U.S.C. §§ 1028A(a)(1), (b), (e)(4), and 2</td>
<td>2 years (mandatory consecutive).</td>
</tr>
<tr>
<td>30</td>
<td>Economic espionage.</td>
<td>18 U.S.C. §§ 1831(a)(2), (a)(4), and 2.</td>
<td>15 years.</td>
</tr>
</tbody>
</table>
**Summary of Defendants’ Conduct Alleged in the Indictment**

<table>
<thead>
<tr>
<th>Defendant</th>
<th>Victim</th>
<th>Criminal Conduct</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sun</td>
<td>Westinghouse</td>
<td>In 2010, while Westinghouse was building four AP1000 power plants in China and negotiating other terms of the construction with a Chinese SOE (SOE-1), including technology transfers, Sun stole confidential and proprietary technical and design specifications for pipes, pipe supports, and pipe routing within the AP1000 plant buildings. Additionally, in 2010 and 2011, while Westinghouse was exploring other business ventures with SOE-1, Sun stole sensitive, non-public, and deliberative e-mails belonging to senior decision-makers responsible for Westinghouse’s business relationship with SOE-1.</td>
</tr>
<tr>
<td>Wen</td>
<td>SolarWorld</td>
<td>In 2012, at about the same time the Commerce Department found that Chinese solar product manufacturers had “dumped” products into U.S. markets at prices below fair value, Wen and at least one other, unidentified co-conspirator stole thousands of files including information about SolarWorld’s cash flow, manufacturing metrics, production line information, costs, and privileged attorney-client communications relating to ongoing trade litigation, among other things. Such information would have enabled a Chinese competitor to target SolarWorld’s business operations aggressively from a variety of angles.</td>
</tr>
<tr>
<td>Wang and Sun</td>
<td>U.S. Steel</td>
<td>In 2010, U.S. Steel was participating in trade cases with Chinese steel companies, including one particular state-owned enterprise (SOE-2). Shortly before the scheduled release of a preliminary determination in one such litigation, Sun sent spear phishing e-mails to U.S. Steel employees, some of whom were in a division associated with the litigation. Some of these e-mails resulted in the installation of malware on U.S. Steel computers. Three days later, Wang stole hostnames and descriptions of U.S. Steel computers (including those that controlled physical access to company facilities and mobile device access to company</td>
</tr>
</tbody>
</table>
networks). Wang thereafter took steps to identify and exploit vulnerable servers on that list.

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Wen</td>
<td>ATI</td>
<td>In 2012, ATI was engaged in a joint venture with SOE-2, competed with SOE-2, and was involved in a trade dispute with SOE-2. In April of that year, Wen gained access to ATI's network and stole network credentials for virtually every ATI employee.</td>
</tr>
<tr>
<td>Wen</td>
<td>USW</td>
<td>In 2012, USW was involved in public disputes over Chinese trade practices in at least two industries. At or about the time USW issued public statements regarding those trade disputes and related legislative proposals, Wen stole e-mails from senior USW employees containing sensitive, non-public, and deliberative information about USW strategies, including strategies related to pending trade disputes. USW's computers continued to beacon to the conspiracy's infrastructure until at least early 2013.</td>
</tr>
<tr>
<td>Sun</td>
<td>Alcoa</td>
<td>About three weeks after Alcoa announced a partnership with a Chinese state-owned enterprise (SOE-3) in February 2008, Sun sent a spear phishing e-mail to Alcoa. Thereafter, in or about June 2008, unidentified individuals stole thousands of e-mail messages and attachments from Alcoa's computers, including internal discussions concerning that transaction.</td>
</tr>
<tr>
<td>Huang</td>
<td></td>
<td>Huang facilitated hacking activities by registering and managing domain accounts that his co-conspirators used to hack into U.S. entities. Additionally, between 2006 and at least 2009, Unit 61398 assigned Huang to perform programming work for SOE-2, including the creation of a “secret” database designed to hold corporate “intelligence” about the iron and steel industries, including information about American companies.</td>
</tr>
<tr>
<td>Gu</td>
<td></td>
<td>Gu managed domain accounts used to facilitate hacking activities against American entities and also tested spear phishing e-mails in furtherance of the conspiracy.</td>
</tr>
</tbody>
</table>

An indictment is merely an accusation and a defendant is presumed innocent unless proven guilty in a court of law.
The FBI conducted the investigation that led to the charges in the indictment. This case is being prosecuted by the U.S. Department of Justice’s National Security Division Counterespionage Section and the U.S. Attorney’s Office for the Western District of Pennsylvania.
information from those entities that would be useful to their competitors in China, including state-owned enterprises ("SOEs").

2. In some cases, the conspirators stole trade secrets that would have been particularly beneficial to Chinese companies at the time they were stolen. For example, as described in more detail below, an Oregon producer of solar panel technology was rapidly losing its market share to Chinese competitors that were systematically pricing exports well below production costs; at or around the same time, members of the conspiracy stole cost and pricing information from the Oregon producer. And while a Pennsylvania nuclear power plant manufacturer was negotiating with a Chinese company over the construction and operation of four power plants in China, the conspirators stole, among other things, proprietary and confidential technical and design specifications for pipes, pipe supports, and pipe routing for those nuclear power plants that would enable any competitor looking to build a similar plant to save on research and development costs in the development of such designs.

3. In the case of both of those American victims and others, the conspirators also stole sensitive, internal communications that would provide a competitor, or adversary in
litigation, with insight into the strategy and vulnerabilities of the American entity.

4. Meanwhile, during the period relevant to this Indictment, Chinese firms hired the same PLA Unit where the defendants worked to provide information technology services. For example, one SOE involved in trade litigation against some of the American victims mentioned herein hired the Unit, and one of the co-conspirators charged herein, to build a "secret" database to hold corporate "intelligence."

THE DEFENDANTS

5. At various times relevant to this Indictment, Defendants WANG DONG, a/k/a "Jack Wang," a/k/a "UglyGorilla" (hereinafter "Defendant WANG"); SUN KAILIANG, a/k/a "Sun Kai Liang," a/k/a "Jack Sun" (hereinafter "Defendant SUN"); WEN XINYU, a/k/a "Wen Xin Yu," a/k/a "WinXYHappy," a/k/a "Win_XY," a/k/a "Lao Wen" (hereinafter "Defendant WEN"); HUANG ZHENYU, a/k/a "Huang Zhen Yu," a/k/a "hzy_lhx," (hereinafter "Defendant HUANG"); and GU CHUNHUI, a/k/a "Gu Chun Hui," a/k/a "KandyGoo" (hereinafter "Defendant GU"). whose photographs are attached as Exhibits A through E, respectively, worked together and with others known and unknown to the Grand Jury for the PLA's General Staff, Third Department ("3PLA"), a signals intelligence component of the PLA, in a Unit known by the Military Unit Code Designator 61398 ("Unit 61398"), and in the vicinity of 208 Datong Road, Pudong District, Shanghai, China.

6. The co-conspirators' hacking activities are described in more detail below but are summarized here as follows:

a. In or about 2007, Westinghouse Electric Company ("Westinghouse"), which is headquartered in the Western District of Pennsylvania, reached an agreement with a Chinese state-owned nuclear power company ("SOE-1") to construct and operate four nuclear power plants in China. Negotiations regarding the details of that transaction, such as limitations on which technology would be provided to SOE-1 and under what conditions, continued up to and including 2013. In or about 2010 and 2011, while negotiations were ongoing, Defendant SUN stole from Westinghouse's computers, among other things, proprietary and confidential technical and design specifications for pipes, pipe supports, and pipe routing within the nuclear power plants that Westinghouse was contracted to build, as well as internal Westinghouse communications concerning the company's strategy for doing business with SOE-1 in China and the potential that SOE-1 may eventually become a competitor.

b. In or about May and July 2012, Defendant WEN hacked into the computers of U.S. subsidiaries of SolarWorld AG, a German solar products manufacturing company, including a production facility located in Hillsboro, Oregon, and a sales
facility located in Camarillo, California (collectively, "SolarWorld"). From in or about May 2012 up to and including at least in or about September 2012, Defendant WEN and at least one unidentified co-conspirator stole thousands of e-mails and related attachments that provided detailed information about SolarWorld’s financial position, production capabilities, cost structure, and business strategy. Meanwhile, contemporaneous with that hacking, SolarWorld was an active litigant in trade cases against Chinese solar manufacturers, several of which reported in filings with the U.S. Securities and Exchange Commission ("SEC") that their sales revenues had increased each year from 2009 through 2011. In or about May 2012, the Department of Commerce imposed significant duties on Chinese imports of solar products, based on its finding that those manufacturers had received unfair subsidies from China and had “dumped” large volumes of solar products into U.S. markets at prices below fair value, severely undercutting competitors like SolarWorld and, in some cases, helping to drive the most vulnerable American solar products manufacturers out of business. Several Chinese solar manufacturers subsequently reported in SEC filings that, in 2012, their sales revenues had decreased from 2011, and their net income and profit margins had dropped to five-year lows.

c. Between in or about 2009 and in or about 2012, United States Steel Corporation ("U.S. Steel"), which is headquartered in the Western District of Pennsylvania, litigated a number of trade cases against the Chinese steel industry, including specifically one large, Chinese state-owned steel company ("SOE-2"). About two weeks before the anticipated decision in one of those disputes in 2010, Defendant SUN targeted one of the employees working in the relevant division of U.S. Steel with an e-mail message, known as a “spear phishing” message, that was designed to trick the employee who received it into allowing SUN access to the employee’s computer. At or about that time, Defendant WANG stole hostnames and descriptions for more than 1,700 servers, including servers that controlled physical access to the company’s facilities and mobile device access to the company’s networks.

d. Allegheny Technologies Incorporated ("ATI"), a specialty metals manufacturer headquartered in the Western District of Pennsylvania, has since in or about 1995 been a partner in a joint venture with SOE-2 and was, between 2009 and 2012, also an adversary of SOE-2 in litigation before the World Trade Organization ("WTO"). In April 2012, the day after a board meeting for the joint venture in Shanghai, China, Defendant WEN stole network credentials for virtually every
employee at the company, which would have allowed wide-ranging and persistent access to ATI's computers.

e. The United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International Union ("USW"), headquartered in the Western District of Pennsylvania, has long been a vocal opponent of Chinese trade practices. In 2012, on or about the day that the USW's President issued a "call to action" against Chinese policies, Defendant WAN stole e-mail messages containing strategic discussions from senior union employees. And two days after the union publicly urged Congress to pass legislation that would have imposed duties on Chinese imports, Defendant WAN stole more e-mail messages containing internal, strategic discussions.

f. In or about 2008, Alcoa Incorporated ("Alcoa"), an aluminum manufacturer whose principal office is located in the Western District of Pennsylvania, announced a partnership with a Chinese state-owned aluminum company to acquire a stake in another foreign mining company. Approximately three weeks later, Defendant SUN targeted senior Alcoa managers with spear phishing messages designed to trick the recipients into providing SUN with access to the company's computers.

7. As described above, Defendants WAN, SUN, and WEN, among others known and unknown to the Grand Jury, hacked or attempted to hack into at least the U.S. companies described above.

8. Contemporaneously, beginning at least in or about 2006 and continuing until at least in or about 2012, Defendant HUANG was a computer programmer within the same military Unit. He facilitated hacking activities by registering and managing domain accounts that his co-conspirators, including at least Defendants WAN, SUN, and WEN, used to commit those crimes. Meanwhile, beginning at least in or about 2006 and continuing until at least in or about 2009, Unit 61398 assigned Defendant HUANG to perform programming work for SOE-2, including the creation of a "secret" database for SOE-2 designed to hold corporate "intelligence" about the iron and steel industries, including information about American companies.

9. Like Defendant HUANG, beginning at least in or about 2006 and continuing until at least in or about 2010, Defendant GU managed domain accounts used to facilitate hacking activities against American companies. Defendant GU also tested spear phishing messages in furtherance of the conspiracy.

MANNER AND MEANS OF THE CONSPIRACY

10. The members of the conspiracy, who are both known and unknown to the Grand Jury, used the following manner and means to accomplish their objectives, which included gaining
authorized access to computers and using that access to steal information.

11. As described above, the co-conspirators used e-mail messages known as "spearphishing" messages to trick unwitting recipients into giving the co-conspirators access to their computers. Spearphishing messages were typically designed to resemble e-mails from trustworthy senders, like colleagues, and encouraged the recipients to open attached files or click on hyperlinks in the messages. However, the attached or linked files, once opened, installed "malware" --- malicious code --- that provided unauthorized access to the recipient's computer (known as a "backdoor"), thereby allowing the co-conspirators to bypass normal authentication procedures in the future.

12. After creating a backdoor, the malware typically attempted to contact other computers controlled by the co-conspirators by sending them a short message known as a "beacon." These beacons typically (1) notified the co-conspirators of the successful penetration of a victim's computer; (2) provided some information about the victim's computer useful for future intrusion activity; and (3) solicited additional instructions from the co-conspirators.

13. During the conspiracy, the co-conspirators controlled compromised computers in the United States besides those belonging to the six entities named above. The co-conspirators generally used those computers, known as "hop points," to access other victims' computers, and in so doing, the co-conspirators attempted to mask the true identity and location of the computers in China from which they were actually conducting their hacking activity. Among other things, the co-conspirators used hop points to research victims, send spearphishing e-mails, store and distribute additional malware, manage malware, and transfer exfiltrated data. Some hop points were used as command-and-control servers, which received communications from, and returned instructions to, malware on other compromised computers.

14. The co-conspirators commonly used domain names to hide malicious communications to and from hop points and other victim computers. "Domain names" are labels used to indicate ownership or control of a resource on the Internet, and they are governed by the rules and procedures of the Domain Name System ("DNS"). Domain names resolve back to specific Internet Protocol (or simply "IP") addresses, which are unique, numeric addresses assigned to computers to route traffic on the Internet.

15. The function of the DNS is to translate an alphanumeric domain name into an IP address of the computer hosting that domain; using the DNS is analogous to using a phone book to look up the phone number of a particular person. Typically, an Internet user attempts to navigate to a website
using its domain name, but computers navigate to a website using an IP address. When a computer user types the domain "websitename.com" into a web browser, for example, the user’s computer contacts a DNS server, which then translates the domain name into an IP address, like "58.247.27.223," and sends that IP address back to the user’s computer. The user’s computer can then immediately communicate directly with websitename.com, because it has identified the corresponding IP address. Dynamic DNS providers enable owners or operators of domain names to change the IP addresses to which the domain names resolve, usually by logging into domain accounts at the providers over the Internet and configuring the settings for the domain names to include the destination IP addresses.

16. The co-conspirators, either directly or through intermediaries, purchased, leased, or otherwise registered domain names from domain registrars, obtained accounts at dynamic DNS providers, and assigned the domain names to those domain accounts (if the domain names were not already assigned to the desired DNS providers as part of the original purchase, lease, or registration). Using those domain accounts, the co-conspirators managed the resolutions of those domain names (that is, the assignments of those domain names to particular IP addresses on the Internet, to which lookup requests for those domain names would be directed). Often, those domain names were designed to mimic the domain names of legitimate websites, but with slight differences in spelling, such as "finaceanalysis.com," "gmaileboxes.com," and "busketball.com." The co-conspirators then used the domain names with their malware. After the malware was installed on victim computers, the domain names served as the destination points for the malware to contact, or beacon, for further instructions. The table below lists some of the other malicious domains used by the conspiracy during the period relevant to this Indictment:

<table>
<thead>
<tr>
<th>Malicious Domain Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>arrowservice.net</td>
</tr>
<tr>
<td>bigish.net</td>
</tr>
<tr>
<td>businessconsults.net</td>
</tr>
<tr>
<td>businessformars.com</td>
</tr>
<tr>
<td>marobrother.com</td>
</tr>
<tr>
<td>purspledaily.com</td>
</tr>
<tr>
<td>newsonet.net</td>
</tr>
<tr>
<td>comrepear.com</td>
</tr>
<tr>
<td>cplaymagazine.com</td>
</tr>
<tr>
<td>hugossoft.org</td>
</tr>
</tbody>
</table>

17. The co-conspirators used the domain accounts at dynamic DNS providers to assign their domain names to the IP addresses of different computers depending on their needs at the time. For example, when the co-conspirators wished to proceed with particular intrusions, they used the applicable accounts at dynamic DNS providers to turn malicious domains associated with their malware "on," that is, to assign the domains to the IP addresses of computers under their control, like hop points. Then, between intrusions, the co-conspirators used the domain
accounts to reassign the malicious domain names to non-routable or innocuous IP addresses (e.g., IP addresses for popular webmail services, like Gmail or Yahoo), which would obscure any beacons their malware sent during that period. At one dynamic DNS provider, for example, domains were typically turned "on" at the beginning of business hours in Shanghai, Monday through Friday, and turned "off" (reassigned to non-routable or innocuous IP addresses) at lunchtime and the close of business, and left off over the weekend, as the charts attached as Exhibit F to this Indictment show.

18. After obtaining a foothold in a victim’s computers, the co-conspirators performed a variety of functions designed to identify, collect, package, and exfiltrate targeted data from the victim’s computers to other computers under the co-conspirators’ control.

THE CONSPIRACY’S INTRUSIONS AT SIX VICTIMS

Westinghouse

19. Westinghouse is one of the world’s leading civilian nuclear power developers, providing fuel, services, and plant design to customers in the commercial nuclear industry worldwide. The company’s designs are the basis for approximately half of the world’s currently operating nuclear power plants. Westinghouse’s AP1000 Nuclear Power Plant is a particularly well-known power plant design, with unique safety features, which took Westinghouse significant resources to develop over a 15-year period.

20. After two years of negotiations, on July 24, 2007, Westinghouse and SOE-1, a Chinese state-owned enterprise in the nuclear power industry, signed contracts for the construction and operation of four AP1000 power plants in China, subject to further negotiations on certain unresolved issues. Those contracts provided for the transfer of some technology to SOE-1, but they limited what SOE-1 was permitted to do with it. For example, SOE-1 was not authorized to send materials and components outside China, to use them in reactor plants that competed with Westinghouse’s products outside China, or to use them for military purposes. Further, the technology transfer contracts limited SOE-1’s ability to provide such technologies to entities other than those listed in the contracts without notifying and receiving approval from Westinghouse. Negotiations regarding the other details, including additional technology transfer issues, continued for years thereafter, up to and including 2013.

21. During the conspiracy, while Westinghouse was building the AP1000 plants and negotiating other terms with SOE-1, hackers repeatedly targeted Westinghouse’s computers, including computers in the Western District of Pennsylvania. For example, on or about May 6, 2010, Defendant SUN gained unauthorized
access to Westinghouse’s computers and stole proprietary and confidential technical and design specifications related to pipes, pipe supports, and pipe routing within the API1000 plant buildings. Among other things, such specifications would enable a competitor to build a plant similar to the API1000 without incurring significant research and development costs associated with designing similar pipes, pipe supports, and pipe routing systems. During the same intrusion, Defendant SUN also stole Westinghouse network credentials that would facilitate additional, unauthorized access.

22. In addition to constructing the API1000 plants and negotiating contractual details relating to those plants, in late 2010, Westinghouse began to explore other business ventures with SOE-1. For example, in or about September 2010, Westinghouse and SOE-1 began negotiating over the construction of additional power plants in China. Westinghouse sought to conclude these negotiations before the arrival of an SOE-1 official in Washington, D.C., as part of a January 2011 Chinese state visit, so that the agreement could be signed during the visit. Meanwhile, Westinghouse management internally discussed what approach to take during upcoming negotiations and in future partnerships with SOE-1, as well as the potential that SOE-1 may eventually become a competitor.

23. While these business initiatives and discussions were underway, beginning at least in or about December 2010 and continuing until at least in or about January 2011, Defendant SUN repeatedly targeted Westinghouse’s computers. For example, on or about December 30, 2010, January 3, 2011, and January 5, 2011, Defendant SUN gained unauthorized access to Westinghouse’s computers and stole sensitive, non-public, and deliberative e-mails belonging to senior decision-makers responsible for Westinghouse’s business relationship with SOE-1, including Westinghouse’s Chief Executive Officer. Some stolen e-mails described the status of the four API1000 plants’ construction. Many other stolen e-mails, however, concerned Westinghouse’s confidential business strategies relating to SOE-1, including Westinghouse’s (a) strategies for reaching an agreement with SOE-1 on future nuclear power plant construction in China; and (b) discussions regarding cooperation and potential future competition with SOE-1 in the development of nuclear power plants elsewhere around the world.

24. In total, between in or about 2010 and in or about 2012, members of the conspiracy stole at least 1.4 gigabytes of data, the equivalent of roughly 700,000 pages of e-mail messages and attachments, from Westinghouse’s computers.
25. At times relevant to this Indictment, SolarWorld had significant business interests relating to China, including as a direct competitor with various Chinese solar products manufacturers. Beginning at least in or about October 2011 and continuing until in or about September 2012, SolarWorld was particularly active in trade litigation involving Chinese manufacturers: it was the lead petitioner in a case before the U.S. Department of Commerce and U.S. International Trade Commission. That litigation ultimately resulted in a finding that Chinese solar manufacturers had received unfair subsidies from China and had "dumped" large volumes of solar products into U.S. markets at prices below fair value. As a result, the Department of Commerce imposed significant countervailing and antidumping duties on Chinese imports of solar products.

26. On or about May 3, 2012, following one preliminary determination by the Department of Commerce and about two weeks before a second determination was scheduled, Defendant WEN hacked into SolarWorld's computers and stole e-mails and files belonging to three senior executives. Then, from on or about May 9, 2012 up to and including on or about September 26, 2012, Defendant WEN and at least one other, unidentified co-conspirator conducted at least twelve more intrusions into and exfiltrations from SolarWorld's computers. Through those intrusions, they stole thousands of e-mail messages and other files from at least seven identified SolarWorld employees who, based on their positions, would be expected to have comprehensive and highly detailed information about SolarWorld's financial position, production capabilities, cost structure, business strategy, or trade litigation strategy.

27. Collectively, the data stolen from SolarWorld would have enabled a Chinese competitor to target SolarWorld's business operations aggressively from a variety of angles. For example, the stolen data included: (1) cash-flow spreadsheets maintained by the Chief Financial Officer that would enable a Chinese competitor to identify the length of time that SolarWorld might survive a financial or market shock; (2) detailed manufacturing metrics, technological innovations, and production line information that would enable a Chinese competitor to mimic SolarWorld's proprietary production capabilities without the need to invest time or money in research and development; (3) specific production costs for all manufacturing inputs that would enable a Chinese competitor to undermine SolarWorld financially through targeted and sustained underpricing of solar products; and (4) privileged attorney-client communications related to SolarWorld's ongoing trade litigation with China, including confidential Question-and-
Answer documents submitted to the Department of Commerce that were not discoverable by the Chinese respondents.

**U.S. Steel**

28. U.S. Steel is the largest steel company in the United States. During the period relevant to this Indictment, U.S. Steel had significant business interests relating to China, including as a competitor of several Chinese steel manufacturers like SOE-2. For example, beginning at least in or about 2009 and continuing until at least in or about 2012, U.S. Steel participated in several international trade disputes with Chinese steel manufacturers, including SOE-2. These disputes involved allegations that China subsidized the Chinese steel industry and that the Chinese steel industry “dumped” steel into U.S. markets at below-market prices.

29. In or about 2010, U.S. Steel was particularly active in that litigation. That year, U.S. Steel was one of several lead petitioners in protracted litigations before the U.S. Department of Commerce and U.S. International Trade Commission involving imports of (a) oil country tubular goods ("OCTG"), which are steel piping used by oil and gas companies; and (b) seamless standard line pipes ("SSLF"), which are steel pipes specifically constructed without a welded seam down the length of the pipes. In both cases, the Department of Commerce found that the respondents — various Chinese steel manufacturers including SOE-2 — received unfair subsidies from China and "dumped" billions of dollars' worth of steel into U.S. markets at prices below fair value. As a result, the Department of Commerce imposed significant countervailing and antidumping duties worth millions of dollars on Chinese imports of OCTG and SSLF. Thereafter, the amount of OCTG and SSLF steel imported by Chinese manufacturers fell dramatically.

30. In or about February 2010, while U.S. Steel was participating in at least the two international trade disputes described above, Defendants SUN and WANG hacked into U.S. Steel's computers.

   a. On or about February 8, 2010, approximately two weeks before the U.S. Department of Commerce was scheduled to release its preliminary determination in the SSLF trade dispute, Defendant SUN sent a spearphishing e-mail purporting to be from U.S. Steel's Chief Executive Officer to approximately 20 U.S. Steel employees affiliated with the U.S. Steel division responsible for OCTG and SSLF. The e-mail contained a link to malware, which some of the recipients clicked on, installing malware on computers located in the Western District of Pennsylvania and providing Defendant SUN and his co-conspirators with backdoor access to U.S. Steel's computers.

   b. On or about February 23, 2010, Defendant SUN sent spearphishing e-mails purporting to be from two U.S. Steel e-
mall accounts to approximately eight U.S. Steel employees, including U.S. Steel’s Chief Executive Officer. The e-mails had the subject line “US Steel Industry Outlook” and contained a link to malware that, once clicked, would surreptitiously install malware on the recipients’ computers, allowing the co-conspirators backdoor access to the company’s computers. Further, beginning on or about February 24, 2010 and continuing until on or about March 2, 2010, an unidentified co-conspirator sent approximately 49 spearphishing e-mails to U.S. Steel employees with the same subject, “US Steel Industry Outlook.”

c. On or about February 26, 2010, Defendant WANG gained unauthorized access to at least one U.S. Steel computer located in the Western District of Pennsylvania. Defendant WANG used that unauthorized access to steal hostnames and descriptions for more than 1,700 U.S. Steel computers, including servers used for emergency response, network monitoring, network security, applications for U.S. Steel employees’ mobile devices, and physical access to U.S. Steel’s facilities in the Western District of Pennsylvania. WANG then took steps to identify and exploit vulnerable servers on that list.

31. ATI is a large specialty metals company. It operates primarily in three business segments: high performance metals (e.g., nickel and cobalt), flat-rolled products (e.g., stainless steel), and engineered products (e.g., tungsten).

32. At times relevant to this Indictment, ATI had significant business interests relating to China, including as a partner with and competitor of various Chinese producers of flat-rolled products. For example, since approximately 1995, ATI, through a wholly owned subsidiary, has partnered in a joint venture with SOE-2 for the manufacture of precision rolled stainless steel strips, which are, among other things, used in the automotive, medical equipment, and semiconductor industries. The board of directors of this joint venture met periodically including, for example, on or about April 12, 2012, in Shanghai, China. That same ATI subsidiary competed with SOE-2 in the production of grain oriented flat-rolled electrical steel (“GOES”), which is used in power distribution and power generation transformers. In addition, beginning at least in or about June 2009 and continuing until at least in or about June 2012, ATI participated in an international trade dispute against SOE-2 regarding ATI’s importation of GOES into China, which the WTO ultimately resolved in ATI’s favor.

33. On or about April 13, 2012, the day after the joint venture board meeting, Defendant WEN gained unauthorized access into ATI computers located in the Western District of Pennsylvania. Defendant WEN then stole the usernames and
passwords for at least 7,000 ATI employees. These network credentials would have facilitated additional unauthorized access to ATI’s computers by Defendant WEN and his co-conspirators, allowing them to monitor activity on those systems and to steal ATI’s information in the future.

34. Thereafter, on at least three occasions in or about May 2012, several of the same compromised ATI computers beaconed to the same hop point used to steal those network credentials, reflecting persistent access by the hackers.

USW

35. USW has approximately one million active and retired members nationwide from a variety of industries including metals, energy, and rubber and plastics. One of USW’s core missions is to oppose Chinese trade practices that it perceives as unfair. USW’s trade strategy includes representing its members in international trade disputes, media campaigns, and lobbying. On at least four occasions between in or about 2010 and 2012 — while USW was particularly vocal about China’s trade practices — Defendant WEN and an unidentified co-conspirator gained unauthorized access to USW’s computers and stole e-mail messages and attachments from the accounts of six to eight USW employees who would be expected to have sensitive, non-public, and deliberative information about USW’s trade strategy concerning China. Each theft targeted messages from a narrow window of time before the intrusion.

36. For example, in or about late January 2012, USW was involved in public disputes over Chinese trade practices in at least two industries, raw materials and auto parts. First, on or about January 30, 2012, the Appellate Body of the WTO issued a report concluding that Chinese trade practices relating to the export of various industrial raw materials were inconsistent with China’s obligations as a member of the WTO. In response and on the same day, USW issued a press release stating that the decision was “a huge victory for American workers.” And the next day, on or about January 31, 2012, USW issued a statement from its International President, calling on the U.S. Government to take action to protect the U.S. auto parts sector from “China’s predatory, protectionist and illegal trade practices.” USW also released a report on Chinese trade practices in the auto parts industry.

37. That same day, on or about January 31, 2012, Defendant WEN gained unauthorized access to USW’s computers, and stole e-mails dated between in or about January 24 and January 31, 2012 that were located in certain folders of the accounts of six senior USW employees, including USW’s International President, most of whom were personally and publicly involved in either the raw materials or auto parts disputes. The stolen e-mails
included sensitive, non-public, and deliberative information about USW’s strategy including, for example, USW’s preparations for the January 31, 2012 news conference where it issued its “call to action” against Chinese trade practices in the auto parts sector; discussion of the merits of the January 31, 2012 WTO report on raw materials; and drafts of press releases announcing that report.

38. Then, on or about March 5, 2012, the International President of USW issued an open letter urging Congress to pass a bill that would grant the U.S. Department of Commerce authority to impose countervailing duties on Chinese exports, stating “[i]t would be a travesty for Congress to stand idle while a country like China . . . can provide lavish subsidies for exports without the United States being able to defend American workers and producers by offsetting the harm.” Approximately two days later, on or about March 7, 2012, Defendant WEN again gained unauthorized access to USW’s computers and stole e-mails received between March 1 and March 7, 2012 from the inboxes of six senior USW employees, including USW’s International President. Those e-mails included sensitive, non-public, and deliberative information about USW’s trade strategy, such as internal discussions of how USW would change its strategy in pending international trade disputes if the bill were enacted, and the union’s decision not to seek an extension of certain tariffs against Chinese companies, which USW had not yet announced.

39. Thereafter, until at least in or about January 2013, USW computers continued to beacon to malicious domains used by the conspiracy on a near daily basis, reflecting persistent access by the co-conspirators to USW’s computers.

Alcoa

40. Alcoa is the largest aluminum company in the United States. At times relevant to this Indictment, Alcoa had significant business interests relating to China. For example, in or about 2001, Alcoa entered into an agreement with a Chinese SOE in the aluminum industry (“SOE-3”) to purchase shares in a Chinese aluminum company that SOE-3 partially owned. Alcoa sold those shares on or about September 12, 2007. Then, on or about February 1, 2008, Alcoa announced a partnership with SOE-3 to acquire a substantial stake in a foreign mining company.

41. Spearphishing activity targeted Alcoa including near in time to significant events in its business relationship with SOE-3. For example, on or about February 20, 2008, about three weeks after Alcoa announced the partnership with SOE-3, Defendant SUN targeted Alcoa with a spearphishing campaign. Specifically, Defendant SUN sent e-mails to approximately 19 senior Alcoa employees, at least some of whom were located in the Western District of Pennsylvania, using an account designed
to impersonate a member of Alcoa’s Board of Directors. In all but one of the e-mails, Defendant SUN attached a file disguised as an agenda for Alcoa’s annual shareholders meeting, which, once opened, would install malware on the recipients’ computers.

42. Thereafter, in or about June 2008, unidentified individuals stole at least 2,907 e-mail messages along with approximately 863 attachments from Alcoa’s computers, including internal messages among Alcoa senior managers discussing the foregoing acquisition.

STATUTORY ALLEGATIONS

43. Beginning at least in or about 2006 and continuing until at least in or about April 2014, the exact dates being unknown to the Grand Jury, in the Western District of Pennsylvania and elsewhere, Defendants

WANG DONG,
a/k/a “Jack Wang,”
a/k/a “Ugly Gorilla,”
SUN KAILIANG,
a/k/a “Sun Kai Liang,”
a/k/a “Jack Sun,”
WEI XINYU,
a/k/a “Wen Xin Yu,”
a/k/a “WinXYHappy,”
a/k/a “Win_XY,”
a/k/a “Lao Wen,”
HUANG ZHENYU,
a/k/a “Huang Zhen Yu,”
a/k/a “hzy_lhx,” and
GU CHUNHUI,
a/k/a “Gu Chun Hui,”
a/k/a “KandyGoo,”

did knowingly and intentionally combine, conspire, confederate, and agree together, with each other and with others known and unknown to the Grand Jury, to commit offenses against the United States, namely:

a. to access a computer without authorization and exceed authorized access to a computer, and to obtain thereby information from a protected computer, for the purpose of commercial advantage and private financial gain, and in furtherance of a criminal and tortious act in violation of the laws of the Commonwealth of Pennsylvania, namely, the common law tort of Invasion of Privacy, and where the value of the information did, and would if completed, exceed $5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B); and

b. to cause the transmission of a program, information, code, and command, and as a result of such conduct, to cause damage without authorization to a protected computer, and where the offense did cause and would, if completed, have caused, loss aggregating $5,000 in value to at least one person during a one-year period from a related course of conduct affecting a protected computer, and damage affecting at least 10 protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B).
OVERT ACTS

44. In furtherance of the conspiracy and to achieve the objects thereof, the conspirators committed the following overt acts, among others, in the Western District of Pennsylvania and elsewhere:

a. On or about April 18, 2006, Defendant SUN created e-mail account c******@yahoo.com.

b. On or about July 17, 2006, Defendant SUN created domain account j****r at a domain provider in the United States.

c. On or about December 12, 2006, Defendant WEN sent Defendant WANG two executable files containing tools that would be useful for intrusions.

d. On or about July 12, 2007, Defendant GU designed and tested a spearphishing message.

e. On or about February 20, 2008, Defendant SUN created an e-mail account using the misspelled name of a person with the initials C.G., who was then a member of Alcoa's Board of Directors (the "C.G. Spearphishing Account").

f. On or about February 20, 2008, Defendant SUN, using the C.G. Spearphishing Account, transmitted e-mail messages with a file named "agenda.zip," which contained malware, to approximately 19 Alcoa employees.

g. On or about October 26, 2008, Defendant GU designed and tested a spearphishing message.

h. On or about February 8, 2010, Defendant SUN sent a spearphishing e-mail purporting to be from U.S. Steel's Chief Executive Officer to approximately 20 U.S. Steel employees.

i. On or about February 23, 2010, Defendant SUN sent spearphishing e-mails purporting to be from two U.S. Steel e-mail accounts to approximately eight U.S. Steel employees.

j. On or about February 26, 2010, Defendant WANG accessed without authorization at least one U.S. Steel computer located in the Western District of Pennsylvania.

k. On or about February 26, 2010, Defendant WANG stole server names and descriptions from a U.S. Steel computer located in the Western District of Pennsylvania.

l. On or about February 26, 2010, Defendant WANG transmitted at least one file that he stole from a U.S. Steel computer to a computer located in China.

m. On or about February 26, 2010, Defendant WANG transmitted a file named "ccapp.exe" to a U.S. Steel computer.

n. On or about May 6, 2010, Defendant SUN accessed without authorization a Westinghouse computer located in the Western District of Pennsylvania with hostname L*****0.

o. On or about May 6, 2010, Defendant SUN transmitted a file named "ccapp.exe" to a Westinghouse computer.
located in the Western District of Pennsylvania with hostname L*****9.

p. On or about May 6, 2010, Defendant SUN transmitted a file named "ccapp.exe" to a Westinghouse computer with the hostname W*****9.

q. On or about May 6, 2010, Defendant SUN stole at least one file from a Westinghouse computer with hostname W*****9.

r. On or about August 24, 2010, Defendant WEN sent a test spearphishing e-mail to Defendant SUN.

s. On or about December 30, 2010, Defendant SUN accessed the malicious domain account "purpledaily.com" and changed the IP address of sub-domain "klwest.purpledaily.com" to a hop point located in Kansas.

t. On or about December 30, 2010, Defendant SUN accessed without authorization a Westinghouse computer with hostname L*****9.

u. On or about December 30, 2010, Defendant SUN transmitted a file named "ccapp.exe" to a Westinghouse computer with hostname L*****9.

v. On or about December 30, 2010, Defendant SUN transmitted at least two files named "wiam.exe" and "ccapp.exe" to a Westinghouse computer located in the Western District of Pennsylvania with hostname T*****9.

w. On or about December 30, 2010, Defendant SUN stole e-mails from the accounts of six Westinghouse employees.


y. On or about January 3, 2011, Defendant SUN transmitted a file named "ccapp.exe" to a Westinghouse computer with hostname W*****9.

z. On or about January 3, 2011, Defendant SUN transmitted a file named "ccapp.exe" to a Westinghouse computer located in the Western District of Pennsylvania with hostname T*****9.

aa. On or about January 3, 2011, Defendant SUN stole e-mails from the accounts of six Westinghouse employees.

bb. On or about January 5, 2011, Defendant SUN accessed the malicious domain account "bigish.net" and changed the IP address assigned to two bigish.net sub-domains, including "finekl.bigish.net," to a hop point located in Kansas.

cc. On or about January 5, 2011, Defendant SUN accessed without authorization a Westinghouse computer located in the Western District of Pennsylvania with hostname L*****4.

dd. On or about January 5, 2011, Defendant SUN transmitted files named "wiam.exe" and "ccapp.exe" to a
Westinghouse computer located in the Western District of Pennsylvania with hostname L*****4.

ee. On or about January 5, 2011, Defendant SUN transmitted files named "wiam.exe" and "ccapp.exe" to a Westinghouse computer with hostname L*****5.

ff. On or about January 5, 2011, Defendant SUN stole e-mails from the accounts of six Westinghouse employees.


hh. On or about January 31, 2012, Defendant WEN transmitted a file named "ccapp.exe" to a USW computer located in the Western District of Pennsylvania with hostname J***********6.

ii. On or about January 31, 2012, Defendant WEN stole hundreds of e-mails from the accounts of six USW employees.

jj. On or about March 7, 2012, Defendant WEN accessed without authorization a USW computer located in the Western District of Pennsylvania with hostname L***********8.

kk. On or about March 7, 2012, Defendant WEN transmitted a file named "gu.exe" to a USW computer.

ll. On or about March 7, 2012, Defendant WEN stole hundreds of e-mails from the accounts of six USW employees.

mm. On or about April 12, 2012, Defendant WEN accessed without authorization an ATI computer located in the Western District of Pennsylvania with hostname L*****3.

nn. On or about April 12, 2012, Defendant WEN executed the program named "ugls.exe" to monitor the status of compromised ATI computers located in the Western District of Pennsylvania and elsewhere.

oo. On or about April 13, 2012, Defendant WEN accessed without authorization an ATI computer located in the Western District of Pennsylvania with hostname A*****5.

pp. On or about April 13, 2012, Defendant WEN transmitted a file named "ccapp.exe" to an ATI computer located in the Western District of Pennsylvania with hostname A********7.

qq. On or about April 13, 2012, Defendant WEN transmitted a file named "i.exe" to an ATI computer located in the Western District of Pennsylvania with hostname A*****0.

rr. On or about April 13, 2012, Defendant WEN stole ATI network usernames and passwords for more than 7,000 ATI employees.

ss. On or about May 3, 2012, Defendant WEN accessed without authorization a SolarWorld computer using malware named "ugls.exe" and stole e-mails and files belonging to three employees.

tt. On or about May 9, 2012, Defendant WEN accessed
without authorization a SolarWorld computer using malware named "ucls.exe" and stole e-mails and files belonging to four employees.

uu. On or about July 27, 2012, Defendant WEN accessed without authorization a SolarWorld computer using malware named "ucls.exe" and stole e-mails and files belonging to five employees.

vv. On or about February 20, 2013, WEN changed the registration information for malicious domain accounts "arrowservice.net," "businessconsults.net," "newsonet.net," and "purpledaily.com," and "marsbrother.com."

ww. In or about April 2014, an unidentified co-conspirator created a malicious domain and configured it to resolve to an IP address in Germany.

All in violation of Title 18, United States Code, Section 1030(b).

COUNTS TWO THROUGH NINE
(Computer Fraud and Abuse)

The Grand Jury further charges:

45. The allegations set forth in paragraphs 1-42 and 44 of this indictment are incorporated herein as if set forth in full.

46. Beginning at least on or about February 26, 2010 and continuing until at least on or about April 13, 2012, in the Western District of Pennsylvania and elsewhere, Defendants

WANG DONG,
a/k/a "Jack Wang,"
a/k/a "UglyGorilla,"
SUN KAILIANG,
a/k/a "Sun Kai Liang,"
a/k/a "Jack Sun,"
WEN XINYU,
a/k/a "Wen Xin Yu,"
a/k/a "WinXYHappy,"
a/k/a "Win_XY,"
a/k/a "Lao Wen,"
HUANG ZHENYU,
a/k/a "Huang Zhen Yu,"
a/k/a "hzylhx,"
and
GU CHENHUI,
a/k/a "Gu Chun Hui,"
a/k/a "KandyGoo,"

aided and abetted by others known and unknown to the Grand Jury, did intentionally access a computer without authorization and exceed authorized access to a computer, and did thereby obtain and attempt to obtain information from a protected computer, for the purpose of commercial advantage and private financial gain, in furtherance of a criminal and tortious act in violation of the laws of Pennsylvania, namely, Invasion of Privacy, and where
the value of the information obtained exceeded, and if completed, would have exceeded, $5,000.

47. On or about the dates identified in Column B of the chart set forth below, each date constituting a separate count as set forth in Column A, Defendants WANG, SUN, WEN, HUANG, and GU, accessed without authorization, and exceeded authorized access to, at least one protected computer belonging to the victim listed in Column C, which was located in the Western District of Pennsylvania, using a computer located outside of the Commonwealth of Pennsylvania. As a result of such unauthorized access and exceeding authorized access, Defendants WANG, SUN, WEN, HUANG, and GU obtained the information listed in Column D.

<table>
<thead>
<tr>
<th>A Count</th>
<th>B Date (On or About)</th>
<th>C Victim</th>
<th>D Stolen Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2/26/2010</td>
<td>U.S. Steel</td>
<td>Information about 1,753 U.S. Steel computers.</td>
</tr>
<tr>
<td>3</td>
<td>5/6/2010</td>
<td>Westinghouse</td>
<td>Proprietary and confidential files related to the AP1000 nuclear power plant.</td>
</tr>
<tr>
<td>4</td>
<td>12/30/2010</td>
<td>Westinghouse</td>
<td>Information from e-mail accounts of Westinghouse employees A.C., D.C., X.L., R.P., W.P., and C.P.</td>
</tr>
<tr>
<td>5</td>
<td>1/3/2011</td>
<td>Westinghouse</td>
<td>Information from e-mail accounts of Westinghouse employees A.C., D.C., X.L., R.P., W.P., and C.P.</td>
</tr>
<tr>
<td>6</td>
<td>1/5/2011</td>
<td>Westinghouse</td>
<td>Information from e-mail accounts of Westinghouse employees A.C., D.C., X.L., R.P., W.P., and C.P.</td>
</tr>
</tbody>
</table>

All in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030 (c)(2)(B)(i)-(iii), and 2.
COUNTS TEN THROUGH TWENTY-THREE
(Damaging a Computer)

The Grand Jury further charges:

46. The allegations set forth in paragraphs 1-42 and 44 of this Indictment are incorporated herein as if set forth in full.

49. Beginning at least on or about February 8, 2010 and continuing until at least on or about April 13, 2012, in the Western District of Pennsylvania and elsewhere, Defendants

WANG DONG,
a/k/a “Jack Wang,”
a/k/a “UglyGorilla,”
SUN KAILIANG,
a/k/a “Sun Kai Liang,”
a/k/a “Jack Sun,”
WEN XINYU,
a/k/a “Wen Xin Yu,”
a/k/a “WinXYHappy,”
a/k/a “Win_XY,”
a/k/a “Lao Wen,”
HUANG ZHENYU,
a/k/a “Huang Zhen Yu,”
a/k/a “hz_y_hx,” and
GU CHUNHUI,
a/k/a “Gu Chun Hui,”
a/k/a “KandyGoo,”

aided and abetted by others known and unknown to the Grand Jury, did knowingly cause and attempt to cause the transmission of a program, information, code, and command, and, as a result of such conduct, did intentionally cause damage and attempt to cause damage without authorization to a protected computer, and which offense caused, and would, if completed, have caused, loss aggregating at least $5,000 in value to at least one person during a one-year period from a related course of conduct, and damage affecting at least ten protected computers during a one-year period.

50. On or about the dates identified in Column B of the chart set forth below, each date constituting a separate count as set forth in Column A, Defendants WANG, SUN, WEN, HUANG, and GU did knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, did intentionally cause damage and attempt to cause damage without authorization to a protected computer belonging to the victim listed in Column C. Each offense caused and would, if completed, have caused loss aggregating at least $5,000 in value to at least one person during a one-year period from a related course of conduct, and damage affecting at least ten protected computers during a one-year period. A summary of the method of transmission of the malicious program, information, code, and command is listed in Column D.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Count</td>
<td>Date (On or About)</td>
<td>Victim</td>
<td>Description of Transmission</td>
</tr>
<tr>
<td>10</td>
<td>2/8/2010</td>
<td>U.S. Steel</td>
<td>Spearphishing e-mail to U.S. Steel employee R.G. with subject “Westing Invitation,” which contained the malicious file “agenda.zip.”</td>
</tr>
<tr>
<td>11</td>
<td>5/6/2010</td>
<td>Westinghouse</td>
<td>Transfer of at least one malicious program, information, code, and command to a Westinghouse computer with hostname</td>
</tr>
<tr>
<td>Count</td>
<td>Date</td>
<td>Victim</td>
<td>Description of Transmission</td>
</tr>
<tr>
<td>-------</td>
<td>----------</td>
<td>--------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>12</td>
<td>5/6/2010</td>
<td>Westinghouse</td>
<td>Transfer of at least one malicious program, information, code, and command to a Westinghouse computer with hostname W****9.</td>
</tr>
<tr>
<td>13</td>
<td>12/30/2010</td>
<td>Westinghouse</td>
<td>Transfer of at least one malicious program, information, code, and command to a Westinghouse computer with hostname W****9.</td>
</tr>
<tr>
<td>14</td>
<td>12/30/2010</td>
<td>Westinghouse</td>
<td>Transfer of at least one malicious program, information, code, and command to a Westinghouse computer with hostname W****9.</td>
</tr>
<tr>
<td>15</td>
<td>1/3/2011</td>
<td>Westinghouse</td>
<td>Transfer of at least one malicious program, information, code, and command to a Westinghouse computer with hostname W****9.</td>
</tr>
<tr>
<td>16</td>
<td>1/3/2011</td>
<td>Westinghouse</td>
<td>Transfer of at least one malicious program, information, code, and command to a Westinghouse computer with hostname W****9.</td>
</tr>
<tr>
<td>17</td>
<td>1/5/2011</td>
<td>Westinghouse</td>
<td>Transfer of at least one malicious program, information, code, and command to a Westinghouse computer with hostname W****9.</td>
</tr>
<tr>
<td>18</td>
<td>1/5/2011</td>
<td>Westinghouse</td>
<td>Transfer of at least one malicious program, information, code, and command to a Westinghouse computer with hostname W****9.</td>
</tr>
<tr>
<td>19</td>
<td>1/31/2012</td>
<td>USW</td>
<td>Transfer of at least one malicious program, information, code, and command to a USW computer with hostname USW****9.</td>
</tr>
<tr>
<td>20</td>
<td>3/7/2012</td>
<td>USW</td>
<td>Transfer of at least one malicious program, information, code, and command to a USW computer with hostname USW****9.</td>
</tr>
<tr>
<td>21</td>
<td>4/13/2012</td>
<td>ATI</td>
<td>Transfer of at least one malicious program, information, code, and command to an ATI computer with hostname A****7.</td>
</tr>
<tr>
<td>22</td>
<td>4/13/2012</td>
<td>ATI</td>
<td>Transfer of at least one malicious program, information, code, and command to an ATI computer with hostname A****7.</td>
</tr>
<tr>
<td>23</td>
<td>4/13/2012</td>
<td>ATI</td>
<td>Transfer of at least one malicious program, information, code, and command to an ATI computer with hostname A****7.</td>
</tr>
</tbody>
</table>

All in violation of Title 18, United States Code, Section 1030(a)(5)(A) and 1030(c)(4)(B), and 2.
COUNTS TWENTY-FOUR THROUGH TWENTY-NINE
(Aggravated Identity Theft)

The Grand Jury further charges:

51. The allegations set forth in paragraphs 1-42 and 44 of this Indictment are incorporated herein as if set forth in full.

52. Beginning at least on or about December 30, 2010 and continuing until at least on or about April 12, 2012, in the Western District of Pennsylvania and elsewhere, Defendants KANG DONG,

a/k/a "Jack Wang," 

a/k/a "UglyGorilla," 

SUN KAILIANG, 

a/k/a "Sun Kai Liang," 

a/k/a "Jack Sun," 

WEN XINYU, 

a/k/a "Wen Xin Yu," 

a/k/a "WinXYHappy," 

a/k/a "Win_XY," 

a/k/a "Lao Wen," 

HUANG ZHENYU, 

a/k/a "Huang Zhen Yu," 

a/k/a "hzy_lhx," and 

GU CHUNHUI, 

a/k/a "Gu Chun Hai," 

a/k/a "KandyGoo," aided and abetted by others known and unknown to the Grand Jury, during and in relation to the crime of conspiracy to commit computer fraud in violation of Title 18, United States Code, Section 1030(b), as more fully set forth in Count One above, did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person.

53. On or about the dates identified in Column B of the chart set forth below, each date constituting a separate count as set forth in Column A, Defendants did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, listed by initials in Column C, who was associated with a victim listed in Column D.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>12/30/2010</td>
<td>D.C.</td>
<td>Westinghouse</td>
</tr>
<tr>
<td>25</td>
<td>1/3/2011</td>
<td>D.C.</td>
<td>Westinghouse</td>
</tr>
<tr>
<td>26</td>
<td>1/5/2011</td>
<td>L.G.</td>
<td>GEW</td>
</tr>
<tr>
<td>27</td>
<td>1/3/2012</td>
<td>L.G.</td>
<td>USW</td>
</tr>
<tr>
<td>28</td>
<td>3/7/2012</td>
<td>P.V.</td>
<td>ATI</td>
</tr>
</tbody>
</table>

All in violation of Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028A(c)(4), and 2.
COUNT THIRTY
(Economic Espionage)

The Grand Jury further charges:

54. The allegations set forth in paragraphs 1-42 and 44 of this Indictment are incorporated herein as if set forth in full.

55. On or about May 6, 2010, in the Western District of Pennsylvania and elsewhere, Defendants

WANG DONG,
a/k/a “Jack Xiang,”
a/k/a “UglyGorilla,”

SUN KALIANG,
a/k/a “Sun Kai Liang,”
a/k/a “Jack Sun,”

WEN XINYU,
a/k/a “Wen Xin Yu,”
a/k/a “WinXYHappy,”
a/k/a “Win XY,”
a/k/a “Lao Wen,”

HUANG ZHENYU,
a/k/a “Huang Zhen Yu,”
a/k/a “hzy_lhx,” and

GU CHUNHUI,
a/k/a “Gu Chun Hui,”
a/k/a “RandyGoo,”

aided and abetted by others unknown to the Grand Jury, intending and knowing that the offense would benefit a foreign government, instrumentality, and agent, namely China, did knowingly and without authorization copy, download, upload, replicate, transmit, deliver, send, mail, communicate, and convey a trade secret, and did attempt to do so, specifically a file named “wd.rac” containing proprietary and confidential technical and design specifications, owned by Westinghouse, which were related
to the pipes, pipe supports, and pipe routing within the AP1000 nuclear power plant.

All in violation of Title 18, United States Code, Sections 1831(a)(2) & (a)(4), and 2.
COUNT THIRTY-ONE
(Theft of a Trade Secret)

The Grand Jury further charges:

56. The allegations set forth in paragraphs 1-42 and 44 of this Indictment are incorporated herein as if set forth in full.

57. On or about May 6, 2010, in the Western District of Pennsylvania and elsewhere, Defendants

WANG DONG,
   a/k/a “Jack Wang,”
   a/k/a “Diplomat,”
   a/k/a “Sun Kai Liang,”
   a/k/a “Sun Kai Liang,”
   SUN KAILIANG,
   a/k/a “Sun Kai Liang,”
   a/k/a “Jack Sun,”
   WEN XINYU,
   a/k/a “Wen Xin Yu,”
   a/k/a “WinXYHappy,”
   a/k/a “Win XY,”
   a/k/a “Luo Wen,”
   HUANG ZHENYU,
   a/k/a “Huang Zhen Yu,”
   a/k/a “hey_lex,” and
   GU CHUNHUI,
   a/k/a “Gu Chun Hui,”
   a/k/a “KandyGoo,”

aided and abetted by others unknown to the Grand Jury, with the intent to convert a trade secret to the economic benefit of someone other than Westinghouse, and intending and knowing that the offense would injure Westinghouse, did knowingly and without authorization copy, duplicate, download, upload, replicate, transmit, deliver, send, mail, communicate, and convey a trade secret, and attempt to do so, specifically, a file named “wd.rar” containing proprietary and confidential technical and design specifications, owned by Westinghouse, which were related to the pipes, pipe supports, and pipe routing in a product, namely the AP1000 nuclear power plant, that was produced for and placed in interstate and foreign commerce.

All in violation of Title 18, United States Code, Sections 1832(a)(2) & (a)(4) and 2.

A true bill,

POREPERSON

DAVID J. RICKERT
United States Attorney
PR 13 No. 34524
EXHIBIT A

Wang Dong
a/k/a "Jack Wang,"
a/k/a "UglyGorilla"

EXHIBIT B

SUN KAILIANG,
a/k/a "Sun Kai Liang,"
a/k/a "Jack Sun"
EXHIBIT C

WEN XINYU,
a/k/a "Wen Xin Yu,"
a/k/a "WinXYHappy,"
a/k/a "Win_XY,"
a/k/a "Lao Wen"

EXHIBIT D

HUANG ZHENYU,
a/k/a "Huang Zhen Yu,"
a/k/a "hzy_lhx"
Exhibit D

2000-2013
For tort damages used by competitors at one time
Dynamic DNS provider

Conspirator Domain Re-assignments (‘on’)

Gu Chunhui,
also known as "Chun Hui," and/or "TandyGuo"
Remarks Prepared for Delivery by James B. Comey
Director, Federal Bureau of Investigation
Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?
Brookings Institution, Washington, D.C.
October 16, 2014

Good morning. It’s an honor to be here.

I have been on the job as FBI Director for one year and one month. I like to express my tenure in terms of months, and I joke that I have eight years and 11 months to go, as if I’m incarcerated. But the truth is, I love this job, and I wake up every day excited to be part of the FBI.

Over the past year, I have confirmed what I long believed – that the FBI is filled with amazing people, doing an amazing array of things around the world, and doing them well. I have also confirmed what I have long known: that a commitment to the rule of law and civil liberties is at the core of the FBI. It is the organization’s spine.

But we confront serious threats – threats that are changing every day. So I want to make sure I have every lawful tool available to keep you safe from those threats.

An Opportunity to Begin a National Conversation

I wanted to meet with you to talk in a serious way about the impact of emerging technology on public safety. And within that context, I think it’s important to talk about the work we do in the FBI, and what we need to do the job you have entrusted us to do.

There are a lot of misconceptions in the public eye about what we in the government collect, and the capabilities we have for collecting information.

My job is to explain and clarify where I can with regard to the work of the FBI. But at the same time, I want to get a better handle on your thoughts, because those of us in law enforcement can’t do what we need to do without your trust and your support. We have no monopoly on wisdom.

My goal today isn’t to tell people what to do. My goal is to urge our fellow citizens to participate in a conversation as a country about where we are, and where we want to be, with respect to the authority of law enforcement.
The Challenge of Going Dark

Technology has forever changed the world we live in. We’re online, in one way or another, all day long. Our phones and computers have become reflections of our personalities, our interests, and our identities. They hold much that is important to us.

And with that comes a desire to protect our privacy and our data – you want to share your lives with the people you choose. I sure do. But the FBI has a sworn duty to keep every American safe from crime and terrorism, and technology has become the tool of choice for some very dangerous people.

Unfortunately, the law hasn’t kept pace with technology, and this disconnect has created a significant public safety problem. We call it “Going Dark,” and what it means is this: Those charged with protecting our people aren’t always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so.

We face two overlapping challenges. The first concerns real-time court-ordered interception of what we call “data in motion,” such as phone calls, email, and live chat sessions. The second challenge concerns court-ordered access to data stored on our devices, such as email, text messages, photos, and videos – or what we call “data at rest.” And both real-time communication and stored data are increasingly encrypted.

Let’s talk about court-ordered interception first, and then we’ll talk about challenges posed by different means of encryption.

In the past, conducting electronic surveillance was more straightforward. We identified a target phone being used by a bad guy, with a single carrier. We obtained a court order for a wiretap, and, under the supervision of a judge, we collected the evidence we needed for prosecution.

Today, there are countless providers, countless networks, and countless means of communicating. We have laptops, smart phones, and tablets. We take them to work and to school, from the soccer field to Starbucks, over many networks, using any number of apps. And so do those conspiring to harm us. They use the same devices, the same networks, and the same apps to make plans, to target victims, and to cover up what they’re doing. And that makes it tough for us to keep up.
If a suspected criminal is in his car, and he switches from cellular coverage to Wi-Fi, we may be out of luck. If he switches from one app to another, or from cellular voice service to a voice or messaging app, we may lose him. We may not have the capability to quickly switch lawful surveillance between devices, methods, and networks. The bad guys know this; they’re taking advantage of it every day.

In the wake of the Snowden disclosures, the prevailing view is that the government is sweeping up all of our communications. That is not true. And unfortunately, the idea that the government has access to all communications at all times has extended — unfairly — to the investigations of law enforcement agencies that obtain individual warrants, approved by judges, to intercept the communications of suspected criminals.

Some believe that the FBI has these phenomenal capabilities to access any information at any time — that we can get what we want, when we want it, by flipping some sort of switch. It may be true in the movies or on TV. It is simply not the case in real life.

It frustrates me, because I want people to understand that law enforcement needs to be able to access communications and information to bring people to justice. We do so pursuant to the rule of law, with clear guidance and strict oversight. But even with lawful authority, we may not be able to access the evidence and the information we need.

Current law governing the interception of communications requires telecommunication carriers and broadband providers to build interception capabilities into their networks for court-ordered surveillance. But that law, the Communications Assistance for Law Enforcement Act, or CALEA, was enacted 20 years ago — a lifetime in the Internet age. And it doesn’t cover new means of communication. Thousands of companies provide some form of communication service, and most are not required by statute to provide lawful intercept capabilities to law enforcement.

What this means is that an order from a judge to monitor a suspect’s communication may amount to nothing more than a piece of paper. Some companies fail to comply with the court order. Some can’t comply, because they have not developed interception capabilities. Other providers want to provide assistance, but they have to build interception capabilities, and that takes time and money.

The issue is whether companies not currently subject to the Communications Assistance for Law Enforcement Act should be required to build lawful intercept capabilities for law enforcement. We aren’t seeking to expand our authority to intercept communications. We are struggling to keep up with changing technology, and to maintain our ability to actually collect the communications we are authorized to intercept.
And if the challenges of real-time interception threaten to leave us in the dark, encryption threatens to lead all of us to a very dark place.

Encryption is nothing new. But the challenge to law enforcement and national security officials is markedly worse, with recent default encryption settings and encrypted devices and networks – all designed to increase security and privacy.

With Apple's new operating system, the information stored on many iPhones and other Apple devices will be encrypted by default. Shortly after Apple's announcement, Google announced plans to follow suit with its Android operating system. This means the companies themselves won't be able to unlock phones, laptops, and tablets to reveal photos, documents, email, and recordings stored within.

Both companies are run by good people, responding to what they perceive is a market demand. But the place they are leading us is one we shouldn't go to without careful thought and debate as a country.

At the outset, Apple says something that is reasonable – that it's not that big a deal. Apple argues, for example, that its users can back-up and store much of their data in "the cloud," and that the FBI can still access that data with lawful authority. But uploading to the cloud doesn't include all of the stored data on a bad guy's phone, which has the potential to create a black hole for law enforcement.

And if the bad guys don't back up their phones routinely, or if they opt out of uploading to the cloud, the data will only be found on the encrypted devices themselves. And it is people most worried about what's on the phone who will be most likely to avoid the cloud, and to make sure that law enforcement cannot access incriminating data.

Encryption isn't just a technical feature; it's a marketing pitch. But it will have very serious consequences for law enforcement and national security agencies at all levels. Sophisticated criminals will come to count on these means of evading detection. It's the equivalent of a closet that can't be opened. A safe that can't be cracked. And my question is, at what cost?

**Correcting Misconceptions**

Some argue that we will still have access to metadata, which includes telephone records and location information from telecommunications carriers. That is true. But metadata doesn't provide the content of any communication. It's incomplete information, and even this is difficult to access when time is of the essence. I wish we had time in our work, especially when lives are on the line. We usually don't.
There is a misconception that building a lawful intercept solution into a system requires a so-called "back door," one that foreign adversaries and hackers may try to exploit.

But that isn’t true. We aren’t seeking a back-door approach. We want to use the front door, with clarity and transparency, and with clear guidance provided by law. We are completely comfortable with court orders and legal process – front doors that provide the evidence and information we need to investigate crime and prevent terrorist attacks.

Cyber adversaries will exploit any vulnerability they find. But it makes more sense to address any security risks by developing intercept solutions during the design phase, rather than resorting to a patchwork solution when law enforcement comes knocking after the fact. And with sophisticated encryption, there might be no solution, leaving the government at a dead end — all in the name of privacy and network security.

Another misperception is that we can somehow guess the password or break into the phone with a so-called "brute force" attack. Even a supercomputer would have difficulty with today’s high-level encryption, and some devices have a setting whereby the encryption key is erased if someone makes too many attempts to break the password, meaning no one can access that data.

Finally, a reasonable person might also ask, “Can’t you just compel the owner of the phone to produce the password?” Likely, no. And even if we could compel them as a legal matter, if we had a child predator in custody, and he could choose to sit quietly through a 30-day contempt sentence for refusing to comply with a court order to produce his password, or he could risk a 30-year sentence for production and distribution of child pornography, which do you think he would choose?

Case Examples

Think about life without your smartphone, without Internet access, without texting or email or the apps you use every day. I’m guessing most of you would feel rather lost and left behind. Kids call this FOMO, or “Fear of Missing Out.”

With Going Dark, those of us in law enforcement and public safety have a major fear of missing out — missing out on predators who exploit the most vulnerable among us ... missing out on violent criminals who target our communities ... missing out on a terrorist cell using social media to recruit, plan, and execute an attack.
Criminals and terrorists would like nothing more than for us to miss out. And the more we as a society rely on these devices, the more important they are to law enforcement and public safety officials. We have seen case after case – from homicides and car crashes to drug trafficking, domestic abuse, and child exploitation – where critical evidence came from smartphones, hard drives, and online communication.

Let’s just talk about cases involving the content of phones.

In Louisiana, a known sex offender posed as a teenage girl to entice a 12-year-old boy to sneak out of his house to meet the supposed young girl. This predator, posing as a taxi driver, murdered the young boy, and tried to alter and delete evidence on both his and the victim’s cell phones to cover up his crime. Both phones were instrumental in showing that the suspect enticed this child into his taxi. He was sentenced to death in April of this year.

In Los Angeles, police investigated the death of a two-year-old girl from blunt force trauma to her head. There were no witnesses. Text messages stored on her parents' cell phones to one another, and to their family members, proved the mother caused this young girl’s death, and that the father knew what was happening and failed to stop it. Text messages stored on these devices also proved that the defendants failed to seek medical attention for hours while their daughter convulsed in her crib. They even went so far as to paint her tiny body with blue paint – to cover her bruises – before calling 911. Confronted with this evidence, both parents pled guilty.

In Kansas City, the DEA investigated a drug trafficking organization tied to heroin distribution, homicides, and robberies. The DEA obtained search warrants for several phones used by the group. Text messages found on the phones outlined the group’s distribution chain and tied the group to a supply of lethal heroin that had caused 12 overdoses – and five deaths – including several high school students.

In Sacramento, a young couple and their four dogs were walking down the street at night when a car ran a red light and struck them – killing their four dogs, severing the young man’s leg, and leaving the young woman in critical condition. The driver left the scene, and the young man died days later. Using “red light cameras” near the scene of the accident, the California Highway Patrol identified and arrested a suspect and seized his smartphone. GPS data on his phone placed the suspect at the scene of the accident, and revealed that he had fled California shortly thereafter. He was convicted of second-degree murder and is serving a sentence of 25 years-to-life.

The evidence we find also helps exonerate innocent people. In Kansas, data from a cell phone was used to prove the innocence of several teens accused of rape. Without access to this phone, or the ability to recover a deleted video, several innocent young men could have been wrongly convicted.
These are cases in which we had access to the evidence we needed. But we're seeing more and more cases where we believe significant evidence is on that phone or a laptop, but we can't crack the password. If this becomes the norm, I would suggest to you that homicide cases could be stalled, suspects could walk free, and child exploitation might not be discovered or prosecuted. Justice may be denied, because of a locked phone, or an encrypted hard drive.

My Thoughts

I'm deeply concerned about this, as both a law enforcement officer and a citizen. I understand some of this thinking in a post-Snowden world, but I believe it is mostly based on a failure to understand why we in law enforcement do what we do, and how we do it.

I hope you know that I'm a huge believer in the rule of law. But I also believe that no one in this country should be above or beyond the law. There should be no law-free zone in this country. I like and believe very much that we need to follow the letter of the law to examine the contents of someone's closet or someone's cell phone. But the notion that the marketplace could create something that would prevent that closet from ever being opened, even with a properly obtained court order, makes no sense to me.

I think it's time to ask: Where are we, as a society? Are we no longer a country governed by the rule of law, where no one is above or beyond that law? Are we so mistrustful of government – and of law enforcement – that we are willing to let bad guys walk away ... willing to leave victims in search of justice?

There will come a day – and it comes every day in this business – where it will matter a great deal to innocent people that we in law enforcement can't access certain types of data or information, even with legal authorization. We have to have these discussions now.

I believe people should be skeptical of government power. I am. This country was founded by people who were worried about government power – who knew that you cannot trust people in power. So they divided government power among three branches, with checks and balances for each. And they wrote a Bill of Rights to ensure that the “papers and effects” of the people are secure from unreasonable searches.

But the way I see it, the means by which we conduct surveillance through telecommunication carriers and those Internet service providers who have developed lawful intercept solutions is an example of government operating in the way the founders intended – that is, the executive, the legislative, and the judicial branches proposing, enacting, executing, and overseeing legislation, pursuant to the rule of law.
Perhaps it’s time to suggest that the post-Snowden pendulum has swung too far in one direction – in a direction of fear and mistrust. It is time to have open and honest debates about liberty and security.

Some have suggested there is a conflict between liberty and security. I disagree. At our best, we in law enforcement, national security, and public safety are looking for security that enhances liberty. When a city posts police officers at a dangerous playground, security has promoted liberty – the freedom to let a child play without fear.

The people of the FBI are sworn to protect both security and liberty. It isn’t a question of conflict. We must care deeply about protecting liberty through due process of law, while also safeguarding the citizens we serve – in every investigation.

Where Do We Go From Here?

These are tough issues. And finding the space and time in our busy lives to understand these issues is hard. Intelligent people can and do disagree, and that’s the beauty of American life – that smart people can come to the right answer.

I’ve never been someone who is a scaremonger. But I’m in a dangerous business. So I want to ensure that when we discuss limiting the court-authorized law enforcement tools we use to investigate suspected criminals that we understand what society gains, and what we all stand to lose.

We in the FBI will continue to throw every lawful tool we have at this problem, but it’s costly. It’s inefficient. And it takes time.

We need to fix this problem. It is long past time.

We need assistance and cooperation from companies to comply with lawful court orders, so that criminals around the world cannot seek safe haven for lawless conduct. We need to find common ground. We care about the same things. I said it because I meant it. These companies are run by good people. And we know an adversarial posture won’t take any of us very far down the road.

We understand the private sector’s need to remain competitive in the global marketplace. And it isn’t our intent to stifle innovation or undermine U.S. companies. But we have to find a way to help these companies understand what we need, why we need it, and how they can help, while still protecting privacy rights and providing network security and innovation. We need our private sector partners to take a step back, to pause, and to consider changing course.
We also need a regulatory or legislative fix to create a level playing field, so that all communication service providers are held to the same standard, and so that those of us in law enforcement, national security, and public safety can continue to do the job you have entrusted us to do, in the way you would want us to.

Perhaps most importantly, we need to make sure the American public understands the work we do, and the means by which we do it.

I really do believe we can get there, with a reasoned and practical approach. And we have to get there together. I don’t have the perfect solution. But I think it’s important to start the discussion. I’m happy to work with Congress, with our partners in the private sector, with my law enforcement and national security counterparts, and with the people we serve, to find the right answer – to find the balance we need.

Thank you for having me here today.

###
Strikes in Syria: The International Law Framework

By Jennifer Daskal, Ashley Deeks and Ryan Goodman

Wednesday, September 24, 2014 at 2:25 AM

[Cross-posted at Just Security]

As is now well-known, the United States last night hit approximately 25 targets inside Syria, some of which were directed at ISIL, and some at a group that has only recently been brought to the public’s attention—the Khorasan Group, which is reportedly comprised of al Qaeda militants and led by senior al Qaeda officials from among Osama bin Laden’s inner circle. According to a letter submitted by the United States to the United Nations on Tuesday, the Administration is justifying the strikes against ISIL as a lawful exercise of collective self-defense of Iraq. The letter then goes on to state that the strikes against the Khorasan Group “address terrorist threats that they pose to the United States and our partners and allies.”

As the letter suggests, the legal justification for strikes against ISIL is presumably not the same as that for strikes against Khorasan. The following unpacks some of the key differences. (See also Ashley Deeks here and here and Ryan Goodman here and here for analysis of some of these issues.)

Collective Self-Defense and ISIL.

The U.S. government received a letter from the Iraqi government explicitly asking for U.S. help in the fight against ISIL, thus supporting a claim of collective self-defense. According to the U.S. notification to the United Nations, Iraq has specifically requested that the United States lead international efforts to strike ISIL sites inside Syria to suppress continuing attacks on Iraq and protect Iraqi citizens. Under a theory of collective self-defense, the United States is assisting Iraq in responding to the direct and ongoing threat posed by ISIL; the threat stems in part from ISIL forces in Syria, and Syria is either unable or unwilling to quell the threat, thereby justifying an incursion into Syria’s territory.

The weakest link in the chain is the unwilling or unable test. As one of us has written, “The ‘unwilling or unable’ test is now a fairly well settled part of the US government’s legal position. Nevertheless, it remains controversial under international law.” And another one of us conducted an exhaustive study, which found that states quite frequently invoke the test, but “found no cases in which states clearly assert that they follow the test out of a sense of legal obligation.” That said, Secretary General Ban Ki-moon’s statement below, which emphasized that the “the strikes took place in areas no longer under the effective control of that Government,” suggests there may be growing acceptance for aspects of at least the “unable” prong of the test in some cases.

Assuming, arguendo, acceptance of the unable or unwilling test, the U.S. legal argument is sound, so long as the force used is necessary to protect against the direct threat that ISIS poses to Iraq, and that the amount and nature of force is proportionate to suppressing that threat. Given ISIL’s rapid advances in Iraq, given claims that planning and support is flowing from Syria, and given Assad’s inability (and potential unwillingness) to quell ISIL operations along the Iraq border, the necessity of the actions seems clear. Targeted strikes against ISIL bases, ISIL training camps, and ISIS-controlled transit points into Iraq seem proportionate to this aim.

If the goal shifts from defending against, repelling, or containing ISIL to destroying ISIL (as President Obama has previously stated is its ultimate goal), this legal ground becomes shakier. The United States (and Iraq) will need to establish that the destruction of the group is necessary and proportionate to the threat—something it very well may do, but which will likely raise questions about proportionality.

Defense of U.S. Nationals and ISIL

According to New York Times reporting, the United States may also be relying on a theory of defense of U.S. nationals in Iraq as a supplementary justification for use of force against ISIL. (Given repeated statements that ISIL does not currently pose a specific threat to the U.S. homeland, the theory of self-defense needs to be instead based on threats to U.S. personnel.) But this is a less convincing rationale—and notably is absent from the final letter submitted to the U.N.

Given that the United States has successfully defended against ISIL advances that would have directly threatened U.S. personnel in Iraq, and given that the United States has not deemed it necessary to evacuate non-military U.S. personnel for their safety, it seems questionable that further attacks in Syria are, at least at the moment, necessary to protect U.S. personnel. (That said, none of us is privy to the relevant intelligence, so it is of course possible that there is information suggesting ISIL in Syria has both the capacity and intent to launch attacks targeting U.S. personnel in Iraq, which would obviously change the calculus.)

This claim, moreover, raises another issue—one that international law does not currently resolve, but that warrants further consideration. The U.S. could, of course, minimize this threat by removing personnel from Iraq. In what situations should a nation’s decision to keep its personnel in a risky environment itself provide the justification for use of force? An obligation to remove personnel sounds, in some ways, like a forced retreat—and not something that international law should demand. On the other hand, a nation should not be permitted to purposefully place its personnel in an inherently risky situation and then claim self-defense as an end-run around rules limiting the use of force.

In any event, the claim of collective self-defense appears a much sounder claim than one based on defense of U.S. nationals.

Collective Self-Defense and Khorasan?

Little was known about the Khorasan Group until earlier last week, when Administration officials first began publicly talking about the threat posed by this...
group. Most claims with respect to Khorasan focus on the threat allegedly posed to U.S. and European allies. In that same vein, the U.S. letter to the U.N. states that the strikes against Khorasan "address terrorist threats that they pose to the United States and our partners and allies."

There is thus no indication that the United States is undertaking attacks against Khorasan with the aim of coming to Iraq’s defense or that the Iraqis have requested the U.S. to take action against Khorasan. As for European allies: under the rules of collective self-defense, at least as articulated by the ICI, those allies (at least one of them) would have to invoke the right of self-defense against an imminent threat of armed attack from Khorasan and formally request the assistance of the United States to use force against the group.

**Possible Theories Justifying Strikes Against Khorasan**

What, then, justifies the strikes against Khorasan? In a *War Powers Report* filed today, President Obama invokes (among other things) his authority to carry out strikes pursuant to the 2001 AUMF. This suggests that the United States is relying on the theory that Khorasan is either “part of” al Qaeda or an “associated force” thereof. Indeed, the WPR describes Khorasan as an “element” of al Qaeda. Under this theory, the U.S. is in an ongoing armed conflict with Khorasan, Syria is unable or unwilling to take action against our enemy in the armed conflict, and thus the United States may use force in Syria against Khorasan without having to undertake a new self-defense analysis to justify the incursion into Syrian territory. This, after all, is what John Brennan argued when he asserted the right to take action against al Qaeda “without doing a separate self-defense analysis each time.”

That said, this is not likely to be a popular position, at least internationally. The United States entered an armed conflict with al Qaeda in late 2001, under a well-accepted theory of self-defense, and initially took action against al Qaeda in Afghanistan with the blessing of the international community. Now, thirteen years later, it is not entirely clear that the same blessing supports a continuing armed conflict model against associated and splinter groups—especially if that theory is used to intervene militarily in another nation’s territory without its consent.

The United States may also be separately asserting a claim of anticipatory self-defense. The Pentagon today seemed to lay the framework for that position, stating that Khorasan was “nearing the execution stage of launching at attack on Europe or the homeland.” If there is reliable information suggesting that Khorasan is planning active, direct attacks on the homeland, then strikes against Khorasan may very well be justified under a theory of self-defense, again assuming one accepts the unwilling or unable test and can establish that Syria meets that standard. Whether the situation squarely falls within a self-defense theory depends on multiple unknown facts, including what the Pentagon means by “nearing the execution stage.” We simply lack intelligence information to assess how credible or imminent such a threat is—essential components to any assessment of the necessity and proportionality requirements of self-defense.

All of this, of course, is focused on the international law issues, and does not assess the domestic law basis for the strikes. As for the domestic law basis, the administration again appears to be invoking the 2001 and 2002 AUMFs—a position that 2/3 of us have been critical of in the past. We thus join President Obama in his call to Congress to put the actions on sounder domestic law footing, and pass a new authorization specifically focused on ISIL, and, depending on the facts, the Khorasan Group as well.

***

Guest Author Ryan Goodman is co-editor-in-chief of Just Security. He is the Anne and Joel Ehrenkranz Professor of Law and Co-Chair of the Center for Human Rights and Global Justice at New York University School of Law, and he is also Professor of Politics and Professor of Sociology at NYU.
The Obama Administration’s Legal Justification for Strikes Against the Islamic State In Syria

By Jack Goldsmith
Tuesday, September 23, 2014 at 3:38 PM

Based on comments from senior Obama administration officials who spoke on "the condition of anonymity," Charlie Savage reports the Obama administration's legal theory for the use of force against the Islamic State.

Savage says that the domestic legal justification is both the 2001 and the 2002 AUMFs:

Administration officials have said that as a matter of domestic law, they believe the United States has statutory authority to attack the Islamic State under Congress’s 2001 authorization to fight Al Qaeda. They also believe that Congress’s 2002 authorization of the Iraq war could provide an alternative source of such authority. The United States has been bombing Islamic State forces in Iraq since August.

Both congressional authorizations provide legal authority for the strikes in Syria, too, the officials contended, because of the Islamic State’s history of ties to Al Qaeda — notwithstanding the fact that the two groups recently split. And, they said, the 2002 Iraq war authorization can be read in part as promising to help foster a stable, democratic government in Iraq, which would include defending it from terrorist attacks.

The administration also appears to rely on Article II. In today’s WPR letter to Congress, the President states:

I have directed these actions, which are in the national security and foreign policy interests of the United States, pursuant to my constitutional and statutory authority as Commander in Chief (including the authority to carry out Public Law 107-40 [2001 AUMF] and Public Law 107-243 [2002 AUMF]) and as Chief Executive, as well as my constitutional and statutory authority to conduct the foreign relations of the United States.

In addition, Savage reports that the international law justification is the self-defense of Iraq, plus, secondarily, the self-defense of U.S. personnel in Iraq:

Senior Obama administration officials said on Tuesday that the airstrikes against the Islamic State — carried out in Syria without seeking the permission of the Syrian government or the United Nations Security Council — were legal because they were done in defense of Iraq. . . .

[T]he senior administration officials said on Tuesday that Iraq had a valid right of self-defense against the Islamic State — also known as ISIS or ISIL — because the militant group was attacking Iraq from its havens in Syria, and the Syrian government had proved unable or unwilling to suppress that threat. Iraq asked the United States for assistance in defending itself, making the strikes legal, the officials said. . . .

The United States is also asserting a right to defend its own personnel in Iraq from the Islamic State. The officials said this should be understood as supplementary authority to helping Iraq defend itself directly.

Quick analysis, more later: The President is on pretty strong legal ground under both domestic and international law. I think the 2001 AUMF argument is weak, but the combination of the three domestic authorities (2001 AUMF, 2002 AUMF, and Article II) is an adequate legal foundation for the strikes. However, for reasons I have argued at length, and that the President articulated in his speech on August 31, 2013, it would have been politically wise and constitutionally prudent for him to force Congress to vote on and authorize this dramatic expansion of the "war on terrorism."
§ 3045. National mission of National Geospatial-Intelligence Agency, 50 USCA § 3045

50 U.S.C.A. § 3045
Formerly cited as 50 USCA § 404e

§ 3045. National mission of National Geospatial-Intelligence Agency

Currentness

(a) In general

In addition to the Department of Defense missions set forth in section 442 of Title 10, the National Geospatial-Intelligence Agency shall support the geospatial intelligence requirements of the Department of State and other departments and agencies of the United States outside the Department of Defense.

(b) Requirements and priorities

The Director of National Intelligence shall establish requirements and priorities governing the collection of national intelligence by the National Geospatial-Intelligence Agency under subsection (a) of this section.

(c) Correction of deficiencies

The Director of National Intelligence shall develop and implement such programs and policies as the Director and the Secretary of Defense jointly determine necessary to review and correct deficiencies identified in the capabilities of the National Geospatial-Intelligence Agency to accomplish assigned national missions, including support to the all-source analysis and production process. The Director shall consult with the Secretary of Defense on the development and implementation of such programs and policies. The Secretary shall obtain the advice of the Chairman of the Joint Chiefs of Staff regarding the matters on which the Director and the Secretary are to consult under the preceding sentence.

CREDIT(S)

CROSS REFERENCES
National Geospatial-Intelligence Agency, see 10 USCA § 441 et seq.

LIBRARY REFERENCES
American Digest System
War and National Emergency c–40.
United States Code Annotated
Title 10. Armed Forces (Refs & Annos)
Subtitle A. General Military Law (Refs & Annos)
Part I. Organization and General Military Powers
Chapter 22. National Geospatial-Intelligence Agency (Refs & Annos)
Subchapter I. Missions and Authority

10 U.S.C.A. § 441

§ 441. Establishment

Currentness

(a) Establishment.--The National Geospatial-Intelligence Agency is a combat support agency of the Department of Defense and has significant national missions.

(b) Director.--(1) The Director of the National Geospatial-Intelligence Agency is the head of the agency.

(2) Upon a vacancy in the position of Director, the Secretary of Defense shall recommend to the President an individual for appointment to the position.

(3) If an officer of the armed forces on active duty is appointed to the position of Director, the position shall be treated as having been designated by the President as a position of importance and responsibility for purposes of section 601 of this title and shall carry the grade of lieutenant general, or, in the case of an officer of the Navy, vice admiral.

(c) Director of National Intelligence collection tasking authority.--Unless otherwise directed by the President, the Director of National Intelligence shall have authority (except as otherwise agreed by the Director and the Secretary of Defense) to--

(1) approve collection requirements levied on national imagery collection assets;

(2) determine priorities for such requirements; and

(3) resolve conflicts in such priorities.

(d) Availability and continued improvement of imagery intelligence support to all-source analysis and production function.--The Secretary of Defense, in consultation with the Director of National Intelligence, shall take all necessary steps to ensure the full availability and continued improvement of imagery intelligence support for all-source analysis and production.

CREDIT(S)

§ 441. Establishment, 10 USCA § 441


10 U.S.C.A. § 441, 10 USCA § 441
Current through P.L. 113-163 (excluding P.L. 113-128) approved 8-8-14
PUBLIC LAW 107–243—OCT. 16, 2002

AUTHORIZATION FOR USE OF MILITARY FORCE AGAINST IRAQ RESOLUTION OF 2002
Joint Resolution

To authorize the use of United States Armed Forces against Iraq.

Whereas in 1990 in response to Iraq's war of aggression against and illegal occupation of Kuwait, the United States forged a coalition of nations to liberate Kuwait and its people in order to defend the national security of the United States and enforce United Nations Security Council resolutions relating to Iraq;

Whereas after the liberation of Kuwait in 1991, Iraq entered into a United Nations sponsored cease-fire agreement pursuant to which Iraq unequivocally agreed, among other things, to eliminate its nuclear, biological, and chemical weapons programs and the means to deliver and develop them, and to end its support for international terrorism;

Whereas the efforts of international weapons inspectors, United States intelligence agencies, and Iraqi defectors led to the discovery that Iraq had large stockpiles of chemical weapons and a large scale biological weapons program, and that Iraq had an advanced nuclear weapons development program that was much closer to producing a nuclear weapon than intelligence reporting had previously indicated;

Whereas Iraq, in direct and flagrant violation of the cease-fire, attempted to thwart the efforts of weapons inspectors to identify and destroy Iraq's weapons of mass destruction stockpiles and development capabilities, which finally resulted in the withdrawal of inspectors from Iraq on October 31, 1998;

Whereas in Public Law 105–235 (August 14, 1998), Congress concluded that Iraq's continuing weapons of mass destruction programs threatened vital United States interests and international peace and security, declared Iraq to be in "material and unacceptable breach of its international obligations" and urged the President "to take appropriate action, in accordance with the Constitution and relevant laws of the United States, to bring Iraq into compliance with its international obligations";

Whereas Iraq both poses a continuing threat to the national security of the United States and international peace and security in the Persian Gulf region and remains in material and unacceptable breach of its international obligations by, among other things, continuing to possess and develop a significant chemical and biological weapons capability, actively seeking a nuclear weapons capability, and supporting and harboring terrorist organizations;

Whereas Iraq persists in violating resolution of the United Nations Security Council by continuing to engage in brutal repression of its civilian population thereby threatening international peace
and security in the region, by refusing to release, repatriate, or account for non-Iraqi citizens wrongfully detained by Iraq, including an American serviceman, and by failing to return property wrongfully seized by Iraq from Kuwait;

Whereas the current Iraqi regime has demonstrated its capability and willingness to use weapons of mass destruction against other nations and its own people;

Whereas the current Iraqi regime has demonstrated its continuing hostility toward, and willingness to attack, the United States, including by attempting in 1993 to assassinate former President Bush and by firing on many thousands of occasions on United States and Coalition Armed Forces engaged in enforcing the resolutions of the United Nations Security Council;

Whereas members of al Qaida, an organization bearing responsibility for attacks on the United States, its citizens, and interests, including the attacks that occurred on September 11, 2001, are known to be in Iraq;

Whereas Iraq continues to aid and harbor other international terrorist organizations, including organizations that threaten the lives and safety of United States citizens;

Whereas the attacks on the United States of September 11, 2001, underscored the gravity of the threat posed by the acquisition of weapons of mass destruction by international terrorist organizations;

Whereas Iraq's demonstrated capability and willingness to use weapons of mass destruction, the risk that the current Iraqi regime will either employ those weapons to launch a surprise attack against the United States or its Armed Forces or provide them to international terrorists who would do so, and the extreme magnitude of harm that would result to the United States and its citizens from such an attack, combine to justify action by the United States to defend itself;


Whereas in the Authorization for Use of Military Force Against Iraq Resolution (Public Law 102–1), Congress has authorized the President "to use United States Armed Forces pursuant to United Nations Security Council Resolution 678 (1990) in order to achieve implementation of Security Council Resolution 660, 661, 662, 664, 665, 666, 667, 669, 670, 674, and 677";

Whereas in December 1991, Congress expressed its sense that it "supports the use of all necessary means to achieve the goals of United Nations Security Council Resolution 687 as being consistent with the Authorization of Use of Military Force Against
Iraq Resolution (Public Law 102–1).” that Iraq’s repression of its civilian population violates United Nations Security Council Resolution 688 and “constitutes a continuing threat to the peace, security, and stability of the Persian Gulf region,” and that Congress, “supports the use of all necessary means to achieve the goals of United Nations Security Council Resolution 688”;

Whereas the Iraq Liberation Act of 1998 (Public Law 105–338) expressed the sense of Congress that it should be the policy of the United States to support efforts to remove from power the current Iraqi regime and promote the emergence of a democratic government to replace that regime;

Whereas on September 12, 2002, President Bush committed the United States to “work with the United Nations Security Council to meet our common challenge” posed by Iraq and to “work for the necessary resolutions,” while also making clear that “the Security Council resolutions will be enforced, and the just demands of peace and security will be met, or action will be unavoidable”;

Whereas the United States is determined to prosecute the war on terrorism and Iraq’s ongoing support for international terrorist groups combined with its development of weapons of mass destruction in direct violation of its obligations under the 1991 cease-fire and other United Nations Security Council resolutions make clear that it is in the national security interests of the United States and in furtherance of the war on terrorism that all relevant United Nations Security Council resolutions be enforced, including through the use of force if necessary;

Whereas Congress has taken steps to pursue vigorously the war on terrorism through the provision of authorities and funding requested by the President to take the necessary actions against international terrorists and terrorist organizations, including those nations, organizations, or persons who planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such persons or organizations;

Whereas the President and Congress are determined to continue to take all appropriate actions against international terrorists and terrorist organizations, including those nations, organizations, or persons who planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such persons or organizations;

Whereas the President has authority under the Constitution to take action in order to deter and prevent acts of international terrorism against the United States, as Congress recognized in the joint resolution on Authorization for Use of Military Force (Public Law 107–40); and

Whereas it is in the national security interests of the United States to restore international peace and security to the Persian Gulf region: Now, therefore, be it

Resolved by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This joint resolution may be cited as the “Authorization for Use of Military Force Against Iraq Resolution of 2002”.

SEC. 2. SUPPORT FOR UNITED STATES DIPLOMATIC EFFORTS.

The Congress of the United States supports the efforts by the President to—

(1) strictly enforce through the United Nations Security Council all relevant Security Council resolutions regarding Iraq and encourages him in those efforts; and

(2) obtain prompt and decisive action by the Security Council to ensure that Iraq abandons its strategy of delay, evasion and noncompliance and promptly and strictly complies with all relevant Security Council resolutions regarding Iraq.

SEC. 3. AUTHORIZATION FOR USE OF UNITED STATES ARMED FORCES.

(a) AUTHORIZATION.—The President is authorized to use the Armed Forces of the United States as he determines to be necessary and appropriate in order to—

(1) defend the national security of the United States against the continuing threat posed by Iraq; and

(2) enforce all relevant United Nations Security Council resolutions regarding Iraq.

(b) PRESIDENTIAL DETERMINATION.—In connection with the exercise of the authority granted in subsection (a) to use force the President shall, prior to such exercise or as soon thereafter as may be feasible, but no later than 48 hours after exercising such authority, make available to the Speaker of the House of Representatives and the President pro tempore of the Senate his determination that—

(1) reliance by the United States on further diplomatic or other peaceful means alone either (A) will not adequately protect the national security of the United States against the continuing threat posed by Iraq or (B) is not likely to lead to enforcement of all relevant United Nations Security Council resolutions regarding Iraq; and

(2) acting pursuant to this joint resolution is consistent with the United States and other countries continuing to take the necessary actions against international terrorist and terrorist organizations, including those nations, organizations, or persons who planned, authorized, committed or aided the terrorist attacks that occurred on September 11, 2001.

(c) WAR POWERS RESOLUTION REQUIREMENTS.—

(1) SPECIFIC STATUTORY AUTHORIZATION.—Consistent with section 8(a)(1) of the War Powers Resolution, the Congress declares that this section is intended to constitute specific statutory authorization within the meaning of section 5(b) of the War Powers Resolution.

(2) APPLICABILITY OF OTHER REQUIREMENTS.—Nothing in this joint resolution supersedes any requirement of the War Powers Resolution.

SEC. 4. REPORTS TO CONGRESS.

(a) REPORTS.—The President shall, at least once every 60 days, submit to the Congress a report on matters relevant to this joint resolution, including actions taken pursuant to the exercise of authority granted in section 3 and the status of planning for efforts that are expected to be required after such actions are completed, including those actions described in section 7 of the Iraq Liberation Act of 1998 (Public Law 105–338).
(b) **Single Consolidated Report.**—To the extent that the submission of any report described in subsection (a) coincides with the submission of any other report on matters relevant to this joint resolution otherwise required to be submitted to Congress pursuant to the reporting requirements of the War Powers Resolution (Public Law 93–148), all such reports may be submitted as a single consolidated report to the Congress.

(c) **Rule of Construction.**—To the extent that the information required by section 3 of the Authorization for Use of Military Force Against Iraq Resolution (Public Law 102–1) is included in the report required by this section, such report shall be considered as meeting the requirements of section 3 of such resolution.

Joint Resolution

To authorize the use of United States Armed Forces against those responsible for the recent attacks launched against the United States. <<NOTE: Sept. 18, 2001 - [S.J. Res. 23]>>

Whereas, on September 11, 2001, acts of treacherous violence were committed against the United States and its citizens; and
Whereas, such acts render it both necessary and appropriate that the United States exercise its rights to self-defense and to protect United States citizens both at home and abroad; and
Whereas, in light of the threat to the national security and foreign policy of the United States posed by these grave acts of violence; and
Whereas, such acts continue to pose an unusual and extraordinary threat to the national security and foreign policy of the United States; and
Whereas, the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States: Now, therefore, be it

Resolved by the Senate and House of Representatives of the United States of America in Congress assembled, <<NOTE: Authorization for Use of Military Force. 50 USC 1541 note.>>

SECTION 1. SHORT TITLE.

This joint resolution may be cited as the `Authorization for Use of Military Force'.

SEC. 2. AUTHORIZATION FOR USE OF UNITED STATES ARMED FORCES.

(a) <<NOTE: President.>> In General.--That the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.

(b) War Powers Resolution Requirements.--
   (1) Specific statutory authorization.--Consistent with section 8(a)(1) of the War Powers Resolution, the Congress declares that this section is intended to constitute specific
statutory authorization within the meaning of section 5(b) of the War Powers Resolution.

[[Page 115 STAT. 225]]

(2) Applicability of other requirements.--Nothing in this resolution supercedes any requirement of the War Powers Resolution.

Approved September 18, 2001.

LEGISLATIVE HISTORY--S.J. Res. 23 (H.J. Res. 64):
---------------------------------------------------------------------

CONGRESSIONAL RECORD, Vol. 147 (2001):
Sept. 14, considered and passed Senate and House.
Sept. 18, Presidential statement.

<all>
The White House
Office of the Press Secretary

For Immediate Release

September 23, 2014

Letter from the President -- War Powers Resolution Regarding Iraq

TEXT OF A LETTER FROM THE PRESIDENT
TO THE SPEAKER OF THE HOUSE OF REPRESENTATIVES
AND THE PRESIDENT PRO TEMPORE OF THE SENATE

September 23, 2014

Dear Mr. Speaker: (Dear Mr. President:)

In my reports of August 8 and 17 and September 1 and 8, 2014, I described a series of discrete military operations in Iraq to stop the advance on Erbil by the Islamic State of Iraq and the Levant (ISIL), support civilians trapped on Mount Sinjar, support operations by Iraqi forces to recapture the Mosul Dam, support an operation to deliver humanitarian assistance to civilians in the town of Amirli, Iraq, and conduct airstrikes in the vicinity of Haditha Dam.

As I noted in my address to the Nation on September 10, with a new Iraqi government in place, and following consultations with allies abroad and the Congress at home, I have ordered implementation of a new comprehensive and sustained counterterrorism strategy to degrade, and ultimately defeat, ISIL. As part of this strategy, I have directed the deployment of 475 additional U.S. Armed Forces personnel to Iraq, and I have determined that it is necessary and appropriate to use the U.S. Armed Forces to conduct coordination with Iraqi forces and to provide training, communications support, intelligence support, and other support, to select elements of the Iraqi security forces, including Kurdish Peshmerga forces. I have also ordered the U.S. Armed Forces to conduct a systematic campaign of airstrikes and other necessary actions against these terrorists in Iraq and Syria. These actions are being undertaken in coordination with and at the request of the Government of Iraq and in conjunction with coalition partners.

It is not possible to know the duration of these deployments and operations. I will continue to direct such additional measures as necessary to protect and secure U.S. citizens and our interests against the threat posed by ISIL.

I have directed these actions, which are in the national security and foreign policy interests of the United States, pursuant to my constitutional and statutory authority as Commander in Chief (including the authority to carry out Public Law 107-40 and Public Law 107-243) and as Chief Executive, as well as my constitutional and statutory authority to conduct the foreign relations of the United States.

I am providing this report as part of my efforts to keep the Congress fully informed, consistent with the War Powers Resolution (Public Law 93-448). I appreciate the support of the Congress in this action.

Sincerely,

BARACK OBAMA

Excellency,

In Iraq’s letter to the United Nations Security Council of September 20, 2014, and other statements made by Iraq, including its letter to the United Nations Security Council of June 25, 2014, Iraq has made clear that it is facing a serious threat of continuing attacks from ISIL coming out of safe havens in Syria. These safe havens are used by ISIL for training, planning, financing, and carrying out attacks across Iraqi borders and against Iraq’s people. For these reasons, the Government of Iraq has asked that the United States lead international efforts to strike ISIL sites and military strongholds in Syria in order to end the continuing attacks on Iraq, to protect Iraqi citizens, and ultimately to enable and arm Iraqi forces to perform their task of regaining control of the Iraqi borders.

ISIL and other terrorist groups in Syria are a threat not only to Iraq, but also to many other countries, including the United States and our partners in the region and beyond. States must be able to defend themselves, in accordance with the inherent right of individual and collective self-defense, as reflected in Article 51 of the UN Charter, when, as is the case here, the government of the State where the threat is located is unwilling or unable to prevent the use of its territory for such attacks. The Syrian regime has shown that it cannot and will not confront these safe-havens effectively itself. Accordingly, the United States has initiated necessary and proportionate military actions in Syria in order to eliminate the ongoing ISIL threat to Iraq, including by protecting Iraqi citizens from further attacks and by enabling Iraqi forces to regain control of Iraq’s borders. In addition, the United States has initiated military actions in Syria against al-Qaida elements in Syria known as the Khorasan Group to address terrorist threats that they pose to the United States and our partners and allies.

I request that you circulate this letter as a document of the Security Council.

Samantha J. Power

His Excellency
Mr. Ban Ki-moon
Secretary-General of the United Nations,
New York, NY
We in the National Geospatial-Intelligence Agency (NGA) take great pride in our support to policymakers, warfighters, first responders, and Intelligence Community (IC) partners. Thanks to our dedicated workforce, we continue to deliver geospatial intelligence that supports national and departmental missions in pursuit of the national security and foreign policy objectives of the United States. NGA must anticipate tomorrow’s challenges against a backdrop of increasingly complex challenges in an era of fiscal constraint to position ourselves for the future.

The NGA Strategy establishes the strategic goals and objectives that will guide our efforts to fulfill NGA’s Mission and Vision and, in so doing, ensure that NGA continues to lead the Community in providing timely, relevant, and accurate geospatial intelligence in support of national security. This strategy is flexible by design and permits us to respond to ever-changing challenges, chief among them Under Secretary of Defense for Intelligence (USD[I]) priorities in the areas of counterterrorism, counterproliferation, cyber, and global coverage. We must also ensure GEOINT’s contribution is integrated into the Director of National Intelligence (DNI) sponsored Unified Intelligence Strategies (UIS), and that GEOINT matures as a key factor in achieving “intelligence integration,” a key DNI objective for the IC.

We can only accomplish our mission through the dedicated men and women of NGA. We will continually enable our workforce by fostering empowerment and accountability and by developing the knowledge, skills, and abilities essential to our success. In this we will always be guided by our Core Values: excellence, accountability, respect, teamwork, and honesty.

Working together, in the context of our shared vision, is the only means through which we will fulfill our mission. The strategy reinforces our belief in the strengths that each employee brings to NGA and in the critical role of partnership and collaboration both inside and outside the agency. The activities of each person and every component in NGA must be guided by the strategy in order that we may achieve its full potential. Thank you for your dedication to our mission and to the security of our fellow citizens as we continue this journey together.

Letitia A. Long
Director, National Geospatial-Intelligence Agency
Table of Contents

Mission, Vision, Core Values ................................................................. 5
Introduction ...................................................................................... 6
Strategic Goals ................................................................................ 7
Strategic Objective 1: Content ............................................................. 8
Strategic Objective 2: Open IT Environment ........................................ 9
Strategic Objective 3: Analytic Capabilities .......................................... 10
Strategic Objective 4: Customer Service ............................................. 11
Strategic Objective 5: Workforce ......................................................... 12
Strategic Objective 6: Workplace ......................................................... 13
Strategic Objective 7: Corporate and Functional Management ............. 14
Conclusion ....................................................................................... 15
Mission

NGA provides timely, relevant, and accurate geospatial intelligence in support of national security

Vision

Putting the Power of GEOINT in Your Hands

Core Values

Excellence — Be first rate in all that you do
Accountability — Answer for your conduct, even when no one is looking
Respect — Leverage diversity and creativity to perform as one NGA team
Teamwork — Work together to achieve a common goal
Honesty — Be truthful at all times
Introduction

The global security environment continues to evolve at an unprecedented rate. In the wake of the death of Osama bin Laden, the advent of the Arab Spring, and the "pivot" to focus on the Asia-Pacific region, we must prepare NGA for future national security challenges in an era of fiscal austerity. NGA and GEOINT are key enablers of our national security interests, actions, and decisions around the globe. The NGA Strategy aligns with the nation’s strategic priorities, goals, and objectives as outlined in the National Intelligence Strategy, the Defense Intelligence Strategy, and the Secretary of Defense strategic guidance: Sustaining U.S. Global Leadership: Priorities for 21st Century Defense.

Our strategy takes into account NGA's need to be agile in supporting multiple mission areas, including support to military and intelligence operations, intelligence analysis, homeland defense, and humanitarian and disaster relief, and to retain its focus on DNI and USD(1) priorities, including counterterrorism, counterproliferation, cyber, anti-access/area denial, and global coverage. It is imperative that NGA contribute to the greatest extent possible in advancing the DNI’s priority to integrate intelligence so that we, as a Community, ensure we produce the most accurate intelligence judgments that best serve the President, policymakers, and warfighters alike.

As we embrace today’s global landscape, we face an austere fiscal environment that demands better governance and deliberate planning to maintain critical Community capabilities while preserving resources for future mission development. The IC as a whole must be more efficient. Together we must leverage our collective resources to meet mission demands. This will require NGA to make difficult choices about current and proposed GEOINT capabilities across the National System for Geospatial Intelligence (NSG). To stay on top of emerging issues, NGA will need to carefully balance investments, resources, risks, and priorities.

Emerging science and technology brings both challenges and opportunities. NGA’s success will depend on how we embrace change, especially that which is enabled by advances in technology. As our adversaries adopt new denial and deception techniques, NGA must use innovative sources, tools, techniques, and processes to maintain our strategic advantage. NGA will be guided by our Vision, as expressed in our strategic goals and objectives, in taking GEOINT to the next level.
Strategic Goals

Provide Online, On-Demand Access to Our GEOINT Knowledge

*Provide ubiquitous access to GEOINT by creating an intuitive online environment that facilitates effortless and seamless access to our content—data and intelligence—anytime, anywhere. This will fulfill NGA's promise to “Put the Power of GEOINT in Your Hands” and provide consumers with the best possible user experience. Improved discovery of and accessibility to content, easy-to-use applications, more services, and richer analysis will define the future of GEOINT.*

Broaden and Deepen Our Analytic Expertise to Produce New Value

*Develop analysts who use the full spectrum of GEOINT sources, continuously sharpen their expertise through training and varied experiences, employ new technologies and techniques, develop new tradecraft, freely share and manage knowledge, collaborate, and lead and mentor others. Greater expertise fuels the “Power of GEOINT” by the creation of new value-products, enriched assessments, and higher value services that enable users to do their jobs better.*
NGA Strategy

Strategic Objective 1

Content

GEOINT data, products, and knowledge are discoverable, accessible, timely, and relevant

By 2017, NGA has empowered the GEOINT community through greatly improved access to varied content and applications, easy-to-use online services in all security domains, and the ability to contribute content to the global GEOINT knowledge base.

Create and make easily accessible and usable GEOINT content that addresses key intelligence questions and anticipates the entire range of our consumers’ needs. Recognizing that GEOINT data, products, services, and knowledge are most relevant when the information is easily accessible, NGA is committed to making its content discoverable, accessible, and usable in multiple security domains.

Develop and implement standards for GEOINT content creation, sharing, and storage. NGA will work with the Community to develop and evolve common standards to permit the sharing of GEOINT content, both to enrich the entirety of our collective GEOINT holdings and to reduce duplication and cost. Through Community engagement, NGA will make every effort to ensure that current and future systems that use, produce, or enable GEOINT are interoperable and adhere to applicable standards.
Open IT Environment

GEOINT processing and exploitation capabilities are rapidly developed and exportable for community use

Deliver a robust, safe, secure, and agile data framework and interfaces that foster community sharing of data and application development. NGA is committed to the development and promulgation of applications within the GEOINT community. NGA will build an open, agile, and resilient data framework to invite Community participation in developing, deploying, and sharing their own applications for use by the entire GEOINT community. It is imperative that the GEOINT enterprise architecture operates in the most efficient and effective manner possible to enable secure and responsive exploitation, analysis, and conception of solutions. NGA will institute a common methodology to organize, identify, and search data.

Leverage and rapidly deploy interoperable collection, processing, and exploitation capabilities in multiple security domains that promote the use of traditional and non-traditional (e.g., human geography and social media) geospatial sources. NGA will develop and deploy intuitive online services that are available for adoption and integration by the GEOINT community. These applications will provide immediate access to GEOINT processing and exploitation capabilities, enabling rapid and precise responses to key intelligence issues.
Analytic Capabilities

GEOINT’s value is increased to better address key intelligence issues

Meet customer needs through anticipatory GEOINT analysis. NGA will deliver robust, holistic, and anticipatory GEOINT analysis to address key intelligence issues and meet operational support needs. NGA will deliver an integrated analytic environment that makes access to data, workflows, and tradecraft easy and intuitive, encourages analysts to broaden their understanding of issues, promotes natural analytic collaboration; and provides analysts the ability to research new and emerging areas of national security concerns. We will transform current GEOINT analysis workflows to increase analysts’ access to data sources and methodologies to enhance GEOINT analysis. In so doing, we will rethink and transform our GEOINT analytic inputs, processes, outputs, and performance measures, enabling us to more effectively align our analytic resources to the nation’s most pressing issues.

Ensure tradecraft, training, and professional development meet the needs of the analytic workforce. As NGA deepens our GEOINT analytic expertise and capabilities, tradecraft, training, and professional development will keep pace. As our analytic processes mature, NGA will develop agile learning solutions and leverage curricula from throughout the NSG. We will emphasize learning from experience and conduct more frequent and systematic retrospective evaluations of analytical performance. NGA will develop analyst qualification and certification standards to enhance the overall standing and expertise of the workforce. We will promote an analytic environment that will leverage expertise and learning across the enterprise.

Take advantage of the full-spectrum of geospatial phenomenologies and make use of traditional and non-traditional sources. To maximize GEOINT analysis, NGA will develop new analytic techniques, leverage new technologies, and integrate advanced geospatial sensor data to enable more sophisticated analytic products and services. To take advantage of these emerging capabilities, NGA will evolve analytical tradecrafts that promote the use of non-literal data in addition to traditional and non-traditional sources. By executing innovative collection strategies, NGA will enable the delivery of cost-efficient solutions that effectively mitigate intelligence gaps.
Customer Service

GEOINT content is integrated, managed, and exposed to all GEOINT users on all domains using self-, assisted-, and full-service delivery models.

Lead the identification of new and emerging GEOINT capabilities for content, products, and services in anticipation of future intelligence and operational GEOINT needs. The timely development of relevant new GEOINT capabilities depends on monitoring emerging requirements, incorporating user feedback on existing capabilities, identifying gaps and shortfalls, and anticipating and understanding technology trends. We will move beyond simply instrumenting product and service utilization to understanding what it means and proactively acting on key trends. NGA will lead and leverage Community forums to identify and transition capabilities to respond to critical gaps and emerging mission needs.

Deliver a three-tiered service model supported by online, on-demand technology and analytic experts to ensure customized and responsive access to GEOINT content. NGA will provide a family of online services that will allow users to better serve themselves. For partners developing their own applications and services, we will lead the definition of GEOINT applications and provide the GEOINT data framework, as well as provide direct access to GEOINT content for those requiring it.

Provide advanced capabilities and content to unify, normalize, and advance online operations. Create upstream, automated GEOINT processes, tools, and techniques that enhance the effectiveness and efficiency of online GEOINT production. NGA will invest in tools that enable analysts and GEOINT users to spend more time analyzing GEOINT content (data, products, services) than finding it (i.e., data search or discovery). Harnessing advanced tools and developing next generation products will allow NGA to enhance user outcomes and position us for a rapidly changing, user-driven operational environment.
Strategic Objective 5

Workforce

NGA has an agile, expert, and diverse workforce and effective leaders who deliver results while collaborating inside NGA and with NGA customers and partners worldwide.

By 2017, NGA will attract, motivate, and retain a highly skilled, innovative, and adaptive workforce, and will reward those who take balanced risks in furtherance of NGA’s mission.

Cultivate an engaged workforce to make the NGA Vision a reality. Engaged employees, effective leaders, an inclusive work environment, and an inspired workforce culture promote a continuous positive cycle of mission accomplishment. NGA will establish responsive teams that embody our Core Values and collectively adapt and respond to emerging mission demands. NGA will coordinate innovative and resourceful solutions to mission challenges.

Adopt enterprise solutions to achieve a lean, agile, and responsive workforce. To meet the challenge of current missions and maintain the flexibility to adapt and change to meet future mission needs, NGA must build upon the diverse skills and backgrounds reflected in its workforce. Through the use of enhanced workforce planning methods and policies, NGA will be able to better determine the right balance of resources against needs.

Keep NGA mission-ready through a continuum of development and key talent acquisition. NGA will sustain continuous learning based on career competencies that outline the knowledge, skills, abilities, and other characteristics essential to effective job performance. NGA will develop agile learning solutions by leveraging innovative capabilities and integrating best practices into our programs of instruction. In order to develop and retain the next generation of leaders and GEOINT professionals, NGA will establish career roadmaps and professional development programs that do the following: define the steps for success, provide opportunities to gain perspective on the full range of NGA activities, and measure performance based on a holistic assessment process.
Strategic Objective 6

Workplace

NGA workplaces are modern, optimized, technically enabled, environmentally friendly, safe, secure, and encourage flexibility and collaboration to support the mission.

Establish a secure and safe environment.
NGA will secure our people, facilities, and information while providing a safe and efficient operating environment.

Find innovative ways to use and manage space to promote collaboration and improve productivity. NGA will look at “outside-the-box” methods to creatively manage and allocate space to promote optimal collaboration and improve productivity.

Bring all NGA facilities in line with world-class standards. NGA will achieve excellence in operating, maintaining, protecting, and modernizing NGA facilities to create a world-class environment for the NGA workforce. NGA will improve operational efficiencies and effectiveness of all facilities by integrating the workplace into all NGA planning, programming, and budgeting processes.

Strengthen counterintelligence and security functions for people, facilities, and network/systems in support of achieving the strategy. In order to mitigate risks to our people, facilities, and network/systems, NGA will strengthen counterintelligence and security programs, including an insider threats, counterintelligence awareness, and information assurance policies. NGA will protect cutting edge GEOINT technologies through identifying critical program information (CPI) that makes our systems world class, assessing the threats to those CPIs and then putting into place rigorous protection plans.

Go Green! NGA is on the forefront with its “green building” initiatives employed at NGA Campus East. By continuing to incorporate innovative technologies at all its sites, NGA will improve the work environment while conserving energy in more efficient ways.

By 2017, NGA will be a leader in the federal government by establishing secure, safe, sustainable, collaborative, and environmentally friendly sites that are in compliance with all federal, state, and local laws, regulations, and standards.
Corporate and Functional Management

NGA’s governance and business operations are streamlined, reflect best practices, and effectively influence the NSG and Allied System for Geospatial Intelligence (ASG)

Strengthen corporate functions through an efficient and consistent set of streamlined business processes. NGA will institute best practices in performance and portfolio management in order to implement mission-essential capabilities, obtain cost-efficiencies, and align acquisition and financial management processes across the GEOINT enterprise.

Lead advancement in the GEOINT field and transition Research and Development and Science and Technology (R&D/S&T) activities to operations. In close cooperation and coordination with IC, Department of Defense, and nontraditional partners, NGA will lead efforts to discover, leverage, adapt, and adopt GEOINT-related R&D/S&T across the enterprise. NGA will promote NSG cross-community discovery and exploitation of R&D/S&T capabilities through an approach that balances strategic scientific investment, improved transition into operations, and effective stewardship of limited R&D/S&T resources.

Advance functional management efforts to unify the GEOINT community. To strengthen the GEOINT discipline, NGA will lead the NSG and ASG through Community engagement by guiding the development of Community-wide solutions to NSG/ASG activities. As the Community leader, the GEOINT Functional Manager will promote GEOINT programs and resources that are transparent and aligned to address the highest priority mission needs, while satisfying the widest possible range of mission requirements that adhere to NSG/ASG policies, standards, and governance. Improvement in coordination, integration, and, where appropriate, synchronization of Community efforts, will increase the scope and effectiveness of GEOINT.

Improve performance through the development and use of metrics. NGA will establish a practical performance management program to enable data-driven decision making and to assess progress in achieving our strategy.
Conclusion

This strategy will guide us as we move forward with providing online, on-demand access to GEOINT knowledge and create new value by broadening and deepening analytic expertise. We will transition from a product producer to a content and services provider. This transition will make GEOINT more accessible, strengthen GEOINT standards and services, and develop better self-, assisted-, and full-service GEOINT so our user base not only grows, but the value we provide enables better outcomes for them. Through all of our activities, we will succeed in ...

Putting the Power of GEOINT in Your Hands

“...This is an exciting time for NGA. Our contributions to national security are undeniable. We are focused on our mission and the needs of our customers. We recognize the importance of collaborative, integrated intelligence. We know that in order to remain relevant, we must be agile and flexible in anticipating and responding to emerging global threats, and we must be responsible stewards of our resources.”

Lettitia A. Long
Director, NGA
Despite President Barack Obama's recent call to reduce the United States' reliance on drones, they will likely remain his administration's weapon of choice. Whereas President George W. Bush oversaw fewer than 50 drone strikes during his tenure, Obama has signed off on over 400 of them in the last four years, making the program the centerpiece of U.S. counterterrorism strategy. The drones have done their job remarkably well: by killing key leaders and denying terrorists sanctuaries in Pakistan, Yemen, and, to a lesser degree, Somalia, drones have devastated al Qaeda and associated anti-American militant groups. And they have done so at little financial cost, at no risk to U.S. forces, and with fewer civilian casualties than many alternative methods would have caused.

Critics, however, remain skeptical. They claim that drones kill thousands of innocent civilians, alienate allied governments, anger foreign publics, illegally target Americans, and set a dangerous precedent that irresponsible governments will abuse. Some of these criticisms are valid; others, less so. In the end, drone strikes remain a necessary instrument of counterterrorism. The United States simply cannot tolerate terrorist safe havens in remote parts of Pakistan and elsewhere, and drones offer a comparatively low-risk way of targeting these areas while minimizing collateral damage.

So drone warfare is here to stay, and it is likely to expand in the years to come as other countries' capabilities catch up with those of the United States. But Washington must continue to improve its drone policy, spelling out clearer rules for extrajudicial and extraterritorial killings so that tyrannical regimes will have a harder time pointing to the U.S. drone program to justify attacks against political opponents. At the same time, even as it solidifies the drone program,
Washington must remain mindful of the built-in limits of low-cost, unmanned interventions, since the very convenience of drone warfare risks dragging the United States into conflicts it could otherwise avoid.

**NOBODY DOES IT BETTER**

The Obama administration relies on drones for one simple reason: they work. According to data compiled by the New America Foundation, since Obama has been in the White House, U.S. drones have killed an estimated 3,300 al Qaeda, Taliban, and other jihadist operatives in Pakistan and Yemen. That number includes over 50 senior leaders of al Qaeda and the Taliban—top figures who are not easily replaced. In 2010, Osama bin Laden warned his chief aide, Atiyah Abd al-Rahman, who was later killed by a drone strike in the Waziristan region of Pakistan in 2011, that when experienced leaders are eliminated, the result is “the rise of lower leaders who are not as experienced as the former leaders” and who are prone to errors and miscalculations. And drones also hurt terrorist organizations when they eliminate operatives who are lower down on the food chain but who boast special skills: passport forgers, bomb makers, recruiters, and fundraisers.

Drones have also undercut terrorists’ ability to communicate and to train new recruits. In order to avoid attracting drones, al Qaeda and Taliban operatives try to avoid using electronic devices or gathering in large numbers. A tip sheet found among jihadists in Mali advised militants to “maintain complete silence of all wireless contacts” and “avoid gathering in open areas.” Leaders, however, cannot give orders when they are incommunicado, and training on a large scale is nearly impossible when a drone strike could wipe out an entire group of new recruits. Drones have turned al Qaeda’s command and training structures into a liability, forcing the group to choose between having no leaders and risking dead leaders.

Critics of drone strikes often fail to take into account the fact that the alternatives are either too risky or unrealistic. To be sure, in an ideal world, militants would be captured alive, allowing authorities to question them and search their compounds for useful information. Raids, arrests, and interrogations can produce vital intelligence and can be less controversial than lethal operations. That is why they should be, and indeed already are, used in stable countries where the United States enjoys the support of the host government. But in war zones or unstable countries, such as Pakistan, Yemen, and Somalia, arresting militants is highly dangerous and, even if successful, often inefficient. In those three countries, the government exerts little or no control over remote areas, which means that it is highly dangerous to go after militants hiding out there. Worse yet, in Pakistan and Yemen, the governments have at times cooperated with
militants. If the United States regularly sent in special operations forces to hunt down terrorists there, sympathetic officials could easily tip off the jihadists, likely leading to firefights, U.S. casualties, and possibly the deaths of the suspects and innocent civilians.

Of course, it was a Navy SEAL team and not a drone strike that finally got bin Laden, but in many cases in which the United States needs to capture or eliminate an enemy, raids are too risky and costly. And even if a raid results in a successful capture, it begets another problem: what to do with the detainee. Prosecuting detainees in a federal or military court is difficult because often the intelligence against terrorists is inadmissible or using it risks jeopardizing sources and methods. And given the fact that the United States is trying to close, rather than expand, the detention facility at Guantánamo Bay, Cuba, it has become much harder to justify holding suspects indefinitely. It has become more politically palatable for the United States to kill rather than detain suspected terrorists.

Furthermore, although a drone strike may violate the local state’s sovereignty, it does so to a lesser degree than would putting U.S. boots on the ground or conducting a large-scale air campaign. And compared with a 500-pound bomb dropped from an F-16, the grenadelike warheads carried by most drones create smaller, more precise blast zones that decrease the risk of unexpected structural damage and casualties. Even more important, drones, unlike traditional airplanes, can loiter above a target for hours, waiting for the ideal moment to strike and thus reducing the odds that civilians will be caught in the kill zone.

Finally, using drones is also far less bloody than asking allies to hunt down terrorists on the United States’ behalf. The Pakistani and Yemeni militaries, for example, are known to regularly torture and execute detainees, and they often indiscriminately bomb civilian areas or use scorched-earth tactics against militant groups.

Some critics of the drone program, such as Ben Emmerson, the UN’s special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, have questioned the lethal approach, arguing for more focus on the factors that might contribute to extremism and terrorism, such as poverty, unemployment, and authoritarianism. Such a strategy is appealing in principle, but it is far from clear how Washington could execute it. Individuals join anti-American terrorist groups for many reasons, ranging from outrage over U.S. support for Israel to anger at their own government’s cooperation with the United States. Some people simply join up because their neighbors are doing so. Slashing unemployment in Yemen, bringing democracy to Saudi Arabia, and building
a functioning government in Somalia are laudable goals, but they are not politically or financially possible for the United States, and even if achieved, they still might not reduce the allure of jihad.

In some cases, the most sensible alternative to carrying out drone strikes is to do nothing at all. At times, that is the right option: if militants abroad pose little threat or if the risk of killing civilians, delegitimizing allies, or establishing the wrong precedent is too high. But sometimes imminent and intolerable threats do arise and drone strikes are the best way to eliminate them.

THE NUMBERS GAME

Despite the obvious benefits of using drones and the problems associated with the alternatives, numerous critics argue that drones still have too many disadvantages. First among them is an unacceptably high level of civilian casualties. Admittedly, drones have killed innocents. But the real debate is over how many and whether alternative approaches are any better. The Bureau of Investigative Journalism reports that in 2011, drone strikes killed as many as 146 noncombatants, including as many as 9 children. Columbia Law School’s Human Rights Clinic also cites high numbers of civilian deaths, as does the Pakistani organization Pakistan Body Count. Peter Bergen of the New America Foundation oversees a database of drone casualties culled from U.S. sources and international media reports. He estimates that between 150 and 500 civilians have been killed by drones during Obama’s administration. U.S. officials, meanwhile, maintain that drone strikes have killed almost no civilians. In June 2011, John Brennan, then Obama’s top counterterrorism adviser, even contended that U.S. drone strikes had killed no civilians in the previous year. But these claims are based on the fact that the U.S. government assumes that all military-age males in the blast area of a drone strike are combatants—unless it can determine after the fact that they were innocent (and such intelligence gathering is not a priority).

The United States has recently taken to launching “signature strikes,” which target not specific individuals but instead groups engaged in suspicious activities. This approach makes it even more difficult to distinguish between combatants and civilians and verify body counts of each. Still, as one U.S. official told The New York Times last year, “Al Qaeda is an insular, paranoid organization—innocent neighbors don’t hitchhike rides in the back of trucks headed for the border with guns and bombs.” Of course, not everyone accepts this reasoning. Zeeshan-ul-hassan Usmani, who runs Pakistan Body Count, says that “neither [the United States] nor Pakistan releases any detailed information about the victims . . . so [although the United States] likes to call everybody Taliban, I call everybody civilians.”
The truth is that all the public numbers are unreliable. Who constitutes a civilian is often unclear; when trying to kill the Pakistani Taliban leader Baitullah Mehsud, for example, the United States also killed his doctor. The doctor was not targeting U.S. or allied forces, but he was aiding a known terrorist leader. In addition, most strikes are carried out in such remote locations that it is nearly impossible for independent sources to verify who was killed. In Pakistan, for example, the overwhelming majority of drone killings occur in tribal areas that lie outside the government’s control and are prohibitively dangerous for Westerners and independent local journalists to enter. Thus, although the New America Foundation has come under fire for relying heavily on unverifiable information provided by anonymous U.S. officials, reports from local Pakistani organizations, and the Western organizations that rely on them, are no better: their numbers are frequently doctored by the Pakistani government or by militant groups. After a strike in Pakistan, militants often cordon off the area, remove their dead, and admit only local reporters sympathetic to their cause or decide on a body count themselves. The U.S. media often then draw on such faulty reporting to give the illusion of having used multiple sources. As a result, statistics on civilians killed by drones are often inflated. One of the few truly independent on-the-ground reporting efforts, conducted by the Associated Press last year, concluded that the strikes “are killing far fewer civilians than many in [Pakistan] are led to believe.”

But even the most unfavorable estimates of drone casualties reveal that the ratio of civilian to militant deaths—about one to three, according to the Bureau of Investigative Journalism—is lower than it would be for other forms of strikes. Bombings by F-16s or Tomahawk cruise missile salvos, for example, pack a much more deadly payload. In December 2009, the United States fired Tomahawks at a suspected terrorist training camp in Yemen, and over 30 people were killed in the blast, most of them women and children. At the time, the Yemeni regime refused to allow the use of drones, but had this not been the case, a drone’s real-time surveillance would probably have spotted the large number of women and children, and the attack would have been aborted. Even if the strike had gone forward for some reason, the drone’s far smaller warhead would have killed fewer innocents. Civilian deaths are tragic and pose political problems. But the data show that drones are more discriminate than other types of force.

FOREIGN FRIENDS

It is also telling that drones have earned the backing, albeit secret, of foreign governments. In order to maintain popular support, politicians in Pakistan and Yemen routinely rail against the U.S. drone campaign. In reality, however, the governments of both countries have supported it.
During the Bush and Obama administrations, Pakistan has even periodically hosted U.S. drone facilities and has been told about strikes in advance. Pervez Musharraf, president of Pakistan until 2008, was not worried about the drone program’s negative publicity: “In Pakistan, things fall out of the sky all the time,” he reportedly remarked. Yemen’s former president, Ali Abdullah Saleh, also at times allowed drone strikes in his country and even covered for them by telling the public that they were conducted by the Yemeni air force. When the United States’ involvement was leaked in 2002, however, relations between the two countries soured. Still, Saleh later let the drone program resume in Yemen, and his replacement, Abdu Rabbu Mansour Hadi, has publicly praised drones, saying that “they pinpoint the target and have zero margin of error, if you know what target you’re aiming at.”

As officials in both Pakistan and Yemen realize, U.S. drone strikes help their governments by targeting common enemies. A memo released by the antisecrecy website WikiLeaks revealed that Pakistan’s army chief, Ashfaq Parvez Kayani, privately asked U.S. military leaders in 2008 for “continuous Predator coverage” over antigovernment militants, and the journalist Mark Mazzetti has reported that the United States has conducted “goodwill kills” against Pakistani militants who threatened Pakistan far more than the United States. Thus, in private, Pakistan supports the drone program. As then Prime Minister Yousaf Raza Gilani told Anne Patterson, then the U.S. ambassador to Pakistan, in 2008, “We’ll protest [against the drone program] in the National Assembly and then ignore it.”

Still, Pakistan is reluctant to make its approval public. First of all, the country’s inability to fight terrorists on its own soil is a humiliation for Pakistan’s politically powerful armed forces and intelligence service. In addition, although drones kill some of the government’s enemies, they have also targeted pro-government groups that are hostile to the United States, such as the Haqqani network and the Taliban, which Pakistan has supported since its birth in the early 1990s. Even more important, the Pakistani public is vehemently opposed to U.S. drone strikes.

A 2012 poll found that 74 percent of Pakistanis viewed the United States as their enemy, likely in part because of the ongoing drone campaign. Similarly, in Yemen, as the scholar Gregory Johnsen has pointed out, drone strikes can win the enmity of entire tribes. This has led critics to argue that the drone program is shortsighted: that it kills today’s enemies but creates tomorrow’s in the process.

Such concerns are valid, but the level of local anger over drones is often lower than commonly portrayed. Many surveys of public opinion related to drones are conducted by anti-drone organizations, which results in biased samples. Other surveys exclude those who are unaware of the drone program and thus overstate the importance of those who are angered by it.
addition, many Pakistanis do not realize that the drones often target the very militants who are wreaking havoc on their country. And for most Pakistanis and Yemenis, the most important problems they struggle with are corruption, weak representative institutions, and poor economic growth; the drone program is only a small part of their overall anger, most of which is directed toward their own governments. A poll conducted in 2007, well before the drone campaign had expanded to its current scope, found that only 15 percent of Pakistanis had a favorable opinion of the United States. It is hard to imagine that alternatives to drone strikes, such as seal team raids or cruise missile strikes, would make the United States more popular.

THE HOME FRONT

Still, public opposition is real, and there is growing concern about the drone strikes even in the United States. The program came under especially heavy criticism domestically in 2011, when Anwar al-Awlaki, a U.S. citizen born in New Mexico, was killed by a drone strike in Yemen. There is no question that Awlaki was dangerous. Adept at interspersing Islamist rhetoric with pop-culture references, Awlaki had been described as a “pied piper for Western ears”: one admirer was Nidal Malik Hasan, the U.S. Army officer who killed 13 U.S. soldiers at Fort Hood, Texas, in 2009.

The Obama administration claims that Awlaki was actively involved in plots against the United States and that the strike against him was legal under the Authorization for the Use of Military Force (AUMF), which Congress passed three days after 9/11 and which gives the president broad authority to use force against terrorist groups linked to the 9/11 attacks. Yet with the war on terrorism almost 12 years old and bin Laden dead, critics, such as the Georgetown University law professor Rosa Brooks, have begun questioning whether the AUMF still justifies drone strikes today. As Brooks has argued, “Many of the groups now being identified as threats don’t fall clearly under the AUMF’s umbrella—and many don’t pose a significant danger to the United States.” As for the case of Awlaki, opponents of his killing have argued that he did not pose an imminent threat to the United States and that in keeping the evidence used to justify his assassination secret, the administration violated the constitutional guarantee of due process for U.S. citizens. As Ron Paul, then a Texas representative, pointed out during his presidential campaign, Awlaki was never charged with any crime. He added, “If the American people accept this blindly and casually, that we now have an accepted practice of the president assassinating people who he thinks are bad guys, I think it’s sad.”

The administration contends that the discussions held within the executive branch and the extensive vetting of evidence constitute a form of due process. Meanwhile, as the legal scholar Benjamin Wittes has pointed out, both Congress and the federal courts have repeatedly
reaffirmed the validity of the AUMF since 2001. The U.S. government argues that given how secretly terrorists operate, it is not always possible to use other means to stop an individual overseas from planning attacks on U.S. forces or allies. As a result, the imminence of a threat should be assessed based on the individual’s propensity for violence and the likelihood of being able to stop him in the future. Wittes compares the decision-making process to that used in hostage situations, when police are not required to ask a judge for authority to kill a hostage taker or refrain from taking a clear shot if they have one. Perhaps most important, the White House has claimed only a very limited right to conduct drone strikes against U.S. citizens. The administration has asserted the authority to kill only senior al Qaeda leaders who cannot be captured, not any American member of al Qaeda. Indeed, it appears that Awlaki is the only U.S. citizen who has been deliberately killed by a drone?

FOLLOW THE LEADER

The fact remains that by using drones so much, Washington risks setting a troublesome precedent with regard to extrajudicial and extraterritorial killings. Zeke Johnson of Amnesty International contends that “when the U.S. government violates international law, that sets a precedent and provides an excuse for the rest of the world to do the same.” And it is alarming to think what leaders such as Syrian President Bashar al-Assad, who has used deadly force against peaceful pro-democracy demonstrators he has deemed terrorists, would do with drones of their own. Similarly, Iran could mockingly cite the U.S. precedent to justify sending drones after rebels in Syria. Even Brennan has conceded that the administration is “establishing precedents that other nations may follow.”

Controlling the spread of drone technology will prove impossible; that horse left the barn years ago. Drones are highly capable weapons that are easy to produce, and so there is no chance that Washington can stop other militaries from acquiring and using them. Nearly 90 other countries already have surveillance drones in their arsenals, and China is producing several inexpensive models for export. Armed drones are more difficult to produce and deploy, but they, too, will likely spread rapidly. Beijing even recently announced (although later denied) that it had considered sending a drone to Myanmar (also called Burma) to kill a wanted drug trafficker hiding there.

The spread of drones cannot be stopped, but the United States can still influence how they are used. The coming proliferation means that Washington needs to set forth a clear policy now on extrajudicial and extraterritorial killings of terrorists—and stick to it. Fortunately, Obama has begun to discuss what constitutes a legitimate drone strike. But the definition remains murky, and this murkiness will undermine the president’s ability to denounce other countries’ behavior
should they start using drones or other means to hunt down enemies. By keeping its policy secret, Washington also makes it easier for critics to claim that the United States is wantonly slaughtering innocents. More transparency would make it harder for countries such as Pakistan to make outlandish claims about what the United States is doing. Drones actually protect many Pakistanis, and Washington should emphasize this fact. By being more open, the administration could also show that it carefully considers the law and the risks to civilians before ordering a strike.

Washington needs to be especially open about its use of signature strikes. According to the Obama administration, signature strikes have eliminated not only low-level al Qaeda and Taliban figures but also a surprising number of higher-level officials whose presence at the scenes of the strikes was unexpected. Signature strikes are in keeping with traditional military practice; for the most part, U.S. soldiers have been trained to strike enemies at large, such as German soldiers or Vietcong guerrillas, and not specific individuals. The rise of unconventional warfare, however, has made this usual strategy more difficult because the battlefield is no longer clearly defined and enemies no longer wear identifiable uniforms, making combatants harder to distinguish from civilians. In the case of drones, where there is little on-the-ground knowledge of who is who, signature strikes raise legitimate concerns, especially because the Obama administration has not made clear what its rules and procedures for such strikes are.

Washington should exercise particular care with regard to signature strikes because mistakes risk tarnishing the entire drone program. In the absence of other information, the argument that drones are wantonly killing innocents is gaining traction in the United States and abroad. More transparency could help calm these fears that Washington is acting recklessly.

The U.S. government also needs to guard against another kind of danger: that the relative ease of using drones will make U.S. intervention abroad too common. The scholars Daniel Brunstetter and Megan Braun have argued that drones provide “a way to avoid deploying troops or conducting an intensive bombing campaign” and that this “may encourage countries to act on just cause with an ease that is potentially worrisome.” Although al Qaeda remains a threat, it has been substantially defanged since 9/11, thanks to the destruction of its haven in Afghanistan and effective global police, intelligence, and drone campaigns against its cells. In addition, the U.S. government needs to remember that many of the world’s jihadist organizations are focused first and foremost on local regimes and that although the United States has an interest in helping its allies fight extremists, Washington cannot and should not directly involve itself in every fight. The Obama administration should spell out those cases in
which the AUMF does not apply and recognize the risks of carrying out so-called goodwill kills on behalf of foreign governments. Helping French and Malian forces defeat jihadists in Mali by providing logistical support, for example, is smart policy, but sending U.S. drones there is not.

In places where terrorists are actively plotting against the United States, however, drones give Washington the ability to limit its military commitments abroad while keeping Americans safe. Afghanistan, for example, could again become a Taliban-run haven for terrorists after U.S. forces depart next year. Drones can greatly reduce the risk of this happening. Hovering in the skies above, they can keep Taliban leaders on the run and hinder al Qaeda’s ability to plot another 9/11.

AUTHOR

Daniel L. Byman
Research Director, Center for Middle East Policy
Senior Fellow, Foreign Policy, Center for Middle East Policy
@dbyman
Why Drones Fail

When Tactics Drive Strategy

Audrey Kurth Cronin

AUDREY KURTH CRONIN is Professor of Public Policy at George Mason University and the author of How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns. Follow her on Twitter @akcronin.

The war-weary United States, for which the phrase “boots on the ground” has become politically toxic, prefers to eliminate its terrorist foes from the skies. The tool of choice: unmanned aerial vehicles, also known as drones. In Pakistan, Somalia, and Yemen -- often far away from any battlefield where American troops are engaged -- Washington has responded to budding threats with targeted killings.

Like any other weapon, armed drones can be tactically useful. But are they helping advance the strategic goals of U.S. counterterrorism? Although terrorism is a tactic, it can succeed only on the strategic level, by leveraging a shocking event for political gain. To be effective, counterterrorism must itself respond with a coherent strategy. The problem for Washington today is that its drone program has taken on a life of its own, to the point where tactics are driving strategy rather than the other way around.

The main goals of U.S. counterterrorism are threefold: the strategic defeat of al Qaeda and groups affiliated with it, the containment of local conflicts so that they do not breed new enemies, and the preservation of the security of the American people. Drones do not serve all these goals. Although they can protect the American people from attacks in the short term, they are not helping to defeat al Qaeda, and they may be creating sworn enemies out of a sea of local insurgents. It would be a mistake to embrace killer drones as the centerpiece of U.S. counterterrorism.

AL QAEDA’s RESILIENCE

At least since 9/11, the United States has sought the end of al Qaeda -- not just to set it back tactically, as drones have surely done, but also to defeat the group completely. Terrorist organizations can meet their demise in a variety of ways, and the killing of their leaders is certainly one of them. Abu Sayyaf, an Islamist separatist group in the Philippines, lost its political focus, split into factions, and became a petty criminal organization after the army killed its leaders in 2006 and 2007. In other cases, however, including those of the Shining Path in Peru and Action Directe
in France, the humiliating arrest of a leader has been more effective. By capturing a terrorist leader, countries can avoid creating a martyr, win access to a storehouse of intelligence, and discredit a popular cause.

This is a preview of a premium article. You must subscribe [1] to access the full text. If you are already a subscriber, please log in here [2].

Copyright © 2002-2012 by the Council on Foreign Relations, Inc.
All rights reserved. To request permission to distribute or reprint this article, please fill out and submit a Permissions Request Form. If you plan to use this article in a coursepack or academic website, visit Copyright Clearance Center to clear permission.

Return to Article: http://www.foreignaffairs.com/articles/139454/audrey-kurth-cronin/why-drones-fail
Home > Essay > Why Drones Fail
Published on Foreign Affairs (http://www.foreignaffairs.com)

Links:
PROJECTING FORCE IN THE 21ST CENTURY - LEGITIMACY AND THE RULE OF LAW

TITLE 50, TITLE 10, TITLE 18, AND ART. 75

Jeff Mustin* & Harvey Rishikof**

I. PROLOGUE: THE MODERN BATTLEFIELD ........................................ 1235
II. EXPERTS ON THE ISSUES ............................................................. 1236
III. LEGAL AUTHORITY FOR COVERT ACTION ...................................... 1240
IV. WHO MAY CONDUCT A COVERT ACTION? ..................................... 1242
IV. ADDITION BY SUBTRACTION: WHAT IS A TRADITIONAL...
    MILITARY ACTIVITY? ................................................................. 1243
V. POLICY IMPLICATIONS ................................................................. 1245
VII. PROSECUTION V. LETHALITY - TITLE 18, ART. 75 AND RULE OF...
    LAW ............................................................................................ 1247
VIII. CONCLUSION ................................................................................ 1251

I. PROLOGUE: THE MODERN BATTLEFIELD

The Prussian strategist Carl von Clausewitz wrote that the first duty of the general and statesman is to understand the nature of the war upon which they are embarking.1 The modern battlefield has complicated this task. The United States military is currently conducting simultaneous counterinsurgency and counterterrorism operations in Afghanistan and Pakistan ("AF/PAK"),2 while the


** B.A., McGill University (1975); M.A. Brandeis University (1978); J.D., New York University (1996). Chair of the ABA Standing Committee on Law and National Security. Former professor of law and chair, Department of National Security Strategy, National War College. The views expressed in this Article are those of the author and do not reflect the official policy or position of the National Defense University, the National War College, the Department of Defense, the Director of National Intelligence, or the U.S. government.


1235
Central Intelligence Agency ("CIA"), traditionally more concerned with espionage than air warfare, has been conducting a robust aerial attack campaign in Pakistan’s Northwest Frontier Province. Conventional military forces, special operations forces, and intelligence professionals are all operating in the same area of operations, trying to enact the same strategies to meet the same policy goals but using contradictory legal authorities to do so.

The modern battlefield, defined in this Article as military operations since 2001, has contributed to the operational synthesis of intelligence and military organizations. The recent news that America’s most visible general officer, David Petraeus, will head the CIA and the former Director of the CIA, Leon Panetta, will take charge of the Department of Defense ("DoD"), illustrates a growing synergy between the nation’s primary spy agency and the military. The melding of executive agency roles and missions recently prompted national security writer and senior fellow at the Council on Foreign Relations, Max Boot, to opine that, "[w]e're in an era of 'covert action.'" But what exactly is covert action?

Perhaps Clausewitz’s guidance to understanding the nature of the counterinsurgency or counterterrorism fight is a difficult but achievable goal; understanding which forces to apply to which fight and what legal authorities authorize such action seems almost impossible. This Article seeks to clarify which forces are legally appropriate for which missions by defining and analyzing the differences between traditional military activities ("TMAs") and covert actions, and the consequences for prosecution. The first step to achieve this goal is to hear what the experts themselves say.

II. EXPERTS ON THE ISSUES

Experts in TMA and covert action convened in May to discuss legal authorities. The event, entitled “The bin Laden Operation – The Legal Framework” and sponsored by the American Bar Association’s Standing Committee on Law and National Security, provided a forum to dissect when operations fall under Title 10 versus Title 50 authorities. The event summary is instructive for this Article:

[T]he panelists addressed whether the bin Laden operation

---

6. Max Boot, Covert Action Makes a Comeback, WALL ST. J., Jan. 5, 2011, at A15 (stating that "covert action can be a valuable part of the policy maker's tool kit, provided that it is integrated into a larger plan").
had been properly designated a Title 50 operation rather than one under Title 10 authority. The panel included Syracuse Law professor William C. Banks; Senior Advisor to the Director of Operations for U.S. Cyber Command, Eric Greenwald; former Acting CIA General Counsel, John Rizzo; and, Deputy Legal Counsel, Office of the Chairman of the Joint Chiefs of Staff, Captain Stephanie Smart. Moderating the discussion was Special Advisor to the Committee, and Principal at Bingham Consulting Group, Suzanne Spaulding.

... [Professor Banks] began by noting that soon after the bin Laden operation was conducted, CIA Director Leon Panetta explained that it was a Title 50 operation and not Title 10. Professor Banks then defined "covert action" as an activity carried out by the United States government that is meant to influence political, economic, or military conditions abroad and where the role of the U.S. government will not be apparent or publicly acknowledged. He went on to highlight the major exceptions to 413b's requirements which are traditional counter-intelligence or police activities and traditional military activities. U.S. government entities carrying out these types of activities are not bound by 413b's requirements.

The traditional military activities exception (TMA) became a central issue of discussion for the panel as it was directly related to the bin Laden operation and has long been an area of confusion and concern vis-à-vis the oversight of covert activity. Professor Banks expressed skepticism as to how the bin Laden operation could be considered a Title 50 operation when the force that executed the mission was primarily military personnel from SEAL Team Six (or DEVGRU, as it is now known), and was commanded by Vice Admiral William McRaven, commander of the U.S. Joint Special Operations Command. He pointed out that a specific element of a TMA is that it be under the direction and control of a military commander which this operation was, thus making the bin Laden raid a TMA under Title 10 and not a covert action under Title 50.

The next panelist to speak was former Acting CIA General Counsel, John Rizzo ... He emphasized that covert operations are not solely the purview of the CIA, and that any U.S. government agency is technically authorized to carry out a covert operation provided that they comply with 413b, but Mr. Rizzo could not recall a single instance in his many years of dealing with this issue in which an agency other than the CIA sought and received the required written finding to conduct a covert action – even the U.S. military. (Later, during the Q & A session, Rizzo and Eric Greenwald further explained that this is partly because the CIA is the only

---

agency equipped with the internal legal mechanisms to easily comply with the oversight requirements of 413b.)

Rizzo also discussed the period during which Congress attempted to codify a statutory framework for covert actions (1990-91) and noted that creating a formal definition for “traditional military activity” had been exceedingly difficult. The definition of a TMA is not explicit in 413b, but legislative history lays out the elements as an activity being a TMA if it is: 1) conducted by military personnel; 2) under the direction and control of a U.S. military commander; 3) preceding or related to hostilities which are either anticipated to involve U.S. military forces, or where such hostilities are ongoing; and, 4) where the U.S. role in the overall operation is apparent or acknowledged publicly. 8

Next to speak was Captain Stephanie Smart . . . . She noted that military and CIA operations are equally subject to Congressional oversight, but that the TMA exception allows for a wide range of military operations not subject to 413b. She questioned Professor Banks’ assertion that the bin Laden raid had been exclusively a Title 10 action because it was conducted under the direction and control of a military commander; Capt. Smart countered by pointing out multiple elements that can define a TMA, not just military “command and control.” She further opined that the bin Laden operation could have been carried out under Title 10 or Title 50, and that the mere involvement of the military does not exclude it from the realm of Title 50 . . . .

The last panelist to speak was Eric Greenwald, whose current job is as a senior advisor to the military’s new Cyber Command . . . . Mr. Greenwald stated that during his time on the Hill, he encountered the blurry distinction between Title 10 and Title 50 authorities with regard to military operations termed “operational preparation of the environment” and intelligence activities under Title 50. While Title 50 intelligence activities are different than covert actions, this gave Mr. Greenwald experience with the often confusing interplay between Title 10 and Title 50; however, he stated that his current work with DoD has shown him how much care the military takes in ensuring that all operations are scrutinized to determine whether they properly fall under Title 10 or Title 50.

. . . . The discussion and audience questions that followed the panelists’ opening remarks continued to swirl around the TMA exception to 413b . . . . Professor Banks and Mr. Greenwald both agreed that the definition of a TMA is a moving target

and that Congress may have intentionally meant the definition to be vague so as to allow flexibility in this area. However, Mr. Greenwald pointed out that an action is not a TMA just because it is carried out by the military and that any such blanket characterization could likely thwart the congressional intent behind 413b of providing additional oversight to the type of paramilitary operations that had been carried out by CIA in the decades preceding the creation of these provisions in 1991.

One of Capt. Smart’s final points highlighted the DoD’s institutional process when it comes to the Title 10 versus Title 50 determination. Earlier in the discussion she pointed out that the department has a number of deconfliction mechanisms to vet operations to make sure that they are conducted under the appropriate legal authority. Later she stated that to her knowledge DoD has never sought a presidential finding for covert action under 413b. If DoD decides that an operation may more properly fall under Title 50, it does not conduct the operation or approaches the CIA and offers to turn the operation over. If the CIA accepts the operation then it will put together the required written finding and it will be conducted as a CIA operation with the military providing support on some level.

The last short issue discussed was the possibility of a “Title 60” that would basically consolidate Title 10 and Title 50 in an attempt to clarify legal boundaries in the area of covert action. The major proponent of this plan was former Director of National Intelligence, Dennis Blair, who suggested this both during his confirmation hearing and during testimony at a recent congressional hearing. The idea of Title 60 would be to provide a more clear legal framework for joint covert activities such as the bin Laden operation.9

Not discussed by the panel was what would have happened if Osama bin Laden had been arrested, returned to the United States, and prosecuted under criminal law, Title 18.10 Another option would have been to use the military commissions structure.11 From a legal perspective, it is important to note there was an outstanding arrest warrant for bin Laden in the Southern District of New York for his involvement in 9/11, and during the last ten years, he remained on

---

the Federal Bureau of Intelligence ("FBI") Top Ten list. Since 9/11, there has been a robust debate among the three branches of our government as to the proper way to detain and prosecute detainees from the war on terrorism. At the time of this Article, the constitutionality of military commissions or the need for a special national security court still remain unclear. Under international law, there are due process regimes for prosecution that have been recognized as legitimate forums for adjudication in complex hostile situations, such as Article 75 under Additional Protocol I.\textsuperscript{12}

As the panel discussion reflects, there is much confusion and debate on how to conceptualize the projection of force in the twenty-first century where traditional military activities and covert operations are merging. Moreover, how prosecution and detention fit our strategic approach to combat extremism has not yet been integrated into a holistic plan. Should these legitimate targets, if detained, be treated as traditional criminals, war criminals, or held as prisoners of war? Moreover, what is the best forum for trial: civil courts, military commissions, a special national security court, a foreign court, or an international court? Much of this confusion flows from the confusion of defining the modern battlefield.

III. LEGAL AUTHORITY FOR COVERT ACTION

The word "covert" carries important connotations. The term, in its colloquial usage, is frequently used to describe any activity the government wants concealed from the public eye, a usage that carries with it implications of illicit activity. However, legal usage of the word "covert" rarely evokes illicit connotations; in fact, the lawfulness of covert action is rarely debated at all. According to one treatise on covert action, "there has been a remarkably consistent national policy in favor of maintaining a competence to conduct a wide range of covert operations . . . . The national debate has, thus, focused not on the lawfulness of covert action but on the constitutional allocation of competence to control it."\textsuperscript{13} The real issue is over accountability and the role of the covert action from a policy perspective.

The ability to control covert action begins with its legal definition. The term "covert action" is statutorily defined as "an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be


\textsuperscript{13} W. MICHAEL REISMAN & JAMES E. BAKER, REGULATING COVERT ACTION: PRACTICES, CONTEXTS, AND POLICIES OF COVERT COERCION ABROAD IN INTERNATIONAL AND AMERICAN LAW 2 (1992) [hereinafter REGULATING COVERT ACTION].
apparent or acknowledged publicly . . . .” 14 The DoD defines covert action similarly, stating that a covert action is “[a]n operation that is so planned and executed as to conceal the identity of or permit plausible denial by the sponsor.” 15 Both definitions focus on concealing the identity of the activity’s sponsor.

As important as it is to define what covert action is, it is equally important to define what covert action is not. Statutorily, covert action does not include:

1) activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities;

2) traditional diplomatic or military activities or routine support to such activities;

3) traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or

4) activities to provide routine support to the overt activities (other than activities described in paragraph (1), (2), or (3)) of other United States Government agencies abroad. 16

Additionally, covert action is prohibited if it is “intended to influence United States political processes, public opinion, policies, or media.” 17

Thus, because of 50 U.S.C. § 413b(e)(1), intelligence activities are not generally considered covert activities. Instead, intelligence collection is generally considered clandestine in nature. 18 The DoD defines clandestine activities as “[a]n operation sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment.” 19 Simply put, covert action

---

15. Joint Chiefs of Staff, Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms 132 (2001) (“A covert operation differs from a clandestine operation in that emphasis is placed on concealment of the identity of the sponsor rather than on concealment of the operation.”).
17. 50 U.S.C. § 413b(f).
18. See 50 U.S.C. §§ 403-04a(f) (“Under the direction of the Director of National Intelligence and in a manner consistent with section 3927 of Title 22, the Director of the Central Intelligence Agency shall coordinate the relationships between elements of the intelligence community and the intelligence or security services of foreign governments or international organizations on all matters involving intelligence related to the national security or involving intelligence acquired through clandestine means.”).
19. Joint Chiefs of Staff, Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms 89 (2001) (“In special operations, an activity may be both covert and clandestine and may focus equally on operational
conceals the identity of the country involved in an operation; clandestine activity hides the very existence of the operation.

IV. WHO MAY CONDUCT A COVERT ACTION?

Ultimately, the ability to conduct covert action lies with the CIA, with some notable exceptions. The initial power to conduct covert action is granted to the Executive through 50 U.S.C. §§ 403-4a(d), which provides the CIA with the authority to collect, correlate, evaluate, and coordinate intelligence collection. Additionally, in pertinent part, the CIA is authorized to "perform such other functions and duties related to intelligence affecting the national security as the President or the Director of National Intelligence may direct." This is the so-called "Fifth Function," or implicit authorization for the CIA to conduct covert action.

This power is defined more explicitly within Executive Order 12,333, which states:

[T]he CIA shall . . . . conduct [covert action] activities approved by the President. No agency except the CIA (or the Armed Forces of the United States in time of war declared by Congress or during any period covered by a report from the President to the Congress under the War Powers Resolution (87 Stat. 855)) may conduct any [covert action] activity unless the President determines that another agency is more likely to achieve a particular objective . . . .

This provides the CIA with clear executive authority to conduct covert action pursuant to a presidential finding. Interestingly, however, there are two major caveats. The first caveat provides for U.S. Armed Forces covert action pursuant to a declaration of war by Congress, or "during any period covered by a report from the President to the Congress under the War Powers Resolution." The second caveat provides that another agency—any other agency—may conduct a covert action if that other agency would be "more likely to

considerations and intelligence-related activities.

21. Id. §§ 403-04a(d)(4).
24. Id. at 5546. No president has ever acknowledged being bound by the War Powers Resolution, but this executive order makes it clear that any military action "consistent with" but not binding the Executive, will suffice. See also BERNET DYCUS ET AL., NATIONAL SECURITY LAW 250-51 (4th ed. 2007) (stating that President Ford reported to Congress "taking note of the provision of Section 4(a)(2) of the War Powers Resolution." President Carter reported "consistent with the reporting provisions of the War Powers Resolution." ) (internal citations omitted).
achieve [the] particular objective." 25 For example, if the Department of Energy had particular expertise in detecting nuclear radiation, it might be authorized, via presidential finding, to conduct a covert action relating to detecting nuclear radiation.

This second caveat opens the door for any agency, including Special Operations Forces ("SOF"), to conduct covert action. The DoD agrees. Joint Publication 3-05.2 defines yet another type of mission that leaves the door open for alternative uses for SOF: collateral missions. 26 Collateral missions are "mission[s] other than those for which a force is primarily organized, trained, and equipped, that the force can accomplish by virtue of the inherent capabilities of that force." 27 The executive summary to Joint Publication 3-05.2 explains, "SOF conduct specific principal missions and can conduct collateral activities using the inherent capabilities resident in the primary missions." 28 Thus, depending on the type of missions, SOF might be the primary choice for covert action if they have inherent capabilities superior to those of the CIA for a particular mission.

In summary, a covert action may be conducted by any agency the President deems appropriate. While the CIA clearly would be the primary agency to perform the Fifth Function, any agency may be authorized by presidential finding to conduct covert action exclusive of the limitations in 50 U.S.C. § 413b(e)(1)-(4). In short, the statute affords the President multiple potential choices, but the issue of accountability remains.

IV. ADDITION BY SUBTRACTION: WHAT IS A TRADITIONAL MILITARY ACTIVITY?

As previously discussed, defining covert action requires an understanding of what covert action is and is not. Referring back to 50 U.S.C. §§ 413b(e)(1)-(4), covert action is statutorily segregated from traditional intelligence and counterintelligence activities, traditional military activities, traditional law enforcement activities, and "activities to provide routine support to the overt activities." 29

Implicitly, this list of "traditional" activities would seem to indicate that covert action was never meant to be traditional. Instead, it was meant to provide policy makers with an option on the "continuum between diplomacy and war." 30 Covert action has not

27. Id.
28. Id. at xi.
29. 50 U.S.C. § 413b(e)(1)-(4).
always been a prominent policy tool; “covert action was not an integral policy tool until the Cold War.”\textsuperscript{31}

Applying this to the modern battlefield, if covert action is not a traditional military activity, then what is a traditional military activity? There is no legal definition. If one sought to define traditional military activities through historical practice, he or she might look to doctrinal or customary missions. A hypothetical list of such activities might include maneuver warfare, aerial attack, artillery barrages, or amphibious landings. However, this list is problematic because the tactics, techniques, and procedures involved with warfare are constantly changing. Prior to 2001, few would have listed counterinsurgency as a primary mission set of the conventional United States Army.\textsuperscript{32} Similarly, a decade ago, few security experts would have listed cyberwarfare among traditional military activities. Consequently, the term “traditional” makes merging historical military practice and modern combat realities difficult in an adaptive environment like war. To compound matters, it is extremely difficult to predict the nature of the next war or even the next evolution of the current war. The adaptive nature of war may or may not drive activities that lie within “traditional” military missions. As a result, looking to doctrinal or customary missions does not help one looking for a legal definition of a traditional military action.

Instead, in absence of positive guidance about what constitutes a traditional military activity, the most precise language can be devised by analyzing what is the absence of covert action. Defining a traditional military activity this way would consist of two elements: 1) those activities on the battlefield that are not covert action and are not authorized by presidential finding but, 2) that are authorized under traditional \textit{jus ad bellum} sources.\textsuperscript{33} Stated another way, traditional military activities would be overt actions (or covert actions not requiring a presidential finding such as preparations for war) authorized under \textit{jus ad bellum}.

\textsuperscript{31} \textit{Id.} at 148 (“Such ‘covert’ mechanisms allowed proxies to engage in hot war, while the great power conflict remained ‘cold.’”).

\textsuperscript{32} Prior to 2001, the counterinsurgency mission set was typically reserved for SOF conducting the foreign internal defense mission. \textit{See generally} Joint Chiefs of Staff, Joint Publication 3-07.1, Joint Tactics, Techniques, and Procedures for Foreign Internal Defense (FID) (2004). The SOF counterinsurgency mission, with their specialized manpower, was a far cry from the “clear, hold, build” strategies made popular by Gen. H.R. McMaster in Tal Afar, Iraq, in 2005. See Oliver Poole, Iraqis in former rebel stronghold now cheer American soldiers, \textit{Telegraph} (Dec. 19, 2005, 12:01 AM), \url{http://www.telegraph.co.uk/news/worldnews/middleeast/iraq/1000872/Iraqis-in-former-rebel-stronghold-now-cheer-American-soldiers.html}.

\textsuperscript{33} Such \textit{jus ad bellum} sources might include United Nations Charter Article 42 or 51 actions, or congressional declarations of war. \textit{See U.N. Charter arts. 42, 51}.
V. POLICY IMPLICATIONS

If these definitions are accepted as true, the result is that it has become legally easier for the executive branch to order covert action than to order conventional armed conflict. To commit military troops for a traditional military action, the President must have a casus belli and subsequently seek jus ad bellum justification and (typically) international support. This would usually involve the political and diplomatic gyrations involved in garnering both domestic legal support from Congress and international legal support from the United Nations Security Council.

Alternatively, to authorize a covert action, the President may forgo these diplomatic and political gyrations and merely issue a classified finding to conduct a covert action. While the President must report this action to Congress, the President may restrict disclosure to the “Gang of Eight” when “it is essential to limit access to the finding to meet extraordinary circumstances affecting vital interests of the United States.”

Thus, while covert action is not without legal accountability, it is a much more direct way for the President to commit forces. Additionally, forces conducting covert action operate by stealth. By their nature, they will have much lower visibility in the public eye. This provides the Executive a lawful option to commit force while theoretically lessening the media accountability for those actions. As a result, covert action also vests an immense amount of authority in the Executive and the “Gang of Eight” to conduct operations without the accountability to their constituents typically found in a democratic society.

Covert action also enables unilateral action. The stealthy nature

---

34. See 50 U.S.C. § 413b(b) (“To the extent consistent with due regard for the protection from unauthorized disclosure of classified information . . . the Director of National Intelligence . . . (1) shall keep the congressional intelligence committees fully and currently informed of all covert actions . . . ; and (2) shall furnish to the congressional intelligence committees any information or material concerning covert actions . . . which is requested by either of the congressional intelligence committees in order to carry out its authorized responsibilities.”).

35. 50 U.S.C. § 413b(c)(2). The “Gang of Eight” consists of “the chairmen and ranking minority members of the congressional intelligence committees, the Speaker and minority leader of the House of Representatives, [t]he majority and minority leaders of the Senate . . . [and] other . . . members of the congressional leadership . . . may be included by the President.” Id.

36. See New York Times Co. v. United States, 403 U.S. 713, 719 (1971) (Black, J., concurring). “Secrecy in government is fundamentally anti-democratic, perpetuating bureaucratic errors. Open debate and discussion of public issues are vital to our national health.” Id. at 724. “[T]he only effective restraint upon executive policy and power in the areas of national defense and international affairs may lie in . . . informed and critical public opinion which alone can here protect the values of democratic government.” Id. at 728 (Stewart, J., concurring).
of covert action means that the Executive would be discouraged from seeking international cooperation. Any international support would likely be limited to notifying host nations of the presence of troops, and those notifications, as a tactical matter, would likely be last minute and very directive in nature. This type of unilateral action contrasts the cooperative intent for international law, and, in the words of one legal scholar, "[u]nilateral action- covert or overt - generates particularly high emotions, because many view it as a litmus test for one's commitment to international law." Excessive use of covert action might be deemed by some nations as a rebuke of international law or evidence of a hubristic foreign policy. The continued and constant use of this instrument when lethality is the goal raises issues of international legitimacy.

Despite these reservations, covert action can be a useful policy tool. It is much more flexible and rapid than a traditional military activity, meaning it is much more suited to countering an adaptive enemy. Covert operations are generally more acute in their scope and objectives, which provides policymakers a scalpel to apply instead of the massive hammer of the U.S. military. Also, there are times when foreign policy maneuvers require stealth. One might imagine the need to retrieve unsecured nuclear material as a mission requiring immediacy and discreetness inappropriate for a large military unit.

A textbook case of covert action as a useful policy tool was the May 2011 raid on the compound of Osama bin Laden. The direct action strike was a Title 50 action conducted by DoD special operations assets. The likely legal scenario for this operation was that President Obama issued his finding, which authorized the CIA to "own" the operation and, under subsequent Title 50 authorities, allowed Joint Special Operations Command to conduct the raid because the President determined "that another agency is more likely to achieve a particular objective ...." The need for stealth,

37. Notification of covert infiltration, as a practical matter, renders the covert nature of the action null. See REISMAN & BAKER, supra note 13, at 14.
38. See U. N. Charter art. 2, para. 4 ("All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.").
39. REISMAN & BAKER, supra note 13, at 3.
42. See Exec. Order No. 12,333, 46 Fed. Reg. 59,941, 59,945-46 (Dec. 4, 1981); see also Sean D. Naylor, Bin Laden raid a triumph for Spec Ops, ARMY TIMES, May 9, 2011 (describing some of the unique capabilities that might cause special operations
even from the host nation, was obvious, and the covert action provided the acute desired result.

While the bin Laden raid demonstrates a positive result and the operation shows a clear need to maintain an ability to conduct covert action, it is important to emphasize that covert action is not without policy hazards. The danger in blurring the line between covert action and traditional military activities is that policymakers will choose to authorize what might normally be characterized as a traditional military activity under the guise of a covert action in order to circumvent the need for accountability or international support. Applying traditional military force without transparency is not the raison d'être for a covert capability.

For a case study, one need not look further than our current military conflict in AF/PAK. Is the precision bombing campaign being conducted truly a traditional military activity or a covert action? While arguments can be made for both sides, the mission of precision bombing, especially over an extended duration, has traditionally fallen to the United States Air Force or United States Navy. The action, despite its legal authorization, is certainly overt; newspapers chronicle the airstrikes daily.43 One must wonder, then, how the concept of “covert” is being understood on the modern battlefield.

VII. PROSECUTION V. LETHALITY - TITLE 18, ART. 75 AND RULE OF LAW

The use of lethality versus capture and prosecution in the covert action context raises the difficult questions of grand strategy and the final goals of the decision to project force. Unless the state has created a legitimate prosecutorial due process regime that is recognized both domestically and internationally, the missions of lethality raise the question of international sovereignty and compliance with host nation laws. These missions are potentially taking place in territories that are not per se war zones or not clearly recognized battlefields in the traditional sense. Lethality against either citizens of the host nation or noncitizens there illegally or legally, raises fundamental questions about the rule of law. Why is capture for prosecution not the first option? In international law, there is much discussion of “international armed conflicts” versus “non-international armed conflicts.” The categorization of these

---

conflicts flows from Additional Protocol I and Additional Protocol II,\(^{44}\) two conventions the United States has declined to ratify at this time. In a non-international armed conflict under Additional Protocol I, the host state may have to accord Geneva Convention rights to the “rebels” as perceived by the host state.\(^ {45}\) Whether the “rebels” is a legitimate target turns on a number of facts, including whether the individual is a “direct participant in hostilities,” a designation that is hotly debated in international circles.\(^ {46}\) In situations of some ambiguity, without capture as an option and some due process, how is the shooter sure the target is the legitimate target? Moreover, two of the principles of the law of armed conflict are the principle of distinction between combatants and civilians and the requirement of proportionality to minimize noncombatant causalities.

If capture becomes an option for strategic reasons, then a choice of using criminal courts, military commissions, special national security courts, host courts, or an international tribunal are then raised. Regardless of the court employed, the issue of appropriate due process is the central question. What is critical is that the process has legitimacy and comports with rule of law. To this end, Additional Protocol I Article 75 establishes the basic due process for individuals captured in conflict situations and deserves to be quoted in full so that the basic rights it entails are understood. It reads as follows:

**Article 75—Fundamental guarantees**

1. In so far as they are affected by a situation referred to in Article 1 of this Protocol, persons who are in the power of a Party to the conflict and who do not benefit from more favourable treatment under the Conventions or under this Protocol shall be treated humanely in all circumstances and shall enjoy, as a minimum, the protection provided by this Article without any adverse distinction based upon race, colour, sex, language, religion or belief, political or other opinion, national or social origin, wealth, birth or other status, or on any other similar criteria. Each Party shall respect the person, honour, convictions and religious practices of all such persons.

2. The following acts are and shall remain prohibited at any time and in any place whatsoever, whether committed by civilian or by military agents:

(a) Violence to the life, health, or physical or mental well-being

---


of persons, in particular:
(i) Murder;
(ii) Torture of all kinds, whether physical or mental;
(iii) Corporal punishment; and
(iv) Mutilation;
(b) Outrages upon personal dignity, in particular humiliating and degrading treatment, enforced prostitution and any form of indecent assault;
(c) The taking of hostages;
(d) Collective punishments; and
(e) Threats to commit any of the foregoing acts.
3. Any person arrested, detained or interned for actions related to the armed conflict shall be informed promptly, in a language he understands, of the reasons why these measures have been taken. Except in cases of arrest or detention for penal offences, such persons shall be released with the minimum delay possible and in any event as soon as the circumstances justifying the arrest, detention or internment have ceased to exist.
4. No sentence may be passed and no penalty may be executed on a person found guilty of a penal offence related to the armed conflict except pursuant to a conviction pronounced by an impartial and regularly constituted court respecting the generally recognized principles of regular judicial procedure, which include the following:
(a) The procedure shall provide for an accused to be informed without delay of the particulars of the offence alleged against him and shall afford the accused before and during his trial all necessary rights and means of defence;
(b) No one shall be convicted of an offence except on the basis of individual penal responsibility;
(c) No one shall be accused or convicted of a criminal offence on account of any act or omission which did not constitute a criminal offence under the national or international law to which he was subject at the time when it was committed; nor shall a heavier penalty be imposed than that which was applicable at the time when the criminal offence was committed; if, after the commission of the offence, provision is made by law for the imposition of a lighter penalty, the offender shall benefit thereby;
(d) Anyone charged with an offence is presumed innocent until proved guilty according to law;
(e) Anyone charged with an offence shall have the right to be tried in his presence;
(f) No one shall be compelled to testify against himself or to
confess guilt;

(g) Anyone charged with an offence shall have the right to examine, or have examined, the witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;

(h) No one shall be prosecuted or punished by the same Party for an offence in respect of which a final judgment acquitting or convicting that person has been previously pronounced under the same law and judicial procedure;

(i) Anyone prosecuted for an offence shall have the right to have the judgment pronounced publicly; and

(j) A convicted person shall be advised on conviction of his judicial and other remedies and of the time-limits within which they may be exercised.

5. Women whose liberty has been restricted for reasons related to the armed conflict shall be held in quarters separated from men’s quarters. They shall be under the immediate supervision of women. Nevertheless, in cases where families are detained or interned, they shall, whenever possible, be held in the same place and accommodated as family units.

6. Persons who are arrested, detained or interned for reasons related to the armed conflict shall enjoy the protection provided by this Article until their final release, repatriation or re-establishment, even after the end of the armed conflict.

7. In order to avoid any doubt concerning the prosecution and trial of persons accused of war crimes or crimes against humanity, the following principles shall apply: (a) Persons who are accused of such crimes should be submitted for the purpose of prosecution and trial in accordance with the applicable rules of international law; and

(b) Any such persons who do not benefit from more favourable treatment under the Conventions or this Protocol shall be accorded the treatment provided by this Article, whether or not the crimes of which they are accused constitute grave breaches of the Conventions or of this Protocol.

8. No provision of this Article may be construed as limiting or infringing any other more favourable provision granting greater protection, under any applicable rules of international law, to persons covered by paragraph 1.47

If such a regime had been in place over the last ten years, the option to capture and prosecute under an internationally recognized process would have given policy makers more choices. To a great extent, the recent changes to the military commissions rules have come very close to replicating the Article 75 guarantees. Covert actions that

47. Protocol I, supra note 12.
also have the option for capture and prosecution make the tool more nuanced and potentially more powerful in the struggle against violent extremism.

VIII. CONCLUSION

In summary, the modern battlefield, and the adaptive enemy therein, presents legal issues in deciding between covert action and traditional military activities. As a matter of law, the President may authorize any agency to conduct a covert action via presidential finding. Alternatively, the President must justify the use of force under traditional military activities under *jus ad bellum* doctrines in domestic and international law. While covert action has an important function in providing policymakers a precise tool to use in the spectrum between diplomatic and military force, legal bodies must use caution to ensure the “Fifth Function” is being used properly and not merely to circumvent legal requirements or media accountability. This accountability is especially important since it is politically easier for the executive branch to authorize covert action. This Article has also explored the idea of expanding covert action with the potential for capture and prosecution under an internationally recognized due process regime. Understanding this increasingly blurred line will not be easy, but if the general and statesman are to truly understand the nature of the war upon which they are embarking, an expanded covert action may function as a useful policy tool within the bounds of the law. In the end, as this Article has underscored, accountability married to the legitimacy of the rule of law is the core to a coherent grand strategy.

---

48. 50 U.S.C. § 413b(a), (e)(1)-(4).
49. Clausewitz, supra note 1.
ARTICLE

Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action

*Andru E. Wall*

Abstract

Modern warfare requires close integration of military and intelligence forces. The Secretary of Defense possesses authorities under Title 10 and Title 50 and is best suited to lead US government operations against external unconventional and cyber threats. Titles 10 and 50 create mutually supporting, not mutually exclusive, authorities. Operations conducted under military command and control pursuant to a Secretary of Defense-issued execute order are military operations and not intelligence activities. Attempts by congressional overseers to redefine military preparatory operations as intelligence activities are legally and historically unsupportable. Congress should revise its antiquated oversight structure to reflect our integrated and interconnected world.

I. Introduction

After being hunted for nearly ten years, Osama Bin Laden was shot and killed by U.S. Navy SEALs in the early hours of May 2, 2011. The identity of the elite special operations unit that conducted the raid on bin Laden’s compound in Pakistan was not immediately released, as the

* Senior Associate with Alston & Bird LLP; former senior legal advisor for U.S. Special Operations Command Central (2007 to 2009). While this article was cleared for publication as required by my security clearance and nondisclosure agreements, the views expressed herein are my own and do not necessarily reflect the position of the U.S. government or Department of Defense. I thank Harvard Law School for its generous support of this paper and Jack Goldsmith, Hagan Scotten, Mark Grdovic, Nick Dotti, Chris Costa, Michael Bahar, and Lenn Ferrer for their invaluable comments and suggestions. To my beloved wife, Yashmin, and two adorable children, Isabella and David Alejandro, thank you for your extraordinary patience and support as I repeatedly disappeared to work on this article.

Copyright © 2011 by the Presidents and Fellows of Harvard College and Andru E. Wall
operation was described as covert. Yet as rumors swirled and information leaked to the media, Leon Panetta, the head of the Central Intelligence Agency (CIA) and soon-to-be-head of the Department of Defense (DoD), clarified during an interview that the operation to kill or capture bin Laden was a “Title 50” covert operation. Panetta explained that the raid was commanded by the President through Panetta, although “the real commander” was the head of Joint Special Operations Command, Vice Admiral William McRaven—the on-scene commander “actually in charge of the military operation that went in and got bin Laden.”

Panetta’s description of the bin Laden raid as a covert “Title 50” operation with a chain of command that included military commanders and the Director of Central Intelligence renewed a long-simmering debate within the national security community over “Title 10” and “Title 50” authorities. Titles 10 and 50 are part of the U.S. Code, but why would Panetta invoke a statute, the legal authority, to explain who was in charge of an operation conducted by military forces? We will see in a moment that the answer has everything to do with an antiquated congressional oversight paradigm and little to do with actual legal authorities.

The Title 10-Title 50 debate is the epitome of an ill-defined policy debate with imprecise terms and mystifying pronouncements. This is a debate, much in vogue among national security experts and military lawyers over the past twenty years, where one person gravely states “there are some real Title 10-Title 50 issues here,” others in the room affirmatively, and with furrowed brows all express agreement. Yet the terms of the debate are typically left undefined and mean different things to different people. If you

---

2 Admiral Vern Clark, former Chief of Naval Operations of the U.S. Navy, Professor John Radsan, a former assistant general counsel for the CIA, and Professor Gregory McNeal, a former Department of Justice lawyer, were asked “what is Title 10 authority?” and “what is Title 50 authority?” during a panel discussion at a law school symposium on national security law. Admiral Clark phrased the debate as one “about the line between covert and overt” (an issue we will examine in Part IV of this paper), yet his articulation of this concern focused on military transparency and public perceptions about the military. Professor Radsan framed the debate in terms of defined roles for the military and intelligence communities, while Professor McNeal opined that military lawyers advising special operations forces are often confused about the legal basis for their actions. National Security Symposium: The Battle Between Congress & The Courts in the Face of an Unprecedented Global Threat: Legislation Panel: Discussion & Commentary, 21 REGENT U.L. REV. 331, 347 (2009) [hereinafter “National Security Symposium”].
ask four military lawyers or DC policy wonks to define what “Title 10-Title 50 issues” means, you could get four different answers each cloaked in another layer of ambiguity, intrigue, and ignorance.

The Title 10-Title 50 debate is essentially a debate about the proper roles and missions of U.S. military forces and intelligence agencies. “Title 10” is used colloquially to refer to DoD and military operations, while “Title 50” refers to intelligence agencies, intelligence activities, and covert action. Concerns about appropriate roles and missions for the military and intelligence agencies, or the “Title 10-Title 50 issues” as commonly articulated, can be categorized into four broad categories: authorities, oversight, transparency, and “rice bowls.” The first two concerns,

3 See, e.g., comments by James A. Lewis of the Center for Strategic and International Studies:

You have intelligence authorities, Title 50, and you have military authorities, Title 10. Well, what does the commander of Cyber Command do? Does he get to pick and choose between them? You need some way to say, “This kind of thing is military, you have to use the military decision chain,” versus, “this kind of thing is intelligence, you have to use the intelligence decision chain.” I’m not sure they’ve worked through all of that.

4 “Authorities” is a term commonly used by government lawyers and military personnel to describe statutory and delegated powers. For example, Title 10 of the U.S. Code created the Office of the Secretary of Defense and assigned the Secretary of Defense all “authority, direction and control” over DoD, including all subordinate agencies and commands. 10 U.S.C. § 113(b). Title 10 later created U.S. Special Operations Command (USSOCOM) and lists several tasks or missions that USSOCOM “shall be responsible for, and shall have the authority to conduct.” 10 U.S.C. § 167. The President, in his role as Commander in Chief, may delegate through the Secretary of Defense additional responsibilities or “authorities” to USSOCOM, just as the Secretary of Defense may delegate certain of his statutory authorities to USSOCOM. These statutory and delegated responsibilities fall under the general rubric of “authorities.” If the Commander of USSOCOM wants to conduct a given activity, he must first determine whether he possesses the statutory or delegated authority to use assigned personnel and resources to conduct the activity in question. Double-Tongued Dictionary defines “rice bowl” as: “in the military, a jealously protected program, project, department, or budget; a fiefdom. Etymological Note: Perhaps related to the Chinese concept of the rice bowl as a metaphor for the basic elements required to live, as seen, for example, in the iron rice bowl, employment that is guaranteed for life.” Dictionary definition of “rice bowl”, DOUBLE-TONGUED DICTIONARY,
authorities and oversight, are grounded in statutes and legislative history and are the focus of this article. The second two concerns, transparency and "rice bowls," can be quickly identified and dismissed as policy arguments rather than legitimate legal concerns.

Before delving into the law, we must first dismiss the policy arguments masquerading as Title 10-Title 50 issues. Transparency is the most amorphous concern in the Title 10-Title 50 debate. Often unacknowledged, the essence of this concern is the belief that intelligence operatives live in a dark and shadowy world, while military forces are the proverbial knights on white horses. Advocates of military transparency want to ensure the reputation of America's men and women in uniform remains unmarred by association with the shadowy world of espionage. For these people, the Title 10-Title 50 debate is a debate about whether military forces should be engaged in "secret operations" or "go over to the dark side." Because secret

http://www.doubletongued.org/index.php/dictionary/rice_bowl (last visited Feb. 9, 2010). For an example of usage, see "Gingrich pledged 'to cooperate in any way I can on a bipartisan basis in really rethinking all of this' because the effort is 'going to require not only reshaping the rice bowls at the Pentagon but breaking a few of them.'" Fred Kaplan, In House, Bipartisan Drive is Growing to Slash Defense, BOSTON GLOBE, Jul. 29, 1990, at 2. See also "Attempting to take the moral high ground in a debate that in the past has been characterized by high emotions as each service sought to protect its own 'rice bowls.'" Army Seeks Moral High Ground In Briefing to Roles Panel, 184 DEFENSE DAILY 53 (Sept. 15, 1994).

5 The U.S. military consistently ranks at the apex of most-trusted institutions in the United States. This trust is critical to America's all-volunteer military and some even suggest the trust disparity between Congress and the military is one reason why Congress is loath to publicly attack military policies. David Hill, Respect for Military Surges, THE HILL (Jul. 18, 2006), http://thehill.com/opinion/columnists/david-hill/8251-respect-for-military-surges. A 2009 Gallop poll found 82% of Americans have a "great deal" or "quite a lot" of respect for the U.S. military, versus only 17% who felt the same way about Congress. Lydia Saad, Congress Ranks Last in Confidence in Institutions, GALLOP (July 22, 2010), http://www.gallup.com/poll/141512/congress-ranks-last-confidence-institutions.aspx.

6 In the words of Admiral Clark:

This line that exists [between covert and overt] is part of our good standing in the world. We have carefully tried to keep the military cut of the covert world . . . . The covert side has appropriately resided within the CIA. We want the citizens, when they look at men and women wearing the cloth of the nation, to know that is who they are.

National Security Symposium, supra note 2, at 347.

7 "Secret operations" includes both covert and clandestine operations, which are terms this article will explore in greater detail in Parts III and IV. Professor Robin Williams argues "our cultural values do greatly affect our willingness as a nation to engage in
operations (used here in the colloquial sense that includes covert and clandestine operations) often require operating out of uniform, there are also concerns that military forces conducting such operations could lose protections under the Geneva Conventions (e.g., treatment as prisoners of war rather than as spies), increase risks to all U.S. military personnel serving abroad, and possibly endanger morale by sacrificing what is viewed as the moral high ground.  

The second policy argument can be colloquially described as the “rice bowls” concern, which employs military jargon to describe those who jealously guard assigned programs, resources, and responsibilities. Bureaucrats jealously protect their “rice bowls” for two main reasons: to strengthen their position in the competition for scarce resources and to preserve their “lanes” or operational primacy in a given area. Broadly speaking, proponents of the “rice bowls” concern contend that Title 50 and Presidential orders make the CIA the lead U.S. agency for the collection of human intelligence and conduct of covert action, yet the military is unconventional warfare and do affect our policies and strategies in dealing with the widespread threats posed by infiltration and subversion on the part of hostile powers in many parts of the world.” Robin M. Williams Jr., Are Americans and Their Cultural Values Adaptable to the Concept and Techniques of Unconventional Warfare?, 341 ANNALS AM. ACAD. POL. & SOC. SCI. 82, 83 (1962), available at http://www.jstor.org/stable/1034146. Professor Williams suggests that “many Americans have come to think of unconventional warfare . . . in connection with the premeditated use of deception, subversion, and terror” and, thus, view unconventional warfare as incompatible with American values.


For a discussion of the term “rice bowls,” see supra note 4.

EXEC. ORDER NO. 12,333, 46 Fed. Reg. 59941 (Dec. 4, 1981), amended by EXEC. ORDER NO. 13,470, 73 Fed. Reg. 45,325 (July 30, 2008) [hereinafter E.O. 12,333], and 50 U.S.C. § 403-4a. During the Cold War, intelligence collection was organized by source and lead agency. The CIA was primarily responsible for human intelligence (HUMINT); the National Security Agency (NSA) was primarily responsible for signals intelligence (SIGINT); and the National Geospatial Intelligence Agency was primarily responsible for overhead imagery intelligence (IMINT). As one intelligence expert explains: “There was, perhaps, a certain logic to that organization during the Cold War. With one overwhelming target—the Soviet Union—the various “INTs” were asked, in effect, what they could contribute to understanding the puzzle of the Soviet Union.” GREGORY F. TREVERTON, INTELLIGENCE FOR AN AGE OF TERROR 6 (2009). Treverton points out that on the analytic side, this organization permitted competition, of sorts, as the CIA focused on the national and political aspects of intelligence, while the Defense Intelligence Agency and service intelligence elements “naturally focused more on military dimensions of problems that cut across the military and political.” Id. at 50. There is an ongoing debate over whether
stealing from the CIA’s “rice bowl” by expanding its human intelligence capabilities under the guise of Title 10 authorities. The belief is that this expansion by the military threatens to divert resources from the CIA and could lead to operational deconfliction issues.\textsuperscript{11} For the CIA and its Congressional proponents, the concern is that the CIA’s legal role as lead agency is diminished as it is dwarfed in size by the military’s rapidly expanding human intelligence capabilities.\textsuperscript{12} When budgets shrink and resources are scarce, the fear is the CIA will be disproportionately impacted.

The related rice bowls concern “lanes” raises actual operational issues. If the military’s human intelligence collection resources dramatically exceed the CIA’s resources, the CIA may find it difficult to execute its statutory role as lead agency for the coordination and deconfliction of U.S. government human intelligence collection.\textsuperscript{13} A few hundred CIA officers may find it impossible to coordinate and deconflict the human intelligence activities conducted by thousands of military personnel, thereby de facto ceding the CIA’s statutory primacy.\textsuperscript{14} In a worst-case scenario, the failure to

organizing intelligence collection in this manner remains appropriate to respond to the threats of the 21st century.

\textsuperscript{11} To those on the CIA’s side, human intelligence collection efforts would see “a quantum improvement in capability” if “lanes” across the intelligence community were enforced. John MacGaffin, \textit{Clandestine Human Intelligence: Spies, Countespies, and Covert Action}, in \textbf{TRANSFORMING U.S. INTELLIGENCE} 79, 91 (Jennifer E. Sims & Burton Gerber, eds., 2005). The term “deconfliction” is commonly used in military and intelligence circles to refer to processes or coordination intended to ensure that various operations or activities do not interfere with each other.


\textsuperscript{13} During confirmation hearings for General Michael Hayden after he was nominated in 2006 to become Director of the CIA, Senator Olympia Snowe opined that as the military seeks to “further expand and encroach in areas . . . [such as] clandestine forces, paying informants, gathering deeper and deeper into human intelligence, I think that this is going to be a serious—potentially—contest if the CIA does not regain its ground and reclaim its lost territory.” \textit{Nomination of General Michael V. Hayden, USAF to be Director of the Central Intelligence Agency: Hearing Before the S. Select Comm. on Intelligence, 109th Cong., 2nd Sess. 50} (2006) [hereinafter \textit{Hayden Nomination}].

\textsuperscript{14} The DoD controls about 80% of the intelligence budget, which presumably only includes DoD agencies that are also part of the intelligence community; most of the 80% is spent on
maintain clear operational lanes could lead to operatives unintentionally impeding or even exposing each other’s human intelligence efforts. The salient point, however, is not that the military is exceeding its statutory authority, but rather that both the military and intelligence agencies possess the statutory authority to conduct intelligence-gathering activities that may be indistinguishable “to the naked eye.”

This is a valid operational concern and unremitting management challenge; intelligence agencies must strive to ensure the military’s intelligence collection activities are coordinated, deconflicted, and conducted according to established standards.

None of these concerns suggest that a certain activity (or method of conducting that activity) is inconsistent with statutory or legal authority; rather, each suggests that a certain activity ought not to be conducted (or ought to be conducted) a certain way because of practical effects. Guarding the U.S. military’s reputation and protecting an agency’s resources are legitimate policy considerations, just as preserving lanes and ensuring deconfliction is a crucial operational concern. Yet it is misleading to couch these policy and operational debates in terms of statutory law, and it is misleading to label these concerns as “Title 10-Title 50” issues. Transparency, rice bowls and lanes are concerns that can be adequately addressed by sound Executive Branch management and proper allocation of resources by Congress.

Having defined the Title 10-Title 50 debate and summarily exposed the policy arguments and operational challenges that often masquerade as legal issues, this article now turns in Part II to analyzing the significant legal authorities given to the President and Secretary of Defense under the U.S. Constitution and Titles 10 and 50 of the U.S. Code. That “Title 10” is commonly used to refer to DoD and to articulate the legal basis for military operations is understandable. However, the use of “Title 50” to refer solely to activities conducted by the CIA is, at best, inaccurate as the Secretary of Defense also possesses significant authorities under Title 50.


15 General Hayden correctly noted “that what DoD is doing under title 10 authorities and what CIA does under title 50 may be indistinguishable to the naked eye . . . get kind of merged so that the actions are actually on the ground, in reality indistinguishable, even though their sources of tasking and sources of authority come from different places.” Hayden Nomination, supra note 13, at 50–51.
After establishing the relevant legal authorities, Part III discusses Congressional oversight, which reveals itself as the true Title 10-Title 50 issue. It is Congress’s antiquated oversight structure and a concomitant misunderstanding of the law that casts a shadow of concern and purported illegitimacy over military operations that resemble activities conducted by intelligence agencies. Congress’s stovepiped view of national security operations is legally incongruous and operationally dangerous because it suggests statutory authorities are mutually exclusive and it creates concerns about interagency cooperation at exactly the time in history when our policy and legal structures should be encouraging increased interagency coordination and cooperation against interconnected national security threats.

Concern over purported Title 10-Title 50 issues arises most often in the context of discussions over unconventional and cyber warfare. While most details of how these operations are conducted are not publicly available, Part IV will define unconventional warfare and cyberwarfare and generally explain their purpose, role, and conduct. These military operations are conducted in secret and in environments where public acknowledgement of the U.S. military’s involvement may raise diplomatic and national security concerns (e.g., other countries and cyberspace), which is why Congressional intelligence committees often mistakenly conclude they should have oversight of these military operations. However, when the law (and even Congress’s own legislative history) is applied to unconventional warfare and cyberwarfare in Part IV, it becomes apparent that these are military operations rather than intelligence activities so long as they remain under the command and control of a military commander and are conducted prior to or during (anticipated or actual) acknowledged military operations. Part V offers a few concluding thoughts and recommendations.

II. The Law Permits While Congress Attempts to Restrict

The Title 10-Title 50 debate is typically invoked to express concerns that the military is taking over missions and activities “properly” within the sole domain of the intelligence agencies. While ordinary Americans in the heartland may care only that U.S. national security objectives are effectively accomplished, military and intelligence bureaucrats and their Congressional overseers remain obsessed with who actually does the mission. Yet a careful
analysis of the law and related legislative history shows how the law permits much of what Congress attempts to restrict with its stovepiped approach to oversight of the military and intelligence community.

A. Legal Authorities

Professor Gregory McNeal, sitting on a law school panel discussing Title 10-Title 50 issues, suggested that lawyers advising special operations units may have trouble discerning whether they are operating under Title 10 or Title 50 authorities. McNeal elaborated:

When the military goes out, there are JAGs who sit with intelligence agents or officials and advise on whether it is lawful to strike a specific target or engage in a specific operation. If a JAG is seated in a targeting cell in a special operations unit, the first question will still be whether a certain target can be attacked. However, the second question that the officer in that cell will oftentimes ask is whether he is operating under Title 10 or Title 50 authority. If it is a CIA drone, the answer may be that it is fine to hit the target. Under Title 10 the answer may be, no you cannot.

Professor McNeal’s hypothetical evidences a misunderstanding or miscalculation of the law and conduct of military operations. Military personnel, including Professor McNeal’s hypothetical “special operations unit,” operate under military direction and control and under Title 10 authority. CIA personnel operating under a CIA direction and control operate under Title 50 authorities. CIA personnel operating with military personnel may use their Title 50 authorities to support a Title 10 operation, but they would still be operating under Title 50 authority; likewise, a

---

16 National Security Symposium, supra note 2, at 348–49.
17 Id. at 349.
18 Professor McNeal may be confusing or merging statutory authority with delegated authorities such as rules of engagement (ROE). For example, in the hypothetical McNeal presents, it is theoretically possible that the CIA drone (operating under Title 50 authority in support of a Title 10 military operation) may be operating under different ROE than the special operations unit it is supporting. The CIA rules of engagement may provide that a target can be attacked if X+Y exists, while the military ROE may require X+Y+Z, i.e. the CIA ROE may be more or less permissive than the military ROE. But rules of engagement are policy directives, not statutes, so their characterization as a “Title 10” or “Title 50” issue is inaccurate and misleading.
military unit operating under Title 10 authority could support a Title 50 operation (if they are given such delegated authority). In other words, when an operation is termed a “Title 10” operation, that statutory label simply refers to the statutory origins of the mission commander’s authority; this does not preclude other government agencies operating under separate statutory authorities from using their personnel and resources to support the “Title 10” operation.

1. The President’s Constitutional Authority

Our analysis of legal authorities possessed by military commanders begins with the executive and commander-in-chief powers, delineated in the U.S. Constitution and applicable federal statutes, and delegated from the President through the Secretary of Defense down to subordinate commanders. Delegated authorities derive from a myriad of Executive Branch policy documents, including directives issued by various echelons within DoD. As the overwhelming majority of directives relating to unconventional and cyber warfare are classified, our discussion here will focus on the statutes: policy may restrict statutory authorities, but policy can also be changed at the President’s direction. While the majority of national security decisions are made on a daily basis pursuant to statutory and delegated authority, there is no question that the President is the head of the executive branch and commander in chief.

The President’s authority to direct military operations and intelligence activities against external threats resides in his Constitutional executive and commander-in-chief powers. The President is vested with

---

19 Challenges do arise when special operations forces (SOF) operate with CIA personnel, as happened in Afghanistan in late 2001 and in Iraq in early 2003. Operators may ask when tasked with a particular mission: “am I conducting this mission under Title 10 or Title 50 authorities?” The question, however, is generally one of fiscal authorities rather than operational authorities. Are CIA funds or DoD funds being used to pay for the operation? If the CIA is paying a particular Northern Alliance commander to employ his forces in furtherance of U.S. military objectives, is that a Title 10 activity or a Title 50 activity? Can SOF employ indigenous forces trained and equipped by the CIA under Title 50 authorities in furtherance of SOF’s Title 10 missions? These are important questions that require close examination of the relevant operational orders and fiscal authorities.


21 The President is vested with executive power by Article II, Section 1 of the U.S. Constitution; Section 2 adds commander-in-chief powers.
executive power and is the "sole organ of the federal government in the field of international relations—a power which does not require as a basis for its exercise an act of Congress." As chief executive, the President may "manage the business of intelligence in such a manner as prudence may dictate." This includes the authority to secretly collect intelligence for reasons of national security. As commander in chief, the President may employ the military to protect the national interests of the United States as he deems necessary.

The President does not wield these powers exclusively, however, as Congress is given the authority to "raise and support Armies," to "provide and maintain a Navy," to appropriate funds to support the military, and to issue formal declarations of war. Simply put, Congress decides how to resource the U.S. military and when to formally declare war, while the President decides how to employ the military in furtherance of U.S. national security objectives—subject always to constitutionally permissive constraints enacted by Congress and available funding.

Perhaps the most significant restraint, or attempted restraint, upon Presidential employment of the military is contained in the War Powers Resolution of 1973, which directs the President to notify Congress within 48-hours after deploying military forces in situations where hostilities are

---

22 U.S. CONST. art. II, § 1.
23 United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 320 (1936). Note, however, that "sole" does not mean the Supreme Court will not on rare occasions conduct its own inquiry to ensure that Presidential assertions that particular actions are grounded in these powers, are so in fact. In Youngstown, President Truman contended that his Constitutional commander-in-chief authorities permitted the seizure of steel mills in the United States, but the Supreme Court held: "we cannot with faithfulness to our constitutional system hold that the Commander in Chief of the Armed Forces has the ultimate power as such to take possession of private property in order to keep labor disputes from stopping production." Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 587 (1952).
24 The Federalist No. 64 (John Jay).
25 See, e.g., Chicago & S. Air Lines v. Waterman S.S. Corp., 333 U.S. 103, 111 (1948); Totten v. United States, 92 U.S. 105, 106 (1876) (The President "was undoubtedly authorized during the war, as commander-in-chief, to employ secret agents to enter rebel lines and obtain information respecting the strengths, resources, and movements of the enemy.").
26 In the Prize Cases, the U.S. Supreme Court held that determinations of belligerency and threats to national security are questions to be decided by the President. Prize Cases, 67 U.S. 635, 670 (1863).
anticipated.\textsuperscript{28} The President must generally withdraw the military forces within sixty days unless Congress formally declares war or otherwise authorizes the combat deployment.\textsuperscript{29} The War Powers Resolution was passed over President Richard Nixon's veto, and every subsequent President has also believed that "the War Powers Resolution is an unconstitutional infringement by the Congress on the President's authority as Commander-in-Chief."\textsuperscript{30}

This Constitutional separation or balancing of power between the President and Congress with respect to war powers sparked intense debate nearly as soon as the Constitution was ratified. Discussions of the President's constitutional authority as commander in chief implicate "some of the most difficult, unresolved, and contested issues in constitutional law."\textsuperscript{31} This debate is perhaps best pictured as a Venn diagram: some assert a circle of "inherent" Presidential power, some favor a circle of Congressional checks on "imperial" Presidential power, while others see a Constitutional overlap or balancing of powers between the two branches. One scholar astutely observes that "[w]riters on the relative powers of the presidency versus the Congress almost invariably lapse into advocacy when they comment on the textual, historical or functional bases of war powers."\textsuperscript{32}

Those who favor presidential powers in the realm of national security point to the President's enumerated powers, namely the "executive

\textsuperscript{29} Two key provisions in the War Powers Resolution link the President's authority to deploy military forces for reason of national security with Congress's power of the purse: the President must notify Congress when troops are deployed equipped for combat, 50 U.S.C. § 1543(a)(1), after which Congress has sixty days to authorize the deployment or the President must terminate the use of force. 50 U.S.C. § 1544(b).
\textsuperscript{30} CONGRESSIONAL RESEARCH SERVICE, WAR POWERS RESOLUTION: PRESIDENTIAL COMPLIANCE 2 (2002). It is worth noting that President Nixon's veto centered on two Constitutional concerns: the provision under which funding would be automatically cut off if Congress fails to act within 60–90 days after Presidential notification (§ 1544(b)), and the provision permitting Congress to direct cessation of the deployment by passage of a mere concurrent resolution, which normally does not have power of law. President Nixon believed that only an affirmative act of Congress could override the President's decision to deploy military forces under his Commander-in-Chief authority. Letter from President Richard M. Nixon to the House of Representativies, Veto of the War Powers Resolution (Oct. 24, 1973), available at http://www.presidency.ucsb.edu/ws/index.php?pid=4021.
\textsuperscript{32} Michael Bahar, Axes of Power: Predicting the Reception of Assertions of Presidential War Powers In the Courts, 58 NAVAL L. REV. 1, 1 (2009).
Power” of Article II, section 1 and the “Commander in Chief” power of Article II, section 2. They assert the only constitutional limitations on those powers are Congress’s power of the purse and power to formally declare war.\textsuperscript{33} In other words, in situations where a declaration of war is not required (e.g., self-defense or peacetime intelligence activities), the only way Congress can impede Presidential power is by cutting off funding.

Advocates of Congressional war powers, however, argue against rigid interpretations of the Constitutional text and quote James Madison and other framers of the Constitution at length to support their vision of a “national security Constitution” where “Congress, the courts, and the Executive should interact in the foreign policy process.”\textsuperscript{34} These advocates argue that “[t]he constitutional framework adopted by the Framers is clear in its basic principles. The authority to initiate war lay with Congress. The President could act unilaterally only in one area: to repel sudden attacks.”\textsuperscript{35}

While reviewing two diametrically opposed books on Presidential war powers, Professor Jack Goldsmith succinctly summarizes the intellectual history of arguments debating Presidential and Congressional war powers before wryly observing “that constitutional theory is usually grounded in a theory of preferred outcomes.”\textsuperscript{36} Presidential power has grown of necessity beyond what the framers could have imagined, yet meaningful Congressional checks on Presidential power remain and “translate, in a


\textsuperscript{35} FISHER, supra note 34, at 11.

rough way, the Framers’ original design.”37 Goldsmith concludes: “the larger picture is one that preserves the original idea of a balanced constitution with an executive branch that remains legally accountable despite its enormous power.”38

2. The Secretary of Defense’s Statutory Authorities

Congress modernized and reorganized the U.S. national security establishment in the National Security Act of 1947.39 The act merged the War and Navy departments into the DoD, and created the National Security Council, CIA, National Security Agency (NSA), and other agencies. The Act also established a formalized process for national security decision-making and Congressional oversight of intelligence activities. The National Security Act of 1947, as amended, is found in Title 50 of the U.S. Code.40

In 1956 and 1962, Congress removed from Title 50 provisions relating to organization and functions of the services and DoD and placed these provisions with amendments in Title 10 of the U.S. Code.41 In 1986, following the failed Iran hostage rescue mission, Congress legislated a new “joint” structure of command and control through which the President exercises his commander-in-chief responsibilities.42

The President exercises Constitutional authority as Commander in Chief through the Secretary of Defense who is also his “principal assistant . . . in all matters relating to the Department of Defense.”43 Title 10 gives the Secretary of Defense all “authority, direction and control” over DoD, including all subordinate agencies and commands.44 Title 10 also created combatant commands, which include geographic commands (e.g., U.S.

37 Id.
38 Id.
41 10 U.S.C. §§ 101–18505. Laws pertaining to the National Guard were transferred to Title 32.
43 10 U.S.C. § 113(b) (2006). Title 10 specifically states that DoD is part of the executive branch, which removes any doubt about the President’s authority over the department under both section 1 (executive power) and section 2 (Commander-in-Chief power) of Article II of the U.S. Constitution. See 10 U.S.C. § 111 (2006).
European Command) and U.S. Special Operations Command (USSOCOM). Title 10 gives combatant commands statutory authorities and their commanders report directly to the Secretary of Defense. For example, Title 10 gives USSOCOM authority over the following activities when conducted by special operations forces: direct action, strategic reconnaissance, unconventional warfare, foreign internal defense, civil affairs, psychological operations, counterterrorism, humanitarian assistance, theater search and rescue, and such other activities as may be specified by the President or the Secretary of Defense.

Title 50 establishes, defines and delineates authorities within the intelligence community, but it also clarifies that the Secretary of Defense controls those members of the U.S. intelligence community, such as the NSA and Defense Intelligence Agency, that are part of DoD. The Secretary of Defense's control and direction of DoD human intelligence activities can be limited only by the President. This provision is reinforced by Title 10, which creates an Undersecretary of Defense for Intelligence to whom the Secretary of Defense may delegate duties and powers "in the area of intelligence." Finally, Executive Order 12,333, which has regulated the U.S. intelligence community for nearly thirty years, directs the Secretary of Defense to "collect (including through clandestine means), analyze, produce, and disseminate information and intelligence [as well as] . . . defense and defense-related intelligence and counterintelligence . . . ."

One source of confusion in the Title 10-Title 50 debate springs from Title 50's use of the term "national intelligence." The discussion of "national intelligence" in Title 50 causes some to opine that "national intelligence" is separate and distinguishable from military intelligence, yet

45 10 U.S.C. §§ 161, 162, 164, 165, 166, 166a, 166b, & 168 (2006). In practice, the combatant commanders communicate with the Secretary of Defense via the Joint Staff. Although the Chairman of the Joint Chiefs of Staff is not technically or legally in the chain-of-command, his statutory role is that of advisor to the President and Secretary of Defense. The Chairman of the Joint Chiefs of Staff has a staff of several thousand personnel, the Joint Staff, through which all operational orders and communications to and from the Secretary of Defense flow.
48 Id. at § 403–5(b)(5) (2006). See also supra note 10.
50 E.O. 12,333, supra note 10, at ¶1.10.
51 See 50 U.S.C. §401a(5) (2006). Intelligence activities are further stove-piped. Following the passage of the National Security Act of 1947 and continuing through the end of the
other provisions of Title 50 include references to the intelligence needs of combatant commanders, tactical intelligence activities, and the intelligence needs of the military's operational forces. These terms, read in the context of Title 50, suggest labels based on the intended primary consumer of the intelligence, or its primary purpose, not an attempt to categorize or label intelligence by type or the agency collecting the intelligence.

There is no rigid separation between Title 10 and Title 50. A more accurate interpretation is simply that Title 10 clarifies roles and responsibilities within DoD, while Title 50 clarifies roles and responsibilities within the intelligence community; both titles explicitly recognize that the Secretary of Defense has statutory roles and authorities under Title 10 and under Title 50. Executive Order 12,333 confirms this reading by directing the Secretary of Defense to collect intelligence for both his department and the intelligence community writ large. U.S. military doctrine further erodes any attempted distinction between tactical, operational, and strategic intelligence:

National assets such as intelligence and communications satellites, previously considered principally in a strategic context, are an important adjunct to tactical operations. Actions can be defined as strategic, operational, or tactical based on their effect or contribution to achieving strategic, operational, or tactical objectives, but many times the accuracy of these labels can only be determined during historical studies.

Read in concert with Title 10, Title 50 does not infringe upon the Secretary of Defense's authorities to collect intelligence. Rather, Title 50 recognizes the authorities assigned to the Secretary of Defense under Title 10 over all

Cold War, the U.S. national security establishment maintained a distinction between military or tactical intelligence and national or foreign intelligence. In the context of the Cold War, this distinction made sense. Domestic, foreign, and military intelligence were three separate categories with separate legal authorities and executing agencies. The Director of Central Intelligence leads and directs national intelligence collection activities under authorities found in Title 50. The Intelligence Community components of DoD often collected foreign intelligence in response to national tasking under Title 50 authorities, but they also collected tactical intelligence for military commanders.

DoD intelligence activities, and adds Title 50’s provisions regarding Congressional oversight to intelligence activities conducted primarily by DoD personnel in support of or in furtherance of tasking from the Director of National Intelligence (DNI) (as opposed to tasking from the Secretary of Defense).

Thus, Title 10 and Title 50 are mutually-reinforcing authorities, not mutually-exclusive authorities; these statutory authorities may even be exercised simultaneously by personnel under the command and control of the Secretary of Defense. Labeling some intelligence activities “Title 50” activities while labeling similar activities “Title 10” activities creates a distinction where the law does not. Importantly, the statutes make distinctions based on direction, control, and funding—not on nomenclature.

B. Congressional Oversight

Confusion over Title 10 and Title 50 authorities has more to do with congressional oversight and its attendant internecine power struggles than with operational or statutory authorities. Operators, be they special operations forces (SOF) operating under Title 10, CIA agents operating under Title 50, or NSA personnel operating under both Title 10 and Title 50, know from whence their authorities are derived. The operators recognize dual lines of authority and are primarily concerned with coordination and deconfliction. To outsiders looking in, such as a Senator in Washington, DC, the activities performed by SOF and CIA operatives, especially during periods preceding possible or anticipated conflict, may appear virtually indistinguishable. Yet similarity in no way vitiates their dual lines of authority, nor does it create great challenges for operators.

A former general counsel of the CIA, Jeffrey H. Smith, spoke of what he perceived as a “dichotomy between Title 10 and Title 50” that gives “executive branch lawyers and members of Congress . . . headaches.”54 These headaches arise, Smith stated, during debates over military activities called “preparation of the battlefield,” which are activities typically carried out by military personnel “in close collaboration with the

54Jeffrey H. Smith, Keynote Address: Symposium: State Intelligence Gathering and International Law, 28 Mich. J. Int’l L. 543, 546–47 (2007). It should be noted that Smith was CIA General Counsel from May 1995 to September 1996. As such, his perspective very much reflects the national security mindset of the mid-1990s, which changed dramatically after the 9/11 attacks.
U.S. intelligence community.\textsuperscript{55} We will examine these activities more closely in Parts III and IV. Smith, however, summarizes the issue as such: if the activity is defined as a military activity ("Title 10") there is no requirement to notify Congress, while intelligence community activities ("Title 50") require presidential findings and notice to Congress.\textsuperscript{56} The natural inclination for executive branch lawyers, according to Smith, is to prefer the Title 10 paradigm to obviate congressional notification requirements.\textsuperscript{57}

This perception—that the Executive Branch is deliberately trying to avoid congressional oversight—naturally irks the intelligence committees. In its report accompanying the Intelligence Authorization Act for Fiscal Year 2010, the House Permanent Select Committee on Intelligence noted "with concern the blurred distinction between the intelligence-gathering activities carried out by the Central Intelligence Agency (CIA) and the clandestine operations of the Department of Defense."\textsuperscript{58} The Committee accused DoD of labeling its clandestine activities as operational preparation of the environment (OPE) in order to justify them under Title 10 and avoid oversight by the intelligence committees "and the congressional defense committees cannot be expected to exercise oversight outside of their jurisdiction."\textsuperscript{59} The Intelligence Committee apparently perceives an oversight lacuna, yet no such lacuna exists. Rather, all activities conducted under Title 10 authorities are subject to oversight by the armed services committees and, for example, commanders of special operations forces regularly brief the armed services committees on their clandestine activities.

\textsuperscript{55} Id. at 546.
\textsuperscript{56} Smith considers it "a curiosity of our legal history that findings and notice to Congress are required even in the most minor of covert actions, whereas no such requirement governs the use of our military forces." Id. Others express a similar envy of what they perceive to be DoD's easier operations approval process: "When the CIA acts, it requires a presidential 'finding' sent to Congress; yet the military can be authorized simply through the chain of command from the president as commander in chief." Treverton, supra note 10, at 13.
\textsuperscript{57} Smith, supra note 54, at 547.
\textsuperscript{59} Id.
As illustrated by Figure 1, the congressional intelligence committees exercise oversight of intelligence activities, while the armed services committees exercise oversight jurisdiction over military operations. The congressional oversight is not coterminous with statutory authorities, as Title 10 includes authority for the Secretary of Defense to engage in both intelligence activities and military operations. Congressional oversight overlaps when non-DoD elements of the intelligence community provide support to military operations and in the unlikely or at least rare instance where the President directs elements of DoD to conduct covert action.

---

Footnotes:

60 Senate Select Committee on Intelligence (SSCI); House Permanent Select Committee on Intelligence (HPSCI); Senate Armed Services Committee (SASC); and House Armed Services Committee (HASC).

61 "No agency except the Central Intelligence Agency (or the Armed Forces of the United States in time of war declared by the Congress or during any period covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law
Oversight would also overlap with respect to intelligence activities carried out by an element of the intelligence community in support of a military operation authorized under Title 10.

Congressional oversight of the military is straightforward: both the Senate and House Armed Services Committees exercise jurisdiction over all aspects of DoD and matters relating to "the common defense." Defense authorization bills originate in the armed services committees, where they must be approved before consideration by the full Senate or House. Problems arose in the wake of 9/11 as DoD expanded its intelligence capabilities in order to support ongoing military operations, and the intelligence committees correspondingly sought to expand their jurisdiction in an attempt to bring all military intelligence collection efforts within their purview, which created clashes with the armed services committees and the Executive Branch and generated debates over appropriate congressional oversight.

Congressional oversight of intelligence activities is considerably more complex. The National Security Act of 1947, which created the CIA, did not include statutory congressional oversight provisions. For nearly thirty years, Congress exercised little oversight of intelligence activities. This changed dramatically, however, following revelations in 1974 by then New York Times reporter Seymour Hersh that U.S. intelligence agencies engaged in domestic spying. The Church Committee’s subsequent investigation “did nothing less than revolutionize America’s attitudes toward intelligence supervision.”

The Senate established its Select Committee on Intelligence (SSCI) in 1976 and the House followed suit a year later with its Permanent Select Committee on Intelligence (HPSCI). The era of benign neglect was over, replaced instead by dynamic if often dysfunctional congressional oversight. In 1980 Congress mandated for the first time that the Director of Central

93-148) may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective.” E.O. 12,333, supra note 10, at ¶ 1.7(a)(4).
62 S. COMM. ON RULES AND ADMIN., 111TH CONG., STANDING RULES OF THE SENATE R. XXV, 1(c)(1) (2009) [hereinafter SENATE RULES]; RULES OF THE HOUSE OF REPRESENTATIVES (111th Cong.) Rule X, 1(c) [hereinafter HOUSE RULES].
64 Id. at 199.
Intelligence and the heads of all other U.S. departments and agencies "involved in intelligence activities" keep the intelligence committees "fully and currently informed of all intelligence activities."\textsuperscript{65} This provision was repealed in 1991 and responsibility for informing the congressional intelligence committees of all intelligence activities, including anticipated activities, was placed directly on the President.\textsuperscript{66}

The intelligence committees exercise broad oversight of the intelligence community. They exercise exclusive authorizing powers for the CIA, the Director of National Intelligence, and the National Intelligence Program.\textsuperscript{67} They share jurisdiction of DoD intelligence components with the Senate and House armed services committees.

While the jurisdictions of the Senate and House intelligence committees are nearly identical, HPSCI exercises broader jurisdiction in two significant respects: HPSCI uses a much broader definition of intelligence activities and adds oversight of "sources and methods."\textsuperscript{68} SSCI

\textsuperscript{65} Intelligence Authorization Act for 1981, 94 Stat. 1981, Pub. L. 96-450 (1980), repealed by Intelligence Authorization Act for 1992, 105 Stat. 441, Pub. L. 102-88 (1991). While a detailed examination of the Constitutional permissibility of this statute is beyond the scope of this essay, it is worth noting that this provision was prefaced with the following caveat: "To the extent consistent with all applicable authorities and duties, including those conferred by the Constitution upon the executive and legislative branches of the Government."


\textsuperscript{67} The National Intelligence Program is defined as:

\begin{quote}
[All programs, projects, and activities of the intelligence community, as well as any other programs of the intelligence community designated jointly by the Director of Central Intelligence and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by United States Armed Forces.
\end{quote}


\textsuperscript{68} Authority to "review and study on an exclusive basis the sources and methods of entities" in the intelligence community was added in January 2001. House Rule 3(l), added by
exercises jurisdiction over “intelligence activities,” while HPSCI exercises jurisdiction more broadly over “intelligence and intelligence-related activities . . . including the tactical intelligence and intelligence-related activities of the Department of Defense.” The House gives “intelligence and intelligence-related activities” this all-encompassing definition:

[The] collection, analysis, production, dissemination, or use of information that relates to a foreign country, or a government, political group, party, military force, movement, or other association in a foreign country, and that relates to the defense, foreign policy, national security, or related policies of the United States and other activity in support of the collection, analysis, production, dissemination, or use of such information.

Thus, the House of Representatives via a rule change gave HPSCI oversight of “intelligence-related activities” including “tactical intelligence” and other military information collection activities for which congressional notification is not statutorily mandated. This would be understandable if HPSCI controlled authorizations for those military activities, but it does not. All authorizations for these military activities originate in the House Armed Services Committee and House rules do not provide for their review by the intelligence committee. In fact, just the opposite occurs as all intelligence authorization bills passed by the intelligence committees must then clear the armed services committees before being considered by the full House.

Intelligence committee oversight is weakened by the bifurcated authorization and appropriations processes. Because most appropriations for intelligence activities are included as a classified section of the annual defense appropriations bill, “the real control over the intelligence purse lies

H.Res. 5, 107th Cong. (Jan. 3, 2001). Sources and methods is a catch-all phrase used by the intelligence community that eludes to how and from whom information is gathered.


70 Id. at Rule X, 11(j)(1). This definition applies to covert and clandestine activities. Title 50 does not define “intelligence activities,” although it does state that the term “includes covert actions . . . and includes financial intelligence activities.” Section 413a of Title 50 sets forth a generalized reporting requirement for intelligence activities other than covert actions, while Section 413b delineates detailed reporting and Presidential approval requirements for covert actions (“findings”). Executive Order 12,333 defines intelligence activities as “all activities that elements of the Intelligence Community are authorized to conduct pursuant to this order.” E.O. 12,333, supra note 10.
with the defense subcommittees of the House and Senate Appropriations Committees.” The 9/11 Commission recognized how “dysfunctional” this arrangement is in practice and recommended the establishment of a single joint intelligence committee with authorizing and appropriating authorities. Congress, to its detriment, has not adopted this recommendation.

Intelligence committee oversight is further weakened by the failure to enact an intelligence authorization bill for five of the past six years. Title 50 prohibits the expenditure or obligation of appropriated funds on intelligence or intelligence-related activities unless “these funds were specifically authorized by Congress for such activities.” Congress meets this “specifically authorized” provision through the use of a catch-all provision inserted into the defense appropriations acts. Over the past 30 years, Congress enacted an intelligence authorization bill prior to the start of the fiscal year on just two occasions—1983 and 1989.

Congress could end the Title 10-Title 50 debate by simply reforming its oversight of military and intelligence activities and align oversight with the statutory authorities. Rather than focus on what the activity in question looks like (what is being done), Congress should simply ask who is funding the activity and who is exercising direction and control; oversight should be aligned in the House and Senate and should correspond to funding,

71 Jennifer Kibbe, Congressional Oversight of Intelligence: Is the Solution Part of the Problem?, 25 INTELLIGENCE AND NAT’L SECURITY 24–49, 29–30 (2010). This process protects national security by sheltering intelligence budgets from public view, but it also dilutes the role of the intelligence committees. Kibbe points out that “the structure of the system precludes the defense subcommittees from conducting stringent intelligence oversight . . . [as] the $75 billion intelligence budget comprises around 10 to 12 percent of the defense budget” and, thus, garners “very little attention.”


74 The catch-all provisions read similar to this one for fiscal year 2009:

Funds appropriated by this Act, or made available by the transfer of funds in this Act, for intelligence activities are deemed to be specifically authorized by Congress for the purposes of section 504 of the National Security Act of 1947 (50 U.S.C. 414) during fiscal year 2009 until enactment of the Intelligence Authorization Act for Fiscal Year 2009.

direction and control. Congress should adopt the recommendations of the 9/11 Commission—align congressional oversight with statutory authorities and reform its bifurcated intelligence authorization and appropriations functions—and thereby eliminate most real and perceived Title 10-Title 50 issues. With the crux of the Title 10-Title 50 debate exposed as dysfunctional congressional oversight, this article now turns to explaining why some military and intelligence activities look alike, yet remain distinguishable.

III. When Military Operations Look Like Intelligence Activities

When American forces entered Afghanistan shortly after the terrorist attacks of 9/11, the picture soon emerged of U.S. Army Special Forces ("Green Berets") and CIA paramilitary officers operating together with Afghan warlords against a common al Qaeda and Taliban enemy.\(^7\) Presidential approval of the unconventional warfare plan for Afghanistan did much to quell rumblings about blurring of military and intelligence authorities, yet as the war in Afghanistan continued and the "war on terror" expanded globally those concerns became more prominent. Some argued the "tight integration" between special operations forces and the CIA in Afghanistan signaled "the erosion of distinctions between SOF and the CIA"—an "erosion" with supposedly dire legal consequences.\(^6\)

A former general counsel for the CIA suggested an erosion of distinctions between military operations and covert action in the context of cyberwarfare.\(^7\) John Rizzo characterized the Title 10-Title 50 debate in

\(^7\) See generally GARY BERNTSEN, JAWBREAKER (2005); HY S. ROTHSTEIN, AFGHANISTAN AND THE TROUBLED FUTURE OF UNCONVENTIONAL WARFARE 33 (2006); DOUG STANTON, HORSE SOLDIERS: THE EXTRAORDINARY STORY OF A BAND OF US SOLDIERS WHO RODE TO VICTORY IN AFGHANISTAN (2009).

\(^6\) COLONEL KATHRYN STONE, "ALL NECESSARY MEANS"—EMPLOYING CIA OPERATIVES IN A WARFIGHTING ROLE ALONGSIDE SPECIAL OPERATIONS FORCES 4 (US ARMY WAR COLLEGE STRATEGY RESEARCH PROJECT) (2003).

\(^7\) Hiding our Cyberwar from Congress, EMPTYWHEEL (Jan. 14, 2011), http://emptywheel.firedoglake.com/2011/01/14/hiding-our-cyberwar-from-congress (last accessed Mar. 9, 2011). This blogger provides three examples to support the thesis that DoD is deliberately trying to avoid reporting information on cyberwarfare programs to Congress. The third example quotes from a speech delivered by John Rizzo, former general counsel of the CIA, to the American Bar Association's Standing Committee on National Security. Rizzo stated: "I've always found fascinating and personally I think it's a key to understanding many of the legal and political complexities of so-called cyberlaw and cyberwarfare is the division between Title 10 operations and Title 50 operations. Title 10
terms of a dichotomy between “war-making authority” and “covert action” before concluding that “how these cyber-operations are described will dictate how they are reviewed and approved in the executive branch, and how they will be reported to Congress, and how Congress will oversee these activities.” Some commentators used Rizzo’s observation to suggest that the executive branch was disingenuously describing cyberwarfare in attempt to evade congressional oversight. We saw in Part II that oversight by the armed services committees is still congressional oversight. Part III will now explain why the same activities can properly be described as military or intelligence activities depending on their command and control, as well as funding, context and mission intent.

A. Unconventional Warfare

Just eight days after the terrorist attacks of September 11, 2001, Gary Schroen, a CIA paramilitary officer, packed three boxes with $9 million and flew to Afghanistan. The money would be used to pay Afghan warlords to fight with CIA and Special Forces personnel against al Qaeda and its Taliban collaborators. The operational plan was drafted by the CIA, vetted by the military and approved by the President. For the first time in American history, Special Forces working with CIA operatives were “the lead element in [a] war.” Yet even Secretary of Defense Donald Rumsfeld reportedly questioned who was really in charge. Eleven Special Forces

operations of course being undertaken by the Pentagon pursuant to its war-making authority, Title 50 operations being covert action operations conducted by CIA. Why is that important and fascinating? Because . . . how these cyber-operations are described will dictate how they are reviewed and approved in the executive branch, and how they will be reported to Congress, and how Congress will oversee these activities.” John A. Rizzo, “National Security Law Issues: A CIA Perspective” (University Club, Washington, DC) (May 5, 2010), available at http://www.americanbar.org/content/dam/aba/multimedia/migrated/natsecurity/multimedia/ws_30274.mp3 (last visited Mar. 9, 2011).

76 Id.
79 STANTON, supra note 75, at 37. See also GARY SCHROEN, FIRST IN (2005); Henry A. Crumpton, Intelligence and War 2001–2, in JENNIFER E. SIMS, TRANSFORMING U.S. INTELLIGENCE (2005).
80 STANTON, supra note 75, at 33. In past wars, SOF were often the first to enter hostile territory, but they always operated under the command and control of conventional military forces.
81 ROTHSTEIN, supra note 75, at 111. The importance of this point will become apparent later in this paper, but the CIA operatives were working under CIA control and Title 50 authorities while the Special Forces and other military personnel were under the operational control of U.S. Central Command and Title 10 authorities. See BERNTSEN,
teams operated with and coordinated the efforts of indigenous Tajik, Uzbek, Hazar, and Pashtun fighters, who were colloquially referred to as the Northern Alliance. Less than three months later, the Taliban government fell in an archetypal unconventional warfare campaign—small groups of highly skilled personnel operating with indigenous forces against a common enemy.

The U.S. military defines unconventional warfare as “[a]ctivities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area.”\textsuperscript{82} This definition reveals three defining characteristics of unconventional warfare: 1) it is conducted “by, with, or through” indigenous forces, 2) those indigenous forces are “irregular” (i.e., non-governmental) forces,\textsuperscript{83} and 3) it supports “activities” against the government or occupying power.\textsuperscript{84}

\textit{supra} note 75, at 86. Notwithstanding their separate lines of authority, the CIA and SOF on the ground in Afghanistan closely coordinated their operations and often operated in concert. In one instance, military commanders initially refused to send a rescue team to the aid of a five-man “CIA” team not realizing that, in fact, three of the five men on the team were active duty military officers. \textit{Id.} at 287.

\textsuperscript{82} U.S. DEPARTMENT OF DEFENSE, JOINT PUBLICATION 3-05, DOCTRINE FOR JOINT SPECIAL OPERATIONS FORCES GL-13 (April 18, 2011).

\textsuperscript{83} ARMY FIELD MANUAL FM 3-05.130, provides this distinction between regular and irregular forces:

\begin{quote}
Regulators are armed individuals or groups of individuals who are members of a regular armed force, police, or other internal security force . . . Regardless of its appearance or naming convention, if the force operates under governmental control, it is a regular force.

Irregulars, or irregular forces, are individuals or groups of individuals who are not members of a regular armed force, police, or other internal security force . . . These forces may include, but are not limited to, specific paramilitary forces, contractors, individuals, businesses, foreign political organizations, resistance or insurgent organizations, expatriates, transnational terrorism adversaries, disillusioned transnational terrorism members, black marketers, and other social or political “undesirables.”
\end{quote}

\textsuperscript{84} The third characteristic serves to distinguish unconventional warfare from irregular warfare. Irregular warfare is “a violent struggle among state and non-state actors for legitimacy and influence,” while unconventional warfare may be waged in support of both conventional state-on-state conflicts and insurgencies.
Activities conducted under the rubric of unconventional warfare include guerilla warfare, subversion, sabotage, intelligence collection, and unconventional assisted recovery.\textsuperscript{85} These activities do not necessarily by themselves constitute unconventional warfare, but rather they typify tactics and techniques commonly employed in unconventional warfare.\textsuperscript{86} In other words, not all intelligence collection falls under the unconventional warfare umbrella—even when it is conducted by SOF. Nor is guerilla warfare always conducted under the rubric of unconventional warfare.

Unconventional warfare is distinguished from other forms of warfare in that it uses irregular indigenous (surrogate) forces against the established or governing power in denied areas.\textsuperscript{87} The indigenous forces may be guerillas waging their own campaign against the government or they may be, essentially, independent agents working for the U.S. government. The indigenous forces have objectives of their own (political or pecuniary), so the mission for U.S. forces is to develop and sustain indigenous capabilities and channel them in ways that simultaneously accomplish U.S. national security objectives. For this reason, unconventional warfare is known colloquially as “by, with, or through.”

The goal of unconventional warfare is to exploit an adversary’s political, military, economic, and psychological vulnerabilities by developing and sustaining indigenous resistance forces to accomplish U.S. objectives. Unconventional warfare is “a classically indirect, and ultimately local, approach to waging warfare.”\textsuperscript{88} Unconventional warfare “is fought by subterranean armies composed of volunteers, revolutionists, guerillas, spies, saboteurs, provocateurs, corrupters, [and] subverters,” and it is waged

---

\textsuperscript{85}\textsc{Army Field Manual FM 3-05, supra note 83, at 130.}

\textsuperscript{86} “While many of the tactics and techniques utilized within the conduct of UW have significant application and value in other types of special operations, many of these techniques, such as sabotage and intelligence collection, are not exclusive to UW....” LTC Mark Grdovic, <textit{A Leader’s Handbook to Unconventional Warfare 9} (SWCS Pub 09-1/2009) (SWCS is an acronym for the U.S. Army John F. Kennedy Special Warfare Center and School located at Ft Bragg, North Carolina).

\textsuperscript{87} This definition distinguishes unconventional warfare from “foreign internal defense”—a form of surrogate warfare where indigenous regular, or official, forces are trained, equipped, organized, and supported to conduct operations against insurgents or other forms of lawlessness. Prime examples of foreign internal defense are the U.S. military operations to organize, train, and equip government security forces in Iraq and Afghanistan to fight against insurgents. See also id. at 9.

\textsuperscript{88} Rothstein, supra note 75, at 159.
through military, political, economic, and psychological means. In peacetime, unconventional warfare "operates at a level below that of outright provocations and the instigators do not appear in the open."

As we saw above, the U.S. military limits its definition of unconventional warfare to activities that take place within the context of insurgencies (conflicts in denied areas against the government or force in power). U.S. support to insurgencies "can be categorized as one of two types of campaign efforts: general war scenarios and limited war scenarios." A typical general war scenario is when the U.S. military wants to prepare for possible conventional invasion of a foreign country by establishing an unconventional capability (i.e., the ability to use indigenous surrogates). During the preparation phase, which consists of initial contact and infiltration, the goal is to identify exactly what U.S. military needs or requirements would be, as well as which indigenous individuals or groups would be willing to work with U.S. personnel. Initial contact is when contact with resistance forces (potential partners) is first made; this may take place in another country (contacting expatriates or exiles), or through intermediaries such as CIA personnel. Infiltration is when U.S. personnel first enter the country where the potential indigenous partners are located; given the clandestine nature of unconventional warfare, the U.S. personnel will not likely enter the country in uniform, nor will their true intentions be apparent. Organization and buildup are stages where the capabilities of indigenous forces are developed through training and equipping. These indigenous capabilities are then employed to accomplish U.S. objectives. Unconventional warfare concludes with a transition phase that may include

---

89 Morris Greenspan, *International Law and Its Protection for Participants in Unconventional Warfare*, 341 ANNALS AM. ACAD. POL. & SOC. SCI. 30, 31 (May 1962). Guerilla warfare generally consists of attacks conducted by irregular indigenous forces in areas they do not control. Insurgencies or other armed resistance movements normally use some form of guerilla warfare against the forces they are engaged in conflict with. "Victory is achieved not so much by knocking the enemy's sword from his hand as by paralysing his arm." Charles Townshend, *The Irish Republican Army and the Development of Guerilla Warfare 1916–1921*, 94 ENG. HIST. REV. 318, 318 (1979).

90 Townshend, supra note 89, at 318. Guerilla warfare is typified by "hit-and-run" attacks by forces that do not wear uniforms or openly advertise their armed nature. For example, when Umkhonto, the paramilitary wing of the African National Congress initiated its guerilla campaign against the apartheid government in South Africa in 1961, it "gave first priority to a campaign of sabotage against power and communication facilities and government buildings." Sheridan, Johns, *Obstacles to Guerilla Warfare-A South African Case Study*, 11 J. AFR. STUD. 267, 273 (1973).

91 GRDOVIC, supra note 86, at 17.
demilitarization. Historical examples of the U.S. military conducting unconventional warfare in the context of general war include the Jedburg teams inserted by the Office of Strategic Services (OSS) into occupied France during World War II, Afghanistan in 2001–2002, and Iraq in 2003.

Unconventional warfare in the context of a limited warfare scenario is conducted in very similar phases. The key difference, however, is significant to our purposes here: in limited warfare the U.S. government seeks to apply pressure against an adversary via internal forces rather than a military invasion. In limited warfare, the U.S. government does not use conventional military forces to overtly invade the adversary, but seeks instead to accomplish political objectives through the use of small numbers of SOF, and often CIA personnel, working “by, with, or through” indigenous forces. Limited warfare is politically risky and, thus, conducted in secret: it is colloquially referred to as secret war, dirty war, small war, or low-intensity conflict. The United States conducted unconventional warfare in the context of limited war in North Vietnam in 1961–1964, the

---


93 ROTHSTEIN, supra note 75, at 27–29. Rothstein also asserts that U.S. forces conducted forms of unconventional warfare in the Revolutionary War, the War of 1812, the Mexican War of 1846–48, the U.S. Civil War and throughout the 20th century.

94 Prior to the initiation of aerial bombardment and the ground campaign in Operation Iraqi Freedom, U.S. Special Forces teams infiltrated northern Iraq and conducted unconventional warfare with Kurdish resistance elements, including the Patriotic Union of Kurdistan. GRDOVIC, supra note 86, at 7.


96 Unconventional warfare activities in North Vietnam between 1961 and 1964 qualify as being conducted in a limited war context as the U.S. government did not originally intend to introduce conventional military forces in large numbers into Vietnam. It was only after the limited war failed to achieve the desired results that the conflict escalated into general warfare. The Special Observations Group (SOG) was a cover name for a U.S. unconventional warfare task force, composed of SOF. SOG regularly infiltrated North Vietnam and conducted unconventional warfare primarily through intelligence activities, propaganda campaigns, sabotage, and guerilla attacks. See generally RICHARD H. SHULTZ

Unconventional warfare is generally effectuated in seven phases: preparation, initial contact, infiltration, organization, buildup, employment, and transition.\textsuperscript{98} Each phase may not always be required, and phases may be conducted simultaneously or out of sequence.\textsuperscript{99} Each phase highlights the Title 10-Title 50 debate and related congressional oversight concerns that are the focus of this paper, yet these concerns are particularly acute in the initial contact and infiltration phases. During the initial contact phase, an interagency pilot team “composed of individuals possessing specialized skills” may make contact with indigenous forces and begin assessing the potential to conduct unconventional warfare.\textsuperscript{100} SOF often augment pilot teams led by, and primarily constituted of, CIA personnel.\textsuperscript{101}

\begin{flushright}
\end{flushright}

\begin{flushright}
\textsuperscript{97} SOF worked with the CIA in supporting various resistance groups in Nicaragua. The operations are generally viewed as an example of how unconventional warfare should not be waged as the resistance groups, collectively referred to as the Contras, never succeeded in building necessary support inside Nicaragua and became viewed as mercenaries with little connection to the local population. \textit{See} GRDOVIC, \textit{supra} note 86, at 36.
\end{flushright}

\begin{flushright}
\textsuperscript{98} ARMY FIELD MANUAL FM 3-05.130, \textit{supra} note 83, at 4-4.
\end{flushright}

\begin{flushright}
\textsuperscript{99} “For example, a large and effective resistance movement may require only logistical support, thereby bypassing the organization phase. The phases may also occur out of sequence, with each receiving varying degrees of emphasis. One example of this is when members of an irregular force are exfiltrated to a partner nation (PN) to be trained and organized before infiltrating back into the UWOA [unconventional warfare operating area], either with or without the ARSOF [Army Special Operations Forces] unit. In this case, the typical order of the phases would change.” \textit{Id}.
\end{flushright}

\begin{flushright}
\textsuperscript{100} \textit{Id}. at 4-5. In the context of limited war, the Title 10-Title 50 issues that are the focus of this paper permeate every aspect of the mission. Indeed, the political risks involved and need for secrecy may dictate that the U.S. government not acknowledge its role in the operations, which strikes at the very heart of this debate.
\end{flushright}

\begin{flushright}
\textsuperscript{101} \textit{Id}. at 5-2. This manual states it is not unusual for SOF “to augment pilot teams led by and primarily constituted of OGA personnel.” The acronym “OGA” stands for other government agency and is generally understood to be a euphemism for the CIA. \textit{See} John Henderson, \textit{The Conflict In Iraq}, L.A. TIMES, Sep. 10, 2004, at A-1. Strictly speaking, a pilot team is not an unconventional warfare mission as much as it is a critical precursor to unconventional warfare. The pilot team’s mission is to conduct a feasibility assessment, which analyzes whether there is an indigenous force with which the U.S. can engage in an unconventional warfare campaign.
\end{flushright}
This brief overview of unconventional warfare illustrates why unconventional warfare often appears very similar to activities conducted by CIA personnel. Indeed, SOF typically work closely with CIA personnel while conducting unconventional warfare, although the relationship tends to be informal and focused more on mutual support. In other words, the relationship is one of cooperation in pursuit of mutual objectives rather than a formal superior-subordinate relationship. As we will examine in more detail in Part IV of this paper, this is an important distinction that directly answers whether the unconventional warfare mission is a military operation or intelligence activity.

B. Cyberwarfare

Cyberwarfare is no longer the future of warfare—it is the present and future. While a “hot” cyber war between major powers has thankfully not occurred, there are minor skirmishes, a silent arms race, and major intelligence gathering. According to Mike Jacobs, formerly of the NSA, countries “are learning as much as they can about power grids and other systems, and they are sometimes leaving behind bits of software that would allow them to launch a future attack.” These may be acts of cyber espionage rather than cyberwarfare, but they are at least preparing cyberspace for warfare—and they highlight the integration of intelligence and warfare in cyberspace.

In January 2011, a front-page New York Times article detailed a sophisticated cyberattack straight out of science fiction. Strong circumstantial evidence suggested Iran’s nuclear program was delayed for several years after a computer worm named Stuxnet infiltrated the industrial control systems responsible for manufacturing Iran’s nuclear centrifuges. Since the computers controlling Iran’s nuclear enrichment

---


facilities are not connected to the Internet, Stuxnet was apparently designed to infiltrate the computers of contractors working for Iran’s nuclear program and hitchhike on thumbdrives or similar removable media devices that were later connected to computers at Iran’s enrichment facilities. Stuxnet then caused the machines spinning centrifuges to create defective centrifuges while simultaneously reporting that all systems were performing normally. Experts suggested Stuxnet could only have been created by American or Israeli intelligence agencies.105 If true, Stuxnet heralded a new age of cyberwarfare able to destroy “targets with utmost determination in military style.”106

On June 23, 2009, U.S. Cyber Command was established to lead U.S. military efforts against “cyber threats and vulnerabilities” and “secure freedom of action in cyberspace.”107 Accepting the recommendation of Secretary of Defense Robert Gates, President Barack Obama nominated Lieutenant General Keith B. Alexander, the Director of the National Security Agency, to also serve as the Commander of U.S. Cyber Command. During the confirmation process, the Senate Armed Services Committee questioned various aspects of General Alexander’s proposed dual responsibilities—questions at the heart of the Title 10-Title 50 debate. How would he carry out his responsibilities as Director of the National Security Agency, an intelligence agency and member of the intelligence community, while also carrying out his responsibilities as Commander of U.S. Cyber Command, a military war-fighting command?

The Committee asked General Alexander, for example, whether the military conducts intelligence gathering of foreign networks, whether intelligence gathering of foreign networks is “authorized and reported to Congress under Title 10 or Title 50,” and whether cyberspace operations are traditional military activities. While many of General Alexander’s answers were provided to the Committee in a classified supplement, his unclassified answers and testimony at his confirmation hearing presumably provide insight into how the Secretary of Defense exercises his statutory and delegated authorities to conduct intelligence activities and military

---

106 Broad et al., *supra* note 104.
operations. General Alexander repeatedly explained that “while there will be, by design, significant synergy between NSA and Cyber Command, each organization will have a separate and distinct mission with its own identity, authorities, and oversight mechanisms.”

Cyberspace is defined by the U.S. government as the “global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.” Others suggest a definition that emphasizes cyberspace as a global information environment unique in its “use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information communications technologies.” Indeed, the distinctive use of electronics and electromagnetic spectrum distinguishes cyberspace from the domains of land, sea, air, and space: it is “a physical environment . . . managed by rules set in software and communications protocols.” Cyberspace is governed by the laws of physics and the logic of computer code.

---

108 It is unlikely that General Alexander would have provided written responses to the Committee without such responses being cleared or reviewed by the Secretary of Defense, or at least his subordinates such as the DoD General Counsel. It is also worth noting that while Cyber Command likely possesses significant delegated authorities, the 2011 National Military Strategy specifically calls for “executive and Congressional action to enable effective action in cyberspace.” CHAIRMAN OF THE JOINT CHIEFS OF STAFF, THE NATIONAL MILITARY STRATEGY OF THE UNITED STATES 10 (2011).
109 Hearing on the Nominations of VADM James A. Winnefeld Jr., USN to be Admiral and Commander, U.S. Northern Command/Commander, North American Aerospace Command; and LTG Keith B. Alexander, USA to be General and Director, National Security Agency/Chief, Central Security Service/Commander, U.S. Cyber Command, S. Comm. on the Armed Services, 105th Cong. 10 (2010).
110 JP 1-02, infra note 115, at 139. This definition is also contained in the 60-day Cyberspace Policy Review directed by President Obama shortly after taking office, which quotes classified NATIONAL SECURITY PRESIDENTIAL DIRECTIVE 54/HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 23 (Jan. 8, 2008).
112 Gregory J. Ratray, An Environmental Approach to Understanding Cyberpower, in CYBERPOWER AND NATIONAL SECURITY, supra note 111, at 254.
113 Id. at 255.
Wikipedia defines Cyberwarfare simplistically: as the use of computers and the Internet to conduct warfare in cyberspace.\footnote{See CYBERWARFARE, WIKIPEDIA http://en.wikipedia.org/wiki/Cyberwarfare (last visited Mar. 7, 2011). Cyberwar is also defined as referring to “conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying the information and communications systems ... on which an adversary relies to 'know' itself.” JOHN ARQUILLA AND DAVID RONFELDT, IN ATHENA’S CAMP: PREPARING FOR CONFLICT IN THE INFORMATION AGE 28 (1997).} The U.S. military does not define cyberwarfare in its unclassified dictionary, wisely avoiding the term “war” with its associated baggage and implications. The U.S. military instead categorizes cyber operations as defense, exploitation, or attack.\footnote{Computer network defense consists of actions “taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks.” Computer network exploitation is “[e]nabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.” Computer network attack consists of 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.” All three, defense, exploitation, and attack, fall under the general umbrella term computer network operations. U.S. DEPARTMENT OF DEFENSE, JOINT PUBLICATION 1-02, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 95 (as amended through Apr. 2010). Examples of cyber operations or activities include mapping networks, scanning networks and industrial control systems (e.g., to find vulnerabilities), denial of service (flooding networks such that they become inoperable), hacking networks or systems to gain stored information (including insertion of malware or spyware), manipulating data on someone else’s network or system, taking over control of a system or network so sensors can be turned off or manipulated, activation of malicious code secretly embedded on computer chips during the manufacturing process, and other disruption or destruction of computer networks or systems.} This article focuses on the last two categories, exploitation and attack, and attempts to define the legal authorities and identify the type of activities associated with these categories. In the minds of some, exploitation infers intelligence activities while attack sounds like a military operation, yet our analysis here will add nuance to this simplistic characterization.

If the distinguishing characteristics of cyberspace are electronics and electromagnetic spectrum governed by the laws of physics and computer code, then how can we best distinguish cyber exploitation from attack? One could argue that cyber attacks affect electronics and electromagnetic spectrum by altering their physical characteristics or computer code, while exploitation merely gathers information. The problem is that cyber attack thus defined would include acts of computer network exploitation where
computer code is left behind or altered (for example, keystroke logging or insertion of a “backdoor”).

Perhaps cyber attack should be defined or interpreted more in the classical international relations sense of forced political coercion.\textsuperscript{116} Cyber operations would not be considered attacks if they seek only to gain information or intelligence, and are not intended to alter or control the primary functions of the adversary’s electronics or electromagnetic spectrum—even if they do leave computer code behind, such as keystroke logging software or the insertion of a back door. Subsequent acts to exploit the identified vulnerabilities by asserting control, or coercion, over the systems would rise to the level of attacks.\textsuperscript{117}

This distinction between merely altering computer code without asserting control or degrading function and actually assuming control or degrading functions is consistent with international law, which does not generally consider intelligence activities to be acts of war. Its weakness, however, is definitional reliance upon the intent of the sponsor. Distinguishing cyber attack from exploitation based on the intent of the sponsor is analogous to the challenge of distinguishing between warning shots and an initiation of armed conflict: intent is clear to the person pulling the trigger, but much less so to those on the receiving end.

The salient point is this: during the initial period after you discover someone is or was inside your network, you may not know whether the other person is initiating an attack or merely attempting to exploit your network. The other party knows why he is inside your network, but you do not. If you know your network is being attacked, a broad range of responses may be justified in self-defense; however, if your network is merely being exploited (an intelligence activity) your range of responses are arguably

\textsuperscript{116} Defining warfare is beyond the scope of this paper, but it suffices to say it involves the forced imposition of political will. It is, in Carl Von Clausewitz’s immortal words, the “continuation of political activity by other means.” CARL VON Clausewitz, ON WAR 87 (Michael Howard & Peter Paret, eds. & trans., Princeton Univ. Press 1976) (1832). See also MYRES S. MCDougal & FLORENTINO P. Feliciano, THE INTERNATIONAL LAW OF WAR: TRANSNATIONAL COERCION AND WORLD PUBLIC ORDER 11 (1994) which defines coercion as “a high degree of constraint exercised by means of any or all of the various instruments of policy.”

\textsuperscript{117} Here is a possible definition of cyberwarfare: politically coercive acts that affect electronics and electromagnetic spectrum by altering their physical characteristics or computer code such that the effect is analogous to an armed attack.
more limited. Thus, this distinction helps define the legal authority to carry out an operation, but does little to define appropriate defensive responses.

Which is why intelligence is the key to successful cyberwarfare. Cyber exploitation plays a critical supporting role in cyber attack. Knowing where an adversary’s cyber systems are vulnerable will likely require computer network exploitation “to understand the target, get access to the right attack vantage point, and collect BDA [battle damage assessment].”\textsuperscript{118} In the words of one expert on cyber attack, “those who prepare and conduct operational cyberwar will have to inject the intelligence operative’s inclinations into the military ethos”—inclinations that include discrete effects, patience, an intuitive understanding of the adversary’s culture, a “healthy wariness of deception, indirection, and concealment . . . [and] a willingness to abandon attack plans to keep intelligence instruments in place.”\textsuperscript{119}

As noted above, the intent or purpose of the actor is typically a key distinction between cyber exploitation and cyber attack. A recent report issued by the National Research Council suggests the distinction is really the nature of the payload, but acknowledges that technical similarities between attack and exploitation “often mean that a targeted party may not be able to distinguish easily between a cyberexploitation and a cyberattack.”\textsuperscript{120} The Report provides this helpful illustration:

\begin{center}
\textsuperscript{118} MARTIN C. LIBICKI, CYBERDETERRENCE AND CYBERWAR 139 (RAND, 2009).
\textsuperscript{119} Id. at 156.
\textsuperscript{120} NATIONAL RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1 (William A. Owens, Kenneth W. Dam, & Herbert S. Lin, eds., 2009).
\end{center}
**Box 1—Cyberattack versus Cyberexploitation**

<table>
<thead>
<tr>
<th></th>
<th>Cyberattack, attack, computer network attack</th>
<th>Cyberexploitation, intelligence, exploitation, computer network exploitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approach and intent</td>
<td>Degradate, disrupt, deny, destroy attacked infrastructure and systems/networks</td>
<td>Achieve smallest intervention consistent with desired operations</td>
</tr>
<tr>
<td>Relevant domestic law</td>
<td>U.S. Code Title 10 authorities and restrictions</td>
<td>U.S. Code Title 50 authorities and restrictions</td>
</tr>
<tr>
<td>Operational agency</td>
<td>U.S. Strategic Command (Joint Functional Component Command for Network Warfare)</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>Main advocate in the U.S. government to date</td>
<td>U.S. Air Force</td>
<td>Director of National Intelligence</td>
</tr>
<tr>
<td>Interactions with tactical military operations</td>
<td>Based on explicit inclusion in battle plans</td>
<td>Based on intelligence reporting</td>
</tr>
<tr>
<td>Characterization of personnel</td>
<td>Warfighters</td>
<td>Intelligence community</td>
</tr>
</tbody>
</table>

*Source: NATIONAL RESEARCH COUNCIL.*

This illustration is a helpful starting point, but its simplistic separation of Title 10 and cyber attack in one column and Title 50 and cyber exploitation in another column belies the stovepiped thinking of congressional overseers and ignores current operational realities. It ignores military intelligence collection efforts and operational preparation of the cyber environment by military personnel operating under military command and control—activities that are properly understood to be military operations and not intelligence activities, as we will see in Part IV of this paper.

Cyberwarfare differs from other forms of warfare in that the skills or tools necessary to collect intelligence in cyberspace are often the same skills or tools required to conduct cyber attack. Furthermore, the time lag between collecting information and the need to act upon that information may be compressed to milliseconds. Unlike the traditional warfighting construct where intelligence officers collect and analyze information before passing that information on to military officers who take direct action, cyber attack may require nearly simultaneous collection, analysis, and action. The same government hacker may identify an enemy computer network,
determine its strategic import, and degrade its capabilities all in a matter of seconds.

This is precisely why President Obama put the same man in charge of cyber intelligence activities and military cyber operations. This is also the reason Congress evidenced considerable apprehension and asked many questions about authorities and oversight. After all, congressional oversight retains its antiquated, stovepiped organizational structure and presumes a strict separation between intelligence activities and military operations even when no such separation is legally required.

IV. Distinguishing Military Operations, Intelligence Activities & Covert Action

Title 10 and Title 50 are mutually supporting authorities that can be exercised by the same person or agency, yet congressional oversight is exercised by separate, often competing, committees and subcommittees. This dysfunctional division of congressional oversight of national security is the fundamental “Title 10-Title 50” challenge. Congressional committees exercise oversight and, importantly, authorize and appropriate funds based in part on whether they perceive an activity to be an intelligence activity or a military operation.

The question of whether an unconventional or cyber warfare activity is a military operation, an intelligence activity, or covert action is more precisely a question of congressional oversight: will the intelligence committees exercise primary oversight jurisdiction, or will the armed services committees? To answer this question, we will first define intelligence activities and identify the key elements that distinguish military operations from intelligence activities. We will then examine covert action, which is not synonymous with intelligence activities despite that persistent misperception, and we will learn why even unacknowledged military operations may be exempt from intelligence committee oversight. Our analysis of the relevant statutes will reveal that traditional military activities are not intelligence activities or covert action. A brief review of military and legislative history will show that military operations preparatory to anticipated conflict are traditional military activities, and that even unacknowledged operations by military personnel under military command and control may not constitute covert action.
A. Military Operation or Intelligence Activity?

Title 50 directs the President “to ensure that the congressional intelligence committees are kept fully and currently informed of the intelligence activities of the United States,” yet there is no statutory definition of the term “intelligence activities.”\textsuperscript{121} The closest Title 50 comes to defining intelligence activities is its stipulation that the term includes “covert action” and “financial intelligence activities.”\textsuperscript{122} Other provisions in Title 50 appear to suggest that “military intelligence activities” and “tactical intelligence activities” are distinguishable from (rather than subsets of) intelligence activities.\textsuperscript{123} This distinction is supported by the statutory definition of the National Intelligence Program, which provides that it “does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by United States Armed Forces.”\textsuperscript{124}

Executive Order 12,333 broadly defines intelligence activities as “all activities that elements of the Intelligence Community are authorized to conduct pursuant to this order.”\textsuperscript{125} The Intelligence Community includes elements from several government agencies, including the CIA, the Department of State, the Department of Treasury, the Department of Energy, and, naturally, DoD.\textsuperscript{126} Indeed, so many elements of DoD are also

\textsuperscript{122} Id. § 413(a)(1), (f) (2006).
\textsuperscript{123} See 50 U.S.C. § 403-3(a) (2006), which expresses the sense of Congress that either the DNI or his Deputy should have experience with or appreciation of “military intelligence activities,” and 50 U.S.C. § 403-5(a)(3) (2006), which directs the Secretary of Defense to coordinate with the DNI to “ensure that the tactical intelligence activities of [DoD] complement and are compatible with intelligence activities under the National Intelligence Program.”
\textsuperscript{125} E.O. 12,333, supra note 10, § 3.5(g).
\textsuperscript{126} Both Title 50 U.S.C. § 401a(4) (2006) and Executive Order 12,333 define the Intelligence Community as including:

(A) The Office of the Director of National Intelligence.
(B) The Central Intelligence Agency.
(C) The National Security Agency.
(D) The Defense Intelligence Agency.
(E) The National Geospatial-Intelligence Agency.
(F) The National Reconnaissance Office.
members of the Intelligence Community—and E.O. 12,333 gives those elements broad authority to carry out intelligence activities—that the statutory distinction between intelligence activities and military intelligence activities we saw in the preceding paragraph is nearly obviated.127

This jumble of defined and undefined terms leads to the confusion discussed throughout this Article about where to draw the line between intelligence activities and military operations. Yet the critical distinction emerges when E.O. 12,333 Sec. 1.10 assigns distinct responsibilities to the Secretary of Defense to: “(a) Collect (including through clandestine means), analyze, produce, and disseminate information and intelligence and be responsive to collection tasking and advisory tasking by the Director; (b) Collect (including through clandestine means), analyze, produce, and disseminate defense and defense-related intelligence and counterintelligence, as required for execution of the Secretary's

---

(G) Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs.

(H) The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Federal Bureau of Investigation, and the Department of Energy.

(I) The Bureau of Intelligence and Research of the Department of State.

(J) The Office of Intelligence and Analysis of the Department of the Treasury.

(K) The elements of the Department of Homeland Security concerned with the analysis of intelligence information, including the Office of Intelligence of the Coast Guard.

(L) Such other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the intelligence community.

Title 50 U.S.C. § 401a(4) (2006). See also E.O. 12,333 supra note 10, § 3.5(h) (defining the elements of the Intelligence Community).

127 For example, the intelligence and counterintelligence elements of the Army, Air Force, Navy, and Marine Corps are part of the Intelligence Community, and E.O. 12,333 directs those elements to “[c]ollect (including through clandestine means), produce, analyze, and disseminate defense and defense-related intelligence and counterintelligence to support departmental requirements, and, as appropriate, national requirements . . . .” E.O. 12,333, supra note 10, at § 1.7(f)(1). Thus, E.O. 12,333 authorizes elements of DoD to conduct military (“departmental”) intelligence activities and national intelligence activities.
The primary question, then, is whether the activity is being conducted in response to tasking from the DNI or the Secretary of Defense.

The foregoing suggests a two-part test to determine whether an activity is an intelligence activity or a military operation. An intelligence activity is: (1) conducted by an element of the intelligence community (2) in response to tasking from the DNI. If the activity in question fulfills both requirements, then it is an intelligence activity authorized primarily by Title 50. If the activity is conducted by a DoD element of the intelligence community pursuant to tasking from the Secretary of Defense, then it should be considered a military operation, or military intelligence activity, conducted under either Title 10 or Title 50 authority. If the activity is conducted by a DoD element that is not part of the Intelligence Community, then the activity is a military operation conducted only under Title 10 authority.

This discussion highlights why the Title 10-Title 50 debate is typically little more than a debate about congressional oversight. The Secretary of Defense possesses authorities under both Title 10 and Title 50. The armed services committees exercise oversight over all DoD activities and operations, including military intelligence activities, tactical intelligence activities, and other departmental intelligence-related activities. The

---

128 EO 12,333, supra note 10, at § 1.10. This distinction is reinforced in subsection (c) where the Secretary of Defense is given authority to “[c]onduct programs and missions necessary to fulfill national, departmental, and tactical intelligence requirements.”

129 The Secretary of Defense may direct DoD personnel to carry out intelligence activities in response to national intelligence requirements, or to meet the intelligence needs of the military. When DoD personnel conduct intelligence activities in response to national intelligence requirements, they do so primarily under Title 50 authorities (50 U.S.C. § 403–5(b)(1) (2006)) and pursuant to priorities and needs determined by the DNI (50 U.S.C. § 403 –1(f) (2006)). When DoD personnel conduct intelligence activities to fulfill military intelligence requirements, those intelligence activities are conducted under Title 10 authorities, e.g., 10 U.S.C. §§ 113, 164 (2006), and delegated authorities from the President and Secretary of Defense; if the DoD personnel are also members of the Intelligence Community (e.g., NSA) the activities are also conducted pursuant to Title 50 authorities (50 U.S.C. § 403–5 (2006). These military operations are also sometimes referred to as “DoD Intelligence Related Activities” or “Tactical Intelligence and Related Activities (TIARA),” CONFERENCE REPORT ON THE INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 1991, H.R. REP. NO. 102-166 (Conf. Rep.) [July 25, 1991] at 21 [hereinafter Conference Report].
challenge is that the intelligence committees also want to assert jurisdiction over the “intelligence-related” activities of the military.

As we saw in Part II, the intelligence committees purport to exercise broad jurisdiction over all intelligence-related activities, including those of the military, which in turn creates overlapping jurisdiction with the armed services committees and needlessly generates confusion over oversight and reporting requirements. While the intelligence committees may be justified in asserting jurisdiction over DoD activities authorized and funded under Title 50 authorities, the same cannot be said of DoD intelligence-related activities authorized and funded under Title 10 authorities. These Title 10 activities should be properly categorized as military operations subject to the exclusive oversight of the armed services committees.

B. Is the Military Operation a Covert Action?

The military operations discussed in Part III, unconventional and cyber warfare, are conducted by SOF and U.S. Cyber Command, respectively. Neither special operations nor U.S. Cyber Command are elements of the Intelligence Community, so if an unconventional or cyber warfare activity is conducted pursuant to tasking from the Secretary of Defense, then there can be little question it is a military operation. Military operations authorized and funded under Title 10 authorities are properly labeled military operations subject to the exclusive oversight of the armed services committees, even if those activities are related to intelligence gathering—so long as they are in response to tasking from the Secretary of Defense and remain under military direction and control. Yet Title 50 includes one provision that would place even military operations meeting these criteria under the jurisdiction of the intelligence committees: the intelligence committees retain jurisdiction over all covert action.

For all that is lacking in the Title 50 definition of intelligence activities, it does stipulate that the term includes “covert action.” Indeed, covert action is arguably the intelligence activity that generates the most attention and concern, especially from members of Congress. The very phrase conjures images of cloak-and-dagger intrigue and rogue actors manipulating foreign powers while possessing “a license to kill.” For most of American history, the term covert action was not statutorily defined—and had little reason to be—until Congress became concerned with oversight.

Indeed, President George H.W. Bush issued a signing statement calling Congress’s definition of covert action “unnecessary” and stated he would continue to consider the historic missions of the U.S. military in determining whether a particular activity constituted a covert action.\footnote{President Bush’s signing statement reads, in pertinent part:}

Following the Iran-Contra affair, Congress statutorily defined covert action as “an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly.”\footnote{I believe that the Act’s definition of “covert action” is unnecessary. In determining whether particular military activities constitute covert actions, I shall continue to bear in mind the historic missions of the Armed Forces to protect the United States and its interests, influence foreign capabilities and intentions, and conduct activities preparatory to the execution of operations.} Accordingly, covert action consists of three essential elements:

\footnote{Statement on Signing the Intelligence Authorization Act, Fiscal Year 1991, in BOOK II PUB. PAPERS 1043–44 (1991). The use of Presidential signing statements is controversial. Some scholars view signing statements as an attempt to influence legislative history by creating “executive . . . history that is expected to be given weight by the courts in ascertaining the meaning of statutory language.” Marc N. Garber & Kurt A. Wimmer, Presidential Signing Statements as Interpretations of Legislative Intent: An Executive Aggrandizement of Power, 24 HARV. J. ON LEGIS. 363, 366 (1987). Nevertheless, the Constitution does envision a significant Presidential role in the legislative process, see, e.g., U.S. CONST. art. I, § 7, cl. 2, and some courts have relied on signing statements when interpreting legislation. See, e.g., United States v. Story, 891 F.2d 988, 994 (2d Cir. 1989); Berry v. Dep’t of Justice, 733 F.2d 1343, 1349–50 (9th Cir. 1984); Clifton D. Mayhew, Inc. v. Wirtz, 413 F.2d 638, 661–62 (4th Cir. 1969). However, signing statements are probably entitled to no more consideration than other forms of “post-passage legislative history, such as later floor statements, testimony or affidavits by legislators, or amicus briefs filed by members of Congress.” Walter Dellinger, Memorandum for Bernard M. Nussbaum, Counsel to the President, The Legal Significance of Presidential Signing Statements (Nov. 3, 1993), 17 Op. O.L.C. 131, 134 (1993).}

\footnote{50 U.S.C. § 413b(e) (2006). A year after its creation by the National Security Act of 1947, the National Security Council issued NSC Directive 1012, which established a policy of containment of the Soviet Union and redefined covert action. Originally crafted by George Kennan, then director of the State Department’s Policy Planning Staff, “NSC 1012 was the turning point for covert action, expanding it from propaganda to direct intervention.” NSC Directive 1012 defined covert action to include “propaganda, economic warfare; preventive direct action, including sabotage, anti-sabotage, demolition and evacuation measures; subversion against hostile states, including assistance to}
1. An activity of the U.S. government;
2. To influence political, economic, or military conditions abroad; and
3. Where it is intended that the role of the U.S. government will not be apparent or acknowledged openly.

This definition was included in the Intelligence Authorization Act for 1991. The accompanying Conference Report emphasized that Congress did not intend for the definition to expand or contract previous definitions of covert action; rather, the intent was to “clarify the understandings of intelligence activities that require presidential approval and reporting to Congress.”

The Senate Report, which was not adopted in whole by the Conference Report, stressed that “the core definition of covert action should be interpreted broadly.” It is not clear that the Executive Branch shares Congress’s interpretation, nor are these congressional interpretations legally binding. Nevertheless, the first element, “an activity of the U.S. government,” naturally includes any activity by U.S. government personnel, as well as any activity by third parties acting on behalf of U.S. government

underground resistance movements, guerrillas and refugee liberation groups, and support of indigenous anticomunist elements.” The Directive stipulated that covert action was to be “so planned and executed that any U.S. Government responsibility for them is not evident to unauthorized persons and that if uncovered the U.S. Government can plausibly disclaim any responsibility for them.” This definition guided U.S. government actions for over forty years. TREVORTON, supra note 10, at 210.


Statements in committee reports may provide persuasive authority, but do not have the force of law. American Hospital Assn. v. NLRB, 499 U.S. 606, 616 (1991); TVA v. Hill, 437 U.S. 153, 191 (1978) (“Expressions of committees dealing with requests for appropriations cannot be equated with statutes enacted by Congress.”).
personnel and under their control.\textsuperscript{137} The second element— Influencing political, military or economic conditions abroad—was intended by Congress (or at least the Senate intelligence committee) to include nearly all “activities to influence conditions” abroad; this purports to be an objective test, and it was not intended to require an articulable link to specific foreign policy or defense objectives.\textsuperscript{138} The third and “essential element of a covert action is that the role of the United States in the activity is not apparent and not intended to be acknowledged at the time it is undertaken.”\textsuperscript{139} The Conference Report stressed an activity is not covert action “unless the fact of United States government involvement in the activity is itself not intended to be acknowledged.”\textsuperscript{140}

Importantly, “covert action” is a noun, which suggests that covert may be used as an adverb in situations that do not amount to covert action. Additionally, the statutory definition of covert action makes no distinction between kinetic activities (e.g., direct action like the operation to kill or capture Osama bin Laden) or nonkinetic activities (e.g., intelligence gathering). What turns a covert activity into “covert action” is its intended effect— influencing conditions abroad.

Returning to our analysis here, any U.S. military operation abroad would certainly meet the first and second element. The first element would be objectively met if the military operation was conducted by U.S. military personnel. Unconventional warfare could potentially require further analysis, but the existence of an unconventional warfare execute order\textsuperscript{141} would certainly suggest the pertinent third parties would be under some

\textsuperscript{137} 50 U.S.C. § 413b(e) (2006). Under the control of U.S. government personnel includes “receiving direction and assistance . . . significant financial support or other significant forms of tangible material support . . . .”

\textsuperscript{138} At the time of this legislation, the working definition of “special activities” (a euphemism for covert action) in E.O. 12,333 included this element: “in support of national foreign policy objectives abroad.” The Senate Report rejected this element as written because it wanted to eliminate the arguable distinction between foreign policy and defense policy, which had been invoked by the executive branch. Id.

\textsuperscript{139} 50 U.S.C. § 413b(e) (2006).

\textsuperscript{140} H.R. REP. NO. 102-166, \textit{supra} note 129, at 29. The Report acknowledges that “it is not possible to craft a definition of ‘covert action’ so precise as to leave no areas of ambiguity in its potential application.”

\textsuperscript{141} JOINT PUBLICATION 5-0, JOINT OPERATION PLANNING (Dec. 26, 2006) at GL-9, GL-11 and I-25 [hereinafter, JP 5-0]. An Execute Order is an “order issued by the Chairman of the Joint Chiefs of Staff, at the direction of the Secretary of Defense, to implement a decision by the President to initiate military operations.” \textit{Id.} at GL-9.
form of U.S. control. The second element would similarly be easily established, as it is difficult to imagine a military operation abroad that would not have some objective influence on conditions abroad (accepting the Senate intelligence committee’s view that the qualifiers “political, military, or economic” are intended to be all-encompassing). Indeed, it is difficult to understand why a military operation would be conducted abroad but for intent to influence conditions. The third “essential” element, then, is key: a military operation could be deemed covert action if it is not intended to be acknowledged.

Simple statutory interpretation suggests several points relevant to our analysis of the acknowledgement element. The first point is simply that acknowledgement must be “intended” at the time the operation is initiated. Circumstances change, but if the U.S. government intends to acknowledge its involvement at the time the military operation is planned and executed, then it is not covert action. The requirement of intention also removes any requirement of actual acknowledgement; whether the operation is actually acknowledged is immaterial, so long as acknowledgement was intended at the time the operation commenced. Second, operational security is distinguishable from attribution—concealment or misrepresentation do not imply or suggest lack of acknowledgement. Military personnel may take great pains to conceal their true identity, but that does not make an operation covert if the intent remains to acknowledge U.S. government involvement at some unspecified time. Third, the statute does not state when the operation must be acknowledged. The legislative history is silent on this point as well, which leaves considerable room for reasonable interpretation by the executive branch. Conceivably, an intention to acknowledge U.S. government involvement two years after the conclusion of the military operation still negates the “is not intended to be acknowledged” element. Fourth, Webster’s Dictionary defines “acknowledge” as “to admit to be real or true,” which implies it is in response to a query or question.142 The U.S. government need not promulgate a press release or make a formal announcement of its involvement in the military operation. Indeed, if the operation is conducted without detection, or if the U.S. government is never asked whether it was

142 Webster’s further explains: “ACKNOWLEDGE implies making a statement reluctantly, often about something previously denied.” WEBSTER’S UNABRIDGED DICTIONARY 17 (Random House, 2d ed. 2001). In the absence of a statutory definition, the courts will generally “construe a statutory term in accordance with its ordinary or natural meaning.” FDIC v. Meyer, 510 U.S. 471, 476 (1994).
responsible for the operation, then the need to acknowledge would not be triggered. The courts generally interpret statutes in a way that gives effect to every word,\textsuperscript{143} which means the intent and acknowledgment elements should be considered independently. In other words, there may be intent to acknowledge without actual acknowledgement, just as there may not be an intent to not acknowledge (deny) that is not exercised because the operation is never discovered.

If a military operation fails any of the three requisite elements in the definition of covert action, it is not covert action. However, even if a military operation meets all three elements, the military operation may still not be covert action. After defining covert action, the statute next lists several exclusions. Covert action "does not include":

(1) activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities;
(2) traditional diplomatic or military activities or routine support to such activities;
(3) traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or
(4) activities to provide routine support to the overt activities (other than activities described in paragraph (1), (2), or (3)) of other United States Government agencies abroad.\textsuperscript{144}

\textsuperscript{143} Bailey v. United States, 516 U.S. 137, 146 (1995) ("[W]e assume that Congress used two terms because it intended each term to have a particular, nonsuperfluous meaning"); Montclair v. Ramsdell, 107 U.S. 147, 152 (1883).

\textsuperscript{144} 50 U.S.C. § 413b(e)(1)-(4) (2006) (emphasis added). The Conference Report that accompanied this statutory definition stated these exclusions "do not fall within the definition of covert action":

1. activities where the primary purpose is to collect intelligence;
2. traditional counterintelligence activities;
3. traditional operational security programs and activities;
4. administrative activities (e.g., pay and employee support);
5. traditional diplomatic activities and their routine support;
6. traditional military activities and their routine support;
7. traditional law enforcement activities and their routine support; or
8. routine support to the overt activities of the U.S. government.
Thus, even unacknowledged unconventional or cyber warfare activities are not covert action if they are a "traditional military activity" or if they could be considered "routine support" to a traditional military activity.

1. Traditional Military Activities are not Covert Action

While several of the activities excluded from the definition of covert action could apply to unconventional and cyber warfare depending on the context and actors involved, our analysis will focus on traditional military activities because of their greater relevance and implications for congressional oversight. The accompanying Conference Report explicitly excludes "traditional military activities" and "routine support" from the definition of covert action, before providing this crucial insight into what Congress intended:

It is the intent of the conferees that "traditional military activities" include activities by military personnel under the direction and control of a United States military commander (whether or not the U.S. sponsorship of such activities is apparent or later to be acknowledged) preceding and related to hostilities which are either anticipated (meaning approval has been given by the National Command Authorities for the activities and for operational planning for hostilities) to involve U.S. military forces, or where such hostilities involving United States military forces are ongoing, and, where the fact of the U.S. role in the overall operation is apparent or to be acknowledged publicly. In this regard, the conferees intend to draw a line between activities that are and are not under the direction and control of the military commander. Activities that are not under the direction and

145 If the primary purpose of an activity is to collect intelligence, then presumably such activities would be considered "intelligence activities" under E.O. 12,333, and the intelligence committees would exercise oversight. However, defining an activity as a traditional military activity places the activity under oversight of the armed services committees. The congressional intelligence committees fear that the military prefers the less intrusive oversight of the armed services committees and, thus, incorrectly defines all military intelligence-related activities as traditional military activities.
control of a military commander should not be considered as "traditional military activities." 146

The Conference Report test for traditional military activities suggests four elements. Traditional military activities are:

1. conducted by U.S. military personnel,
2. under the direction and control of a U.S. military commander,
3. preceding and related to anticipated hostilities or related to ongoing hostilities involving U.S. military forces, and
4. the U.S. role "in the overall operation is apparent or to be acknowledged publicly"

Elements 1 and 2 are relatively straightforward: traditional military activities must be conducted, directed, and controlled by U.S. military personnel. Element 2, military command and control, distinguishes traditional military activities from any situation in which special operations personnel are seconded to the CIA and operating under the direction and control of CIA personnel. 147 The most recent example of such a scenario was the operation to kill or capture Osama bin Laden, which is discussed in the introduction to this Article. The chain of command, as described by Panetta, apparently ran from the President to the Director of Central Intelligence to the Commander of Joint Special Operations Command. 148 As the operation was conducted under the direction and control of the CIA and was not (originally) intended to be acknowledged, the operation could not be considered a traditional military activity and was classified as covert action.

Element 2, or direction and control, will not necessarily be dispositive because the Secretary of Defense is authorized by law and executive order to conduct intelligence activities and military operations. As we saw in Part II, the Secretary of Defense's statutory authorities are grounded in his Title 10 authorities as head of DoD (e.g., 10 U.S.C. §113), his Title 10 intelligence authorities (e.g., 10 U.S.C. § 137), his Title 50

146 Conference Report, supra note 129 (emphasis added).
147 In 1962, President John F. Kennedy issued National Security Action Memorandum 162, which assigned Army Special Forces ("Green Berets") to support CIA covert paramilitary operations and even directed DoD to provide funding to those CIA-led operations. ROTHSTEIN, supra note 75, at 38.
148 See supra note 2 and accompanying text.
intelligence authorities (e.g., 50 U.S.C. §403-5), and his delegated authorities contained in Executive Order 12,333 and elsewhere.\footnote{149} Element 3 introduces the subjective terms “preceding and related to” and “anticipated” hostilities. These terms raise several questions: how far in advance does “preceding” include, how closely “related” must the activities and hostilities be, and does “anticipated” imply imminence or require a high probability of occurrence? With respect to the word “anticipated,” the Conference Report provides some clarity by stating that “anticipated” means “approval has been given by the National Command Authorities for the activities and for the operational planning for hostilities.”\footnote{150} Such approval is evidenced by the existence of a Planning Order, Warning Order, or Execute Order issued at the direction of the Secretary of Defense.\footnote{151} Thus, actual hostilities will be obvious and anticipated hostilities will be evidenced by an order of some sort, so any ambiguity with respect to element 3 will likely center on the phrase “preceding and related to.”

Congress did not define “preceding and related to,” but the Conference Report stressed that “the conferees intend to draw a line between activities that are and are not under the direction and control of the military commander.”\footnote{152} This point is particularly illuminating as the

\footnote{149} The Secretary of Defense may direct DoD personnel to carry out intelligence activities in response to national intelligence requirements, or to meet the intelligence needs of the military. When DoD personnel conduct intelligence activities in response to national intelligence requirements, they do so primarily under Title 50 authorities (50 U.S.C. § 403-5(b)(1) (2006)) and pursuant to priorities and needs determined by the Director of National Intelligence (50 U.S.C. § 403-1(f) (2006)). When DoD personnel conduct intelligence activities to fulfill military intelligence requirements, those intelligence activities are conducted under Title 10 authorities, e.g., 10 U.S.C. §§ 113, 164 (2006), and delegated authorities from the President and Secretary of Defense; if the DoD personnel are also members of the Intelligence Community (e.g., the National Security Agency) the activities are also conducted pursuant to Title 50 authorities (50 U.S.C. § 403-5 (2006)).


\footnote{151} JP 5-0, supra note 141, at GL-11 and I-25. The issuance of an Execute Order is no mere technicality. Execute Orders are typically preceded by Planning Orders and a planning phase, so the Execute Order signals the transition from planning to operations. A Planning Order is a “directive that provides essential planning guidance and directs the initiation of execution planning before the directing authority approves a military course of action.” Id. at GL-20.

\footnote{152} Conference Report, supra note 129, at 30.
Conference Report next suggests that unacknowledged “activities undertaken well in advance of a possible or eventual U.S. military operation” will be deemed covert action unless they can be considered “routine support” to the anticipated military operation.\(^{153}\)

“Routine support” as defined by Congress includes “cacheing communications equipment or weapons, the lease or purchase from unwitting sources of residential or commercial property to support an aspect of an operation, or obtaining currency or documentation for possible operational uses, if the operation as a whole is to be publicly acknowledged.”\(^{154}\) The report continues:

The Committee would regard as "other-than-routine" support activities undertaken in another country that involve other than unilateral activities. Examples of such activity include clandestine attempts to recruit or train foreign nationals with access to the target country to support U.S. forces in the event of a military operation; clandestine effects to influence foreign nationals of the target country concerned to take certain actions in the event of a U.S. military

\(^{153}\) Id. The Conference Report then refers readers to the Senate Report, which states

The Committee also recognizes that even in the absence of anticipated or ongoing hostilities involving U.S. military forces there could potentially be requirements to conduct activities abroad which are not acknowledged by the United States to support the planning and execution of a military operation should it become necessary. Whether or not other forms of support for the planning and execution of military operations could constitute 'covert actions' will depend, in most cases, upon whether they constitute 'routine support' to a military operation.”

S. REP. NO. 102-85, supra note 135, at 47. The Senate Report contained more restrictive language than what was included in the final Conference Report. For example, the Senate report found acknowledgement (or the lack thereof) to be a deciding factor, while the Conference Report rightfully concluded that the exercise of command and control is decisive. Compare Conference report, supra note 135, with S. REP. NO. 102-85 (1991) (Conf. Rep.). See also Gross, infra note 169, at 8. This issue was revisited in 2003 when the SSCI attempted to assert that unacknowledged operations in countries where U.S. military forces do not have an acknowledged presence would fall within the definition of covert action. The unclassified portion of the intelligence authorization act that passed the Senate in November 2003 did not include this controversial assertion and instead reaffirmed “the functional definition of covert action.” Kibbe, supra note 8, at 107.

\(^{154}\) Conference Report, supra note 129, at 30.
operation; clandestine efforts to influence and effect public opinion in the country concerned where U.S. sponsorship of such efforts is concealed; and clandestine efforts to influence foreign officials in third countries to take certain actions without the knowledge or approval of their government in the event of a U.S. military operation.  

The Conference Report defines traditional military activities and stresses that military “direction and control” is a deciding factor. The Conference Report then defers to the Senate Report to further define “routine support” of traditional military activities, which then introduces the distinction between unilateral activities and the use of foreign nationals. Read in context, the “routine support” definition only applies to activities that are not under the direction and control of a military commander.  

To summarize, an essential element of covert action is lack of intended acknowledgement of the overall operation, so the existence of intended acknowledgement obviates any need for further analysis under the traditional military activities exception. The only time the military would need to concern itself with analysis under the traditional military activities exception is when the specific military operation is not intended to be acknowledged. In that situation, the next analytical step is to determine whether the specific unacknowledged military operation is a traditional military activity. If an unacknowledged activity is 1) conducted by military personnel, 2) under military direction and control, and 3) pursuant to an order issued or authorized by the Secretary of Defense, then the only remaining requirement to escape falling within the definition of covert action is that 4) the U.S. role in the overall anticipated military operation must be acknowledged. Notwithstanding this relatively straightforward analysis, military preparatory operations continue to raise congressional ire.

---

155 Id.
156 It is inconceivable that U.S. military personnel would conduct an activity overseas without the existence of an authorization order from the Secretary of Defense. Thus, the routine support provision seems intended to address those situations where non-military personnel are used to provide support to anticipated military operations. Read as such, Congress’s distinction between unilateral activities and those involving foreign nationals seems logical.
2. Military Preparatory Operations are Traditional Military Activities

Over the past ten years, members of the congressional intelligence committees repeatedly expressed frustration with what they see as DoD’s deliberate side-stepping of their oversight by renaming intelligence activities as “operational preparation of the environment.” These congressional concerns are most commonly raised in the context of intelligence activities conducted during the period preceding hostilities. This is the period where conflict is portended but not yet inevitable: when military forces begin making preparations for possible conflict. These preparatory operations are what the U.S. military calls “operational preparation of the environment,” or OPE.

In its report accompanying the Intelligence Authorization Act for 2010, HPSCI criticized DoD for frequently labeling its clandestine activities as OPE “to distinguish particular operations as traditional military activities and not as intelligence functions” and, implicitly, escape intelligence oversight. HPSCI opined that this practice made the distinction all but meaningless as DoD “has shown a propensity to apply the OPE label where the slightest nexus of a theoretical, distant military operation might one day exist.” HPSCI argues that this practice obfuscates the military operations from congressional oversight, yet our analysis in Part II revealed that oversight of OPE should still be exercised by the armed services committee.

A fundamental concern of the intelligence committees is that DoD’s clandestine activities labeled as OPE “carry the same diplomatic and

---


158 House Permanent Select Committee on Intelligence, Report Accompanying the Intelligence Authorization Act for Fiscal Year 2010, 111th Congress, 2nd Session, at 10 (Jun. 25, 2009). This bill was passed by the House but not by the Senate. In fact, the House and Senate have failed to enact an intelligence authorization act for the past five years. The Intelligence Community is able to expend appropriations only because of the unique provision of 10 U.S.C. § 413 (2006), which pre-authorizes intelligence appropriations.

159 Id. at 11.

160 See, e.g., the written questions posed to General Keith Alexander by the Senate Armed Services Committee prior to his confirmation as Commander of U.S. Cyber Command.
national security risks as traditional intelligence-gathering activities."\(^{161}\) Where Title 50 requires that the intelligence committees be kept "fully and currently informed" of all intelligence activities, Title 10 does not have a corresponding requirement that the armed services committees be kept informed of all military operations. More importantly, the intelligence committees fear that DoD is skirting the formal Presidential approval and reporting requirements for covert action by evasively naming equivalent activities as OPE.\(^{162}\)

Clandestine activities are generally distinguished from covert activities in that clandestine activities are conducted secretly, but if activity is discovered the role of the United States will ultimately be acknowledged.\(^{163}\) If the U.S. government intends to acknowledge the clandestine activities at some point, then they fail the third definitional element for covert action. If the U.S. government does not intend to acknowledge clandestine activities of the U.S. military, then the question becomes whether those clandestine activities are traditional military activities. If so, then the statutory covert action paradigm does not apply as a matter of law.

The Senate Select Committee on Intelligence expressed frustration in 2009 with what it viewed as overly broad interpretations of traditional military activities by the Executive Branch. In questions submitted to Admiral Dennis Blair, the nominee for Director of National Intelligence, and Leon Panetta, then the nominee for the position of Director of Central Intelligence, SSCI asked both nominees to distinguish "between covert action, military support operations, and operational preparation of the

\(^{161}\) HPSCI Report, supra note 158, at 11.

\(^{162}\) See Nomination of General Michael V. Hayden USAF to be Director of the Central Intelligence Agency: Hearing Before the S. Select Comm. on Intelligence, 109th Cong., 2d Sess. 26–7 (May 18, 2006).


An operation sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment. A clandestine operation differs from a covert operation in that emphasis is placed on concealment of the operation rather than on concealment of the identity of the sponsor. In special operations, an activity may be both covert and clandestine and may focus equally on operational considerations and intelligence-related activities."

JP 1-02, supra note 115, at 89.
environment." Panetta answered by correctly emphasizing that covert action is defined by statute to be actions "where the role of the U.S. will not be acknowledged" and "traditional military activities are exempt from the definition." Panetta opined that "the line between covert actions under Title 50 and clandestine military operations under Title 10 has blurred" and expressed concern that "Title 10 operations, though practically identical to Title 50 operations, may not be subjected to the same oversight as covert actions, which must be briefed to the Intelligence Committees."

When Panetta stated "the line between covert actions under Title 50 and clandestine military operations under Title 10 has blurred," he seems to have meant that the activities in question appear increasingly similar—not that the statutory authorities to conduct the activities have blurred. General Michael Hayden emphasized this distinction during his confirmation hearings prior to becoming Director of the NSA: OPE and foreign intelligence gathering may appear similar in terms of "tradecraft" but the "legal blood line[s]" are different—"different authorities, somewhat different purposes, mostly indistinguishable activities."

---

164 Here is the Committee's complete question: "As you know, the Under Secretary of Defense for Intelligence has Title 10 and Title 50 authorities. The USD(I) was dual-hatted by DNI McConnell to serve concurrently as his Deputy Director for Defense. Yet, the USD(I) has, on occasion, asserted that this Committee does not have primary jurisdiction over his programs. This is of particular concern to this Committee as the USD(I) has interpreted Title 10 to expand "military source operations" authority, allowing the Services and Combatant Commands to conduct clandestine HUMINT operations worldwide. These activities can come awfully close to activities that constitute covert action." Nomination of the Honorable Leon E. Panetta to be Director, Central Intelligence Agency: Hearing Before S. Select Comm. on Intelligence, 111th Cong., 1st Sess. 94 (2009); Nomination of Dennis C. Blair to be Director of National Intelligence: Hearing Before the S. Select Comm. on Intelligence, 111th Cong., 1st Sess. 116 (2009).

165 Blair, supra note 164, at 117.


167 Id.

168 Nomination of General Michael V. Hayden USAF to be Director of the Central Intelligence Agency, Hearing Before the S. Select Comm. on Intelligence, 109th Cong., 2d Sess. 116 (May 18, 2006). General Hayden continued,
The concern of the intelligence committees, then, is that the military is increasingly conducting activities that appear very similar to activities conducted by the CIA and other members of the intelligence community, yet those activities are not subject to the oversight of the intelligence committees. These secret military activities are not covert action because they are either intended to be acknowledged at some point or they are traditional military activities. The intended acknowledgement element is difficult to argue against, so the intelligence committees seem to be centering their arguments for oversight of the military’s secret activities by suggesting that these are not actually traditional military activities.

Unacknowledged unconventional or cyber warfare may legally be conducted when directed by the President and Secretary of Defense in preparation for an anticipated conventional conflict, and those unacknowledged activities are excluded from the definition of covert action. Put another way, if the unconventional or cyber warfare activity at issue can be considered a “traditional military activity,” then it is not covert action; if the activity at issue is “routine support” to a traditional military activity,” then it is not covert action. Neither exclusion from the definition of covert action makes any reference to whether the activity at issue will be acknowledged by the U.S. government should its existence become public.

VI. Conclusion

This article identified four general concerns that are colloquially described as “Title 10-Title 50” issues. Two concerns, military transparency and rice bowls, fall squarely within the policy realm. They are genuine

My view is that, as the national HUMINT manager, the Director of CIA should strap on the responsibility to make sure that this thing down here that walks and quacks and talks like human intelligence is conducted to the same standards as human intelligence without questioning the Secretary's authority to do it or the legal authority under which that authority is drawn.

concerns, but generally reflect policy concerns, including a competition for scarce resources, rather than legal challenges. Military leaders must vigilantly ensure the U.S. military retains the respect and admiration of the American public and executive branch bureaucrats will always seek to protect their domains, but debates over transparency and rice bowls should not keep military operators awake at night. On the other hand, the critical questions of operational authorities and congressional oversight are central to our national security framework and must be carefully defined and understood by operators and policy-makers alike.

Congress’s failure to provide necessary interagency authorities and budget authorizations threatens our ability to prevent and wage warfare. Congress’s stubborn insistence that military and intelligence activities inhabit separate worlds casts a pall of illegitimacy over interagency support, as well as unconventional and cyber warfare. The U.S. military and intelligence agencies work together more closely than perhaps at any time in American history, yet Congressional oversight and statutory authorities sadly remain mired in an obsolete paradigm. After ten years of war, Congress still has not adopted critical recommendations made by the 9/11 Commission regarding congressional oversight of intelligence activities. Congress’s stovepiped oversight sows confusion over statutory authorities and causes Executive Branch attorneys to waste countless hours distinguishing distinct lines of authority and funding. Our military and intelligence operatives work tirelessly to coordinate, synchronize, and integrate their efforts; they deserve interagency authorities and Congressional oversight that encourages and supports such integration.
Panel II:

Role of the Judiciary in National Security

Moderator: Viet Dinh
National Security Case Studies

Special Case-Management Challenges

Robert Timothy Reagan
Federal Judicial Center

June 25, 2013

This Federal Judicial Center publication was undertaken in furtherance of the Center’s statutory mission to develop and conduct research and education programs for the judicial branch. While the Center regards the content as responsible and valuable, it does not reflect policy or recommendations of the Board of the Federal Judicial Center.
Contents

Table of Challenges xi
Table of Judges xiii
INTRODUCTION 2

TERRORISM PROSECUTIONS 3

First World Trade Center Bombing
United States v. Salameh (Kevin Thomas Duffy) and United States v. Abdel Rahman (Michael B. Mukasey) (S.D.N.Y.) 5

Challenge: Interpreters 24
Challenge: Court Security 24
Challenge: Pro Se Defendant 24
Challenge: Jury Security 24
Challenge: Classified Evidence 25
Challenge: Terrorist Communications 26

Kenya and Tanzania

Challenge: Attorney-Client Contacts 42
Challenge: Interpreters 44
Challenge: Mental Health During Detention 44
Challenge: Jury Security 46
Challenge: Court Security 46
Challenge: Witness Security 47
Challenge: Religious Accommodation 48
Challenge: Classified Evidence 49
Challenge: Classified Arguments 51
Challenge: Classified Orders and Opinions 51
Challenge: Subpoenaing a Cabinet Officer 52

Millennium Bomber

Challenge: Classified Evidence 63
Challenge: Examination of Foreign Witnesses 64
Challenge: Court Security 64
Challenge: Jury Security 65
Challenge: Witness Security 65

Mujaheddin Khaliji
Challenge: Classified Evidence 68

Detroit
United States v. Koubriri (Gerald E. Rosen, E.D. Mich.) 69
Challenge: Jury Security 74
Challenge: Sanctioning a Cabinet Officer 74
Challenge: Classified Evidence 76

Twentieth Hijacker
United States v. Moussaoui (Lonnie M. Brinkema, E.D. Va.) 78
Challenge: Attorney Appointment 88
Challenge: Pro Se Defendant 89
Challenge: Court Security 89
Challenge: Jury Security 90
Challenge: Classified Evidence 90
Challenge: Classified Arguments 92
Challenge: Closed Proceedings 94
Challenge: Classified Opinion 95
Challenge: Terrorist Communications 95

American Taliban
United States v. Ladd (T.S. Ellis III, E.D. Va.) 98
Challenge: Protected National Security Information 100
Challenge: Classified Evidence 102
Challenge: Interviewing Guantanamo Bay Detainees 102
Challenge: Witness Security 103
Challenge: Religious Accommodation 104

Dirty Bomber
Challenge: Attorney-Client Contacts 114
Challenge: Mental Health During Detention 115
Challenge: Classified Arguments 116
Challenge: Witness Security 117
Challenge: Court Security 117
Challenge: Jury Security 118
Challenge: Classified Evidence 118
Challenge: FISA Evidence 119

Lackawanna
United States v. Goba (William M. Skretny and H. Kenneth Schroeder, Jr., W.D.N.Y.) 121
Challenge: Classified Evidence 126
Challenge: Court Security 126
Challenge: Religious Accommodation 127
A Plot to Kill President Bush
United States v. Abu Ali (Gerald Bruce Lee, E.D. Va.) ........................................ 128
Challenge: Examination of Foreign Witnesses and Witness Security 130
Challenge: Attorney-Client Contacts ................................................................. 131
Challenge: Classified Evidence ........................................................................ 131
Challenge: Classified Arguments .................................................................. 133

Paintball
Challenge: Classified Evidence ........................................................................ 143
Challenge: Closed Proceedings ....................................................................... 143
Challenge: Classified Arguments .................................................................... 144
Challenge: Attorney-Client Contacts .............................................................. 144
Challenge: Religious Accommodation ............................................................ 145

Minneapolis
United States v. Warsame (John R. Tunheim, D. Minn.) ................................. 146
Challenge: Mental Health During Detention .................................................. 148
Challenge: Attorney-Client Contacts .............................................................. 148
Challenge: Classified Evidence ....................................................................... 149
Challenge: FISA Evidence .............................................................................. 150

Ashland and Moscow
United States v. Al-Haramain Islamic Foundation, Inc. (Michael R. Hogan and
Thomas M. Coffin, D. Or.), Al-Haramain Islamic Foundation, Inc. v. United
States (Garr M. King, D. Or.), United States v. Al-Husayen and Al-Kidd v.
Gonzalez (Edward J. Lodge and Mikel H. Williams, D. Idaho) ....................... 151
Challenge: Classified Evidence ....................................................................... 161
Challenge: Classified Arguments ................................................................... 165
Challenge: Closed Proceedings ..................................................................... 165
Challenge: Classified Orders and Opinions .................................................... 166
Challenge: Examination of Foreign Witnesses ............................................. 166
Challenge: FISA Evidence ............................................................................. 167

Prosecution of a Charity
United States v. Holy Land Foundation (A. Joe Fish and Jorge A. Solis,
N.D. Tex.) ........................................................................................................ 169
Challenge: Classified Evidence ....................................................................... 175
Challenge: FISA Evidence ............................................................................. 176
Challenge: Witness Security ........................................................................... 177
Challenge: Jury Security ................................................................................. 178

Chicago
United States v. Abu Marzook (Amy St. Eve, N.D. Ill.) ................................... 180
Challenge: Foreign Government Evidence .................................................. 186
Challenge: Witness Security ........................................................................... 187

Challenge: Classified Evidence ................................................................. 188
Challenge: Classified Arguments ................................................................ 190
Challenge: Classified Opinion ..................................................................... 190
Challenge: Jury Security ............................................................................... 190

Lodi
United States v. Hayat (Garland E. Burrell, Jr., E.D. Cal.) ......................... 191
Challenge: Classified Evidence ...................................................................... 195

Toledo
United States v. Amawi and Related Actions (James G. Carr, N.D. Ohio) ..... 198
Challenge: Attorney-Client Contacts .............................................................. 202
Challenge: FISA Evidence ............................................................................. 203
Challenge: Court Security ............................................................................. 203
Challenge: Jury Security ............................................................................... 204

Atlanta
United States v. Ahmed (Clarence Cooper, William S. Daffey, Jr., and Gerrilyn
G. Brill, N.D. Ga.) ............................................................................................ 205
Challenge: Closed Proceeding ...................................................................... 210
Challenge: Attorney Appointment ................................................................. 210
Challenge: Classified Evidence ...................................................................... 210
Challenge: FISA Evidence ............................................................................. 212

Sears Tower
United States v. Batiste (Joan A. Lenard, S.D. Fla.) ....................................... 214
Challenge: Classified Evidence ...................................................................... 218
Challenge: Jury Security ............................................................................... 218
Challenge: Pro Se Defendant ......................................................................... 218

Fort Dix
United States v. Shouwer (Robert B. Kugler, D.N.J.) ..................................... 219
Challenge: Classified Evidence ...................................................................... 223
Challenge: FISA Evidence ............................................................................. 223
Challenge: Classified Opinion ...................................................................... 224
Challenge: Jury Security ............................................................................... 224
Challenge: Court Security ............................................................................. 224
Challenge: Attorney Appointment ................................................................. 225

Triangle Takedown
United States v. Boyd (Louise W. Flanagan, Malcolm J. Howard, William Arthur
Webb, and James E. Gates) and United States v. Sherif (W. Earl Britt)
(E.D.N.C.) ....................................................................................................... 226
Challenge: Attorney Appointment ................................................................. 232
Challenge: Pro Se Defendants ........................................................................ 233
Challenge: Interpreters .................................................................................. 235
Challenge: Court Security .............................................................................. 235
Challenge: Jury Security ............................................................................... 236
Challenge: FISA Evidence ............................................................................. 237
Challenge: Classified Evidence .................................................. 237
Challenge: Sensitive Unclassified Evidence ............................... 239
ESPIONAGE PROSECUTIONS .................................................. 240
Would-Be Spy
United States v. Began (Gerald Bruce Lee, E.D. Va.) ................. 241
Challenge: Classified Evidence ................................................. 242
Giving State Secrets to Lobbyists
United States v. Franklin (T.S. Ellis III, E.D. Va.) ....................... 245
Challenge: Classified Evidence ................................................. 249
Challenge: Subpoenaing a Cabinet Officer ............................... 250
Challenge: Classified Orders .................................................... 251
Challenge: Closed Proceedings .................................. 251
Challenge: Classified Arguments ............................................. 252
OTHER CRIMINAL CASES .................................................. 253
Interrogation Death in Afghanistan
United States v. Parsaro (Terrence W. Boyle, E.D.N.C.) ............. 254
Challenge: Classified Evidence ................................................. 257
Challenge: Classified Arguments ............................................. 258
Challenge: Subpoenaing Senior Government Officials ............... 258
Challenge: Witness Security .................................................... 259
Challenge: Closed Proceeding ................................................. 259
Castro Foe
United States v. Posada Carriles (Kathleen Cardone, W.D. Tex.) 260
Challenge: Classified Evidence ................................................. 267
Challenge: Classified Orders .................................................... 268
Challenge: Sensitive Unclassified Evidence .............................. 269
Challenge: Court Security ....................................................... 269
Challenge: Jury Security ........................................................ 269
Challenge: Witness Security .................................................... 269
HABEAS CORPUS .................................................................. 271
Guantanamo Bay
Challenge: Attorney-Client Contacts ........................................ 337
Challenge: Classified Evidence ................................................. 348
Challenge: Sensitive Unclassified Information .......................... 356
Challenge: Classified Arguments ............................................. 358
Challenge: Closed Proceedings and Remote Participation ....... 362
Challenge: Classified Orders and Opinions ............................. 366
Challenge: Interpreters ........................................................... 372
Challenge: Mental and Physical Health During Detention ......... 372
Challenge: Religious Accommodation ................................... 378
Challenge: Ordering Testimony from an Ambassador ............ 378
OTHER CIVIL CASES .................................................. 380
Burma
Horn v. Huddle (Royce C. Lambert, D.D.C.) ............................. 381
Challenge: Classified Evidence ................................................. 383
Challenge: Classified Arguments ............................................. 384
September 11 Damages
In re Terrorist Attacks on September 11, 2001 (Richard Connway Casey and George B. Daniels) and In re September 11 Litigation and Related Actions (Alvin K. Hellerstein, S.D.N.Y.) ................................. 385
Challenge: Service of Process on International Terrorists .......... 404
Challenge: Classified Evidence ................................................. 405
Challenge: Sensitive Unclassified Information .......................... 405
Challenge: Witness Security .................................................... 408
Challenge: Foreign Government Evidence ............................. 408
Mistaken Rendition
El-Masri v. Tenet (T.S. Ellis III, E.D. Va.) ................................. 409
Challenge: Classified Arguments ............................................. 411
Detainee Documents
ACLU v. Department of Defense (Alvin K. Hellerstein, S.D.N.Y.) 413
Challenge: Classified Evidence ................................................. 416
Challenge: Classified Arguments ............................................. 417
Surveillance Software
Challenge: Classified Evidence ................................................. 422
Warrantless Wiretaps
Challenge: Classified Evidence ................................................. 451
Challenge: Classified Arguments ............................................. 457
Challenge: Classified Opinion ............................................... 471
Challenge: Redacting Secrets .................................................. 471
<table>
<thead>
<tr>
<th>Table of Case-Management Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attorney Issues</td>
</tr>
<tr>
<td>Attorney Appointment</td>
</tr>
<tr>
<td>Attorney-Client Contacts</td>
</tr>
<tr>
<td>Foreign Evidence</td>
</tr>
<tr>
<td>Examination of Foreign Witnesses</td>
</tr>
<tr>
<td>Foreign Government Evidence</td>
</tr>
<tr>
<td>Information Protection</td>
</tr>
<tr>
<td>Classified Arguments</td>
</tr>
<tr>
<td>Classified Evidence</td>
</tr>
<tr>
<td>Classified Orders and Opinions</td>
</tr>
<tr>
<td>Closed Proceedings</td>
</tr>
<tr>
<td>Court-Appointed National Security Expert</td>
</tr>
<tr>
<td>FISA Evidence</td>
</tr>
<tr>
<td>Interviewing Detainees</td>
</tr>
<tr>
<td>Protected National Security Information</td>
</tr>
<tr>
<td>Redacting Secrets</td>
</tr>
<tr>
<td>Remote Participation</td>
</tr>
<tr>
<td>Sensitive Unclassified Information</td>
</tr>
<tr>
<td>Interpreters</td>
</tr>
<tr>
<td>Mental and Physical Health During Detention</td>
</tr>
<tr>
<td>Physical Security</td>
</tr>
<tr>
<td>Court Security</td>
</tr>
<tr>
<td>Jury Security</td>
</tr>
<tr>
<td>Witness Security</td>
</tr>
<tr>
<td>Pro Se Defendants</td>
</tr>
<tr>
<td>Religious Accommodation</td>
</tr>
<tr>
<td>Senior Government Officers</td>
</tr>
<tr>
<td>Sanctions</td>
</tr>
<tr>
<td>Subpoenas</td>
</tr>
<tr>
<td>Terrorist Contacts</td>
</tr>
<tr>
<td>Service of Process on International Terrorists</td>
</tr>
<tr>
<td>Terrorist Communications</td>
</tr>
<tr>
<td>Table of Judges</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>Bulkelder, Alice M. (6th Cir.)</td>
</tr>
<tr>
<td>Bates, John D. (D.D.C.)</td>
</tr>
<tr>
<td>Boyle, Terrence W. (E.D.N.C.)</td>
</tr>
<tr>
<td>Brill, Gerrilyn G. (N.D. Ga.)</td>
</tr>
<tr>
<td>Brinkema, Leonie M. (E.D. Va.)</td>
</tr>
<tr>
<td>Britt, W. Earl (E.D.N.C.)</td>
</tr>
<tr>
<td>Burrell, Garland E., Jr. (E.D. Cal.)</td>
</tr>
<tr>
<td>Cabrera, José A. (2d Cir.)</td>
</tr>
<tr>
<td>Cacheris, James C. (E.D. Va.)</td>
</tr>
<tr>
<td>Cardone, Kathleen (W.D. Tex.)</td>
</tr>
<tr>
<td>Carney, Cormac J. (C.D. Cal.)</td>
</tr>
<tr>
<td>Carr, James G. (N.D. Ohio)</td>
</tr>
<tr>
<td>Carter, David O. (C.D. Cal.)</td>
</tr>
<tr>
<td>Casey, Richard Conway (S.D.N.Y.)</td>
</tr>
<tr>
<td>Coffin, Thomas M. (D. Or.)</td>
</tr>
<tr>
<td>Collyer, Rosemary M. (D.D.C.)</td>
</tr>
<tr>
<td>Cooke, Marcia G. (S.D. Fla.)</td>
</tr>
<tr>
<td>Cooke, Valerie P. (D. Nev.)</td>
</tr>
<tr>
<td>Cooper, Clarence (N.D. Ga.)</td>
</tr>
<tr>
<td>Coughenour, John C. (W.D. Wash.)</td>
</tr>
<tr>
<td>Daniels, George B. (S.D.N.Y.)</td>
</tr>
<tr>
<td>Duffy, William S., Jr. (N.D. Ga.)</td>
</tr>
<tr>
<td>Duffy, Kevin Thomas (S.D.N.Y.)</td>
</tr>
<tr>
<td>Duncan, Allysion K. (4th Cir.)</td>
</tr>
<tr>
<td>Ellis, T.S., III (E.D. Va.)</td>
</tr>
<tr>
<td>Feinberg, Wilfred (2d Cir.)</td>
</tr>
<tr>
<td>Fish, A. Joe (N.D. Tex.)</td>
</tr>
<tr>
<td>Flanagan, Louise W. (E.D.N.C.)</td>
</tr>
<tr>
<td>Floyd, Henry F. (D.S.C.)</td>
</tr>
<tr>
<td>Friedman, Paul L. (D.D.C.)</td>
</tr>
<tr>
<td>Gates, James E. (E.D.N.C.)</td>
</tr>
<tr>
<td>Gibbons, Julia Smith (6th Cir.)</td>
</tr>
<tr>
<td>Gilman, Ronald Lee (6th Cir.)</td>
</tr>
<tr>
<td>Green, Joyce Hens (D.D.C.)</td>
</tr>
<tr>
<td>Gregory, Roger L. (4th Cir.)</td>
</tr>
</tbody>
</table>

Hawkins, Michael Daly (9th Cir.) | 426 |
Hellerstein, Alvin (S.D.N.Y.) | 385, 413 |
Hogan, Michael R. (D. Or.) | 151 |
Hilton, Claude M. (E.D. Va.) | 135 |
Hogan, Thomas F. (D.D.C.) | 272, 426 |
Howard, Malcolm J. (E.D.N.C.) | 226 |
Huvelle, Ellen Segal (D.D.C.) | 272 |
Kaplan, Lewis A. (S.D.N.Y.) | 27 |
Kay, Alan (D.D.C.) | 272 |
Keenan, John F. (S.D.N.Y.) | 54 |
Kennedy, Henry H., Jr. (D.D.C.) | 272, 426 |
Kennelly, Matthew F. (N.D. Ill.) | 426 |
Kessler, Gladys (D.D.C.) | 272 |
King, Garry M. (D. Or.) | 151, 426 |
King, Robert B. (4th Cir.) | 245, 409 |
Kollar-Kotelly, Colleen (D.D.C.) | 272 |
Kugler, Robert B. (D.N.J.) | 219 |
Lambert, Royce C. (D.D.C.) | 272, 381 |
Lee, Gerald Bruce (E.D. Va.) | 128, 241 |
Lenard, Joan A. (S.D. Fla.) | 214 |
Leon, Richard J. (D.D.C.) | 272 |
Lodge, Edward J. (D. Idaho) | 151 |
Lynch, Gerard E. (S.D.N.Y.) | 426 |
McKeown, M. Margaret (9th Cir.) | 426 |
Motz, Diana Gribbon (4th Cir.) | 128 |
Mukasey, Michael B. (S.D.N.Y.) | 5, 105 |
Newman, Jon O. (2d Cir.) | 27 |
Oberdorfer, Louis F. (D.D.C.) | 272 |
Pregerson, Harry (9th Cir.) | 426 |
Pro, Philip M. (D. Nev.) | 418 |
Roberson, James (D.D.C.) | 272 |
Rosen, Gerald E. (E.D. Mich.) | 69 |
St. Eve, Amy (N.D. Ill.) | 180 |
Sand, Leonard B. (S.D.N.Y.) | 27 |
Schroeder, H. Kenneth, Jr. (W.D.N.Y.) | 121 |
Shedd, Dennis W. (4th Cir.) | 78, 245, 409 |
INTRODUCTION

National security cases often pose unusual and challenging case-management issues for the courts. Evidence or arguments may be classified; witnesses or the jury may require special security measures; attorneys' contacts with their clients may be diminished, other challenges may present themselves.

The purpose of this Federal Judicial Center resource is to assemble methods federal judges have employed to meet these challenges so that judges facing the challenges can learn from their colleagues' experiences.

These case studies include background factual information about a selection of national security cases as well as descriptions of the judges' challenges and solutions. The information presented is based on a review of case files and news media accounts and on interviews with the judges.

Classified Information Security Officers. Crucial in courts' handling of classified information are classified information security officers, who are detailed to the courts by the Department of Justice's Litigation Security Group. Until January 15, 2011, they were known as "court security officers," which was confusing because that term is used for persons who provide courthouses with physical security.

Hyperlinks. An Acrobat copy of this document posted within the judiciary at FJC Online includes hyperlinks among the footnotes. Embedded in citations to published opinions are hyperlinks to their Westlaw postings. Citations to unpublished orders and opinions often include hyperlinks to copies of the documents available at FJC Online. Embedded in citations to other court documents are hyperlinks to the relevant court's PACER site.

Other Publications. Lessons learned from these case studies are summarized in National Security Case Management: An Annotated Guide (2011), also available from the Federal Judicial Center.

This publication supersedes the following:

• Terrorism-Related Cases: Special Case-Management Challenges: Case Studies (September 20, 2007)
• Terrorism-Related Cases: Special Case-Management Challenges: Case Studies (March 26, 2008)
• National Security Case Studies: Special Case-Management Challenges (February 22, 2010)
• National Security Case Studies: Special Case-Management Challenges (November 14, 2011)

The following chapters are new: "Mujahedeen Khalqi," "Ashland and Moscow," and "Triangle Takedown" (terrorism prosecutions); "Interrogation Death in Afghanistan" and "Castro Foe" (other criminal cases); and "Surveillance Software" and "Muslim Surveillance" (civil cases).
TERRORISM PROSECUTIONS

Terrorism prosecutions include prosecutions for acts of terrorism, conspiracy on sometimes thwarted acts of terrorism, and material support. Proscribed material support can include financial support ("Ashland and Moscow," "Prosecution of a Charity") or attending terrorism training camps ("Lackawanna," "Lodi"). Some cases include additional charges for false statements.

These prosecutions typically present courts with enhanced security concerns. In addition to physical security concerns about the courthouse, the jury, and sometimes witnesses, there are often information security concerns involving the court’s handling of classified information. Classified information security officers provided by the Justice Department are the experts on how courts keep classified information secure.  

The terrorism prosecutions selected for this collection of case studies range in time from the 1993 bombing of the World Trade Center to 2012 pro se trials in the Eastern District of North Carolina. Prosecutions related to the “First World Trade Center Bombing” included both prosecutions for the 1993 bombing and for thwarted plots to bomb Manhattan tunnels and landmarks and American airplane flights in Asia.

The prosecutions for the 1998 bombings of American embassies in "Kenya and Tanzania" were interrupted by the stabbing of a detention guard, which resulted in another prosecution. One fugitive defendant was not prosecuted until 2009 and 2010; other indicted defendants remain fugitives.

Handling classified information is perhaps the most unusual case-management challenge for courts presiding over national security cases. Occasionally, judges have immersed themselves in classified information ("Detroit"). For one of these cases, that did not become necessary until it was time to sentence the defendants ("Mujahedeen Khalaf"). A terrorism prosecution, however, may involve no classified information at all ("Sears Tower").

Sometimes, to protect national security, a jury is presented with an unclassified substitute for classified information, such as a summary or an admission. A jury instruction may help the jury understand how and why classified information is avoided in the trial ("Chicago"). Courts might also employ the silent witness rule, in which a limited amount of classified information is presented to the jury, such as the identity of a person or a country referred to. The classified information is kept from the public, but it must not be kept from the defendant himself ("A Plot to Kill President Bush").

Witnesses are sometimes afforded extra protection to conceal their identities from the public ("American Taliban," "Chicago"). It is also not uncommon for terrorism prosecutions to require foreign evidence ("Millennium Bomber," "A Plot to Kill President Bush," "Ashland and Moscow," "Chicago").

As with other types of litigation, terrorism prosecutions are sometimes complex because of intertwined cases ("First World Trade Center Bombing," "Paintball," "Ashland and Moscow," "Prosecution of a Charity," "Toledo"). Management of the cases' complexity and high profile could benefit from careful developments of protocol, such as the decorum order developed for a prosecution for conspiracy to attack "Fort Dix.

Some terrorism defendants elect to proceed pro se. Perhaps the most famous example is Zacarias Moussaoui ("Twentieth Hijacker"), whose pro se privilege ultimately was taken away because of his disruptive filing behavior. Defendants in other cases were less disruptive ("Atlanta," "Triangle Takedown").

The mental health of defendants subject to strict security measures during pretrial detention can be an issue of concern ("Dirty Bomber," "Minneapolis").

Terrorism prosecutions frequently result in convictions, but sometimes defendants are acquitted. Some acquittals have been followed by deportation ("Ashland and Moscow," "Sears Tower") or a prosecution for something else ("Paintball").

1. Titles in this introductory text refer to chapters in this publication.
First World Trade Center Bombing
United States v. Salameh (Kevin Thomas Duffy) and United States v. Abdel Rahman (Michael B. Mukasey) (S.D.N.Y.)

On Friday, February 26, 1993, a bomb exploded in the parking garage of the World Trade Center in Manhattan, killing six people and injuring more than one thousand. The Bombing of the World Trade Center

On April 24, 1992, Ahmad Mohammad Ajay moved from Houston, Texas, to Pakistan, where he attended a terrorist training camp on the border between Afghanistan and Pakistan called Camp Khalid. He learned how to make bombs, and he met Ramzi Ahmed Yousef. On September 1, 1992, Ajay and Yousef entered the United States using false identities. Ajay’s passport was discovered to be a forgery. He was indicted in the Eastern District of New York, where John F. Kennedy International Airport is located, and imprisoned for six months on a guilty plea. Yousef was stopped for traveling on an Iraqi passport without a visa but released on his own recognizance because the detention center was full. Yousef was convicted of conspiring to commit an act of terrorism, and Yousef and Ajay were found guilty of conspiring to place a bomb in a public place.

In the United States, Yousef assembled a conspiracy of terrorists with the assistance of Mahmoud Abo-Alshemin, Yousef and Mohammad A. Salameh rented in Jersey City, New Jersey, an apartment and a storage unit, where they made and stored explosive materials. Nidal Ayyad, a chemical engineer, acquired the explosives. On February 23, 1993, Salameh rented a Ryder van, which the conspirators loaded with explosive materials. Three days later, Yousef and Eyad Ismoil drove the van to the World Trade Center, where they exploded the bomb by timer at 12:18 p.m. Ayyad anonymously contacted the New York Daily News by telephone and the New York Times by mail to take responsibility for the bomb as retaliation for the United States’ support of Israel. His DNA was found on the New York Times envelope, and a draft of the letter to the Times was found on his computer.

---

3. The 9/11 Commission Report 280 (2004), id. at 71 (“The ensuing explosion opened a hole seven stories up.”)
5. Yousef, 327 F.3d at 78; Salameh, 152 F.3d at 107, Salameh, 54 F. Supp. 2d at 246, 290.
9. Salameh, 152 F.3d at 107; Salameh, 54 F. Supp. 2d at 246, 204, see Blumenthal, supra note 3, McDermott & Mayer, supra note 5, at 45.
11. Yousef, 327 F.3d at 78 n.2, Salameh, 152 F.3d at 107, see Richard Bernstein, Inspector Tertives She Urged No Asylum for Defendant, N.Y. Times, Nov. 16, 1993, at B3, Blumenthal, supra note 3; Lance, supra note 5, at 102; Terry McDermott, Perfect Soldiers 131–32 (2005), McDermott & Meyer, supra note 5, at 45.

---

National Security Case Management Studies (06/25/2013) 5

National Security Case Management Studies (06/25/2013) 6
Investigators discovered the van's vehicle identification number in the bomb's debris. 13 Salameh was arrested when he returned to the Ryder rental office on March 4 to recover a $400 rental deposit on the destroyed van, which he had reported stolen. 18 Because [Yousef] was the financier and had fled the country, leaving his accomplices on their own, Salameh was broke and desperately needed the cash from the deposit. 19

Abouhalima fled to Egypt after the explosion, and he was arrested by Egyptian authorities on March 13. 20 He was returned to the United States on March 25. 21 Yousef and Abdul Rahman Yasin, another conspirator, also fled the country. 22 Yousef was captured in a guesthouse in Pakistan on February 7, 1995. 23 For a $2 million reward, and to avoid prison, one of Yousef's recruits turned him in to the FBI. 24 Yousef's uncle, Khalid Sheikh Mohammed (KSM), was staying in the same guesthouse and was an on-the-scene witness to news media about the arrest. 25


Although a fugitive with a $25 million reward offered for his capture, he was interviewed by Lesley Stahl for CBS News' 60 Minutes on May 23, 2002. See Tina Kelley, Suspect in 1993 Bombing Says Trade Center Wast’s First Turger, N.Y. Times, June 1, 2002, at A10 (reporting that Yasin originally wanted to blow up Jewish neighborhoods in Brooklyn, but Yousef thought destroying the World Trade Center would be more effective). 26

Salameh, 152 F.3d at 108, see Tabor, supra note 6. 27

Salameh, 152 F.3d at 108, see Tabor, supra note 6.


33 United States v. Salameh, 992 F.2d 445, 446 (2d Cir. 1993), see Tabor, supra note 31.


35 See Blumenthal, supra note 3, Mitchell, supra note 20.


Ismoil was apprehended in Jordan on July 30. 26 Yasin, who was questioned but released by the FBI after the bombing, remains a fugitive. 27

Ajay was released from his six-month sentence on March 1. 28 On March 9, he was rearrested on an immigration detainer. 29

Saltameh and Ayyad were indicted in the Southern District of New York on March 17. 30 The district court assigned the case to Judge Kevin Thomas Duffy. 31 On March 31, a superseding indictment added Abouhalima and Yousef as defendants. 32 The next day, the court ordered the parties and their attorneys not to discuss publicly anything related to the case. 33 The court of appeals vacated this gag order as overbroad on April 30. 34

Bilal Akkaisi turned himself in on March 24, 35 and a second superseding indictment added him as a defendant on April 7. 36 Because evidence against him


Although a fugitive with a $25 million reward offered for his capture, he was interviewed by Lesley Stahl for CBS News' 60 Minutes on May 23, 2002. See Tina Kelley, Suspect in 1993 Bombing Says Trade Center Wast’s First Turger, N.Y. Times, June 1, 2002, at A10 (reporting that Yasin originally wanted to blow up Jewish neighborhoods in Brooklyn, but Yousef thought destroying the World Trade Center would be more effective). 26

Salameh, 152 F.3d at 108, see Tabor, supra note 6. 27

Salameh, 152 F.3d at 108, see Tabor, supra note 6.


33 United States v. Salameh, 992 F.2d 445, 446 (2d Cir. 1993), see Tabor, supra note 31.


35 See Blumenthal, supra note 3, Mitchell, supra note 20.

was weaker than evidence against the others, his prosecution was severed.\textsuperscript{37} On May 9, 1994, he pleaded guilty to an immigration violation and agreed to deportation.\textsuperscript{38} Judge Duffy sentenced him on July 13 to one year and eight months in prison, which was four months more than the time already served.\textsuperscript{39}

A third superseding indictment added Ajaj as a defendant on May 26, 1993.\textsuperscript{40} A fourth superseding indictment added the fugitive Yasin as a defendant on August 4.\textsuperscript{41} Salameh, Ayyad, Abouhalima, Ajaj, Yousef, and Yasin were named as defendants in a fifth superseding indictment filed on September 1.\textsuperscript{42}

Jury selection in the trial against Salameh, Ayyad, Abouhalima, and Ajaj began on September 14.\textsuperscript{43} The court issued 5,000 extra jury summonses to assemble a jury pool for the case.\textsuperscript{44} Opening arguments began on October 5.\textsuperscript{45} The jury began its deliberations on February 23, 1994, and convicted the defendants on March 4.\textsuperscript{46}

Between conviction and sentencing, the defendants dismissed their attorneys.\textsuperscript{47} Salameh, Abouhalima, and Ajaj sought to hire as sentencing attorneys the law firm representing other defendants in a related trial, which is described below.\textsuperscript{48}

\textsuperscript{37} See Bernstein, supra note 11, Mitchell, supra note 27, Tabor, supra note 16, Mary B. W. Tabor, Trade Center Defendant Agrees to a Plea Bargain, N.Y. Times, May 10, 1994, at B3 (hereinafter Plea Bargain).

\textsuperscript{38} A sixth superseding information against Alkaisi was filed on May 9, 1994. S.D.N.Y. Salameh Docket Sheet, supra note 26.

\textsuperscript{39} S.D.N.Y. Salameh Docket Sheet, supra note 26, see Tabor, Plea Bargain, supra note 37.

\textsuperscript{40} S.D.N.Y. Salameh Docket Sheet, supra note 26, see Ronald Sullivan, Bombing Figure Gets 20 Months for an Immigration Violation, N.Y. Times, July 14, 1994.

\textsuperscript{41} Alkaisi was released from prison on November 7, 1994. http://www.bop.gov (reg. no. 28065-054).

\textsuperscript{42} S.D.N.Y. Salameh Docket Sheet, supra note 26, see Mitchell, U.S. Widens Charges, supra note 11.


\textsuperscript{44} S.D.N.Y. Salameh Docket Sheet, supra note 26, see Ralph Blumenthal, Jury Selection Starts in World Trade Center Case, N.Y. Times, Sept. 15, 1993, at B1; Tabor, supra note 16.

\textsuperscript{45} Judge Duffy does not use jury questionnaires. United States v. Salameh, No. 1:93-cr-180, 1993 WL 364488, at *2 (S.D.N.Y. Sept. 15, 1993) ("There has been absolutely no showing that jury questionnaires are of any particular help in the selection of a jury in highly publicized cases where a searching voir dire is conducted."); see Gross, supra note 31, at 23-24.


\textsuperscript{50} Salameh, 152 F.3d at 161.


\textsuperscript{52} See Bernstein, supra note 31; Gross, supra note 31, at 11.

\textsuperscript{53} Salameh, 152 F.3d at 161, see Convictions Are Upheld in Trade Center Case, N.Y. Times, Aug. 5, 1998, at B6, Gross, supra note 31, at 11.

\textsuperscript{54} United States v. Salameh, 261 F.3d 271, 279 (2d Cir. 2001).

\textsuperscript{55} Id. (noting sentences of 1,403 months for Salameh, 1,300 months for Abouhalima, 1,405 months for Ayyad, and 1,378 months for Ajaj); S.D.N.Y. Salameh Docket Sheet, supra note 26 (same), see http://www.bop.gov (noting release dates of January 22, 2005, for Salameh, reg. no. 34338-054, September 20, 2007, for Mahmod Abouhalima, reg. no. 28064-054, April 3, 2005, for Ayyad, reg. no. 16917-050, and June 25, 2003, for Ajaj, reg. no. 40637-053), see also United States v. Tecoco, 135 F.3d 116, 131-32 (2d Cir. 1998) (approving a sentencing scheme by Judge Jack B. Weinstein of the Eastern District of New York).

\textsuperscript{56} Salameh, 261 F.3d 271, see Benjamin Wesner, Trade Center Bombing Terms, N.Y. Times, Aug. 7, 2001, at B4.

\textsuperscript{57} In re World Trade Center Bombing Litig., 17 N.Y.3d 428, 957 N.E.2d 733 (2011), see id. at 446, 957 N.E.2d at 744 ("We . . . hold that the Port Authority acted within its governmental capac-
Plots to Bomb New York Landmarks

When Salameh rented the van used to bomb the World Trade Center, he used as identification a New York driver’s license with an address belonging to Ibrahim el-Gabrówny. 58 On March 4, 1993, federal agents searched el-Gabrówny’s home, where they found stun guns and taped messages from el-Gabrówny’s cousin, El Sayyid Nosair, urging aggressive reactions to Jewish immigration to Israel. 59 Agents found el-Gabrówny near his home, and he was belligerent when frisked. 60 He was discovered to have fraudulent Nicaraguan passports for Nosair and Nosair’s family. 61

El-Gabrówny was indicted for assault in the Southern District of New York on March 17.62 The court assigned the case to Judge Michael B. Mukasey, 63 who tried to conduct this case as much like other criminal trials as possible. 64

64. Interview with Michael B. Mukasey, June 25, 2007.
66. Rahman, 189 F.3d at 105 & n.3, Rahman, 861 F. Supp. at 270, see Blumenthal, supra note 3; 67. Morano, supra note 56; 68. Nosair shot and was shot at the scene by Carlos Acosta, a postal police officer. Rahman, 189 F.3d at 105, see supra note 55, at 57, 81–83. Although Nosair was convicted of assault with a deadly weapon on Acosta, Nosair sued Acosta and the postal service for his own injury. Nosair v. Acosta, No. 1992-cv-2874, 1993 WL 336996 (S.D.N.Y. Sept. 1, 1993). His suit was dismissed as precluded by his conviction, id., and his appeal was dismissed as frivolous, Docket Sheet, Nosair v. Acosta, No. 93-2661 (2d Cir. Oct. 7, 1993).
67. Rahman, 189 F.3d at 104, 116, see Richard Bernstein, Biggest U.S. Terrorism Trial Begins as Arguments Clash, N.Y. Times, Jan. 31, 1995, at 1 (reporting that Salem was paid more than $1 million by the United States government for his assistance), Lance, supra note 5, at 209 (reporting that Salem was “going to get $1.5 million and a new life in the Witness Protection Program”), Alison Mitchell, Bomb Informer Active in 1991, Authorities Say, N.Y. Times, July 15, 1993, at A1 [hereinafter Bomb Informer], Alison Mitchell, Egyptian Was Informer, Officials Say, N.Y. Times, June 26, 1993, at B2 [hereinafter Egyptian Informer], Alison Mitchell, Official Recalls Delay in Using Informer, N.Y. Times, July 16, 1993, at B2 (reporting that Salem had entered the federal witness protection program), Mitchell, supra note 60 (describing Abdel Rahman as “blond, with one eye without a pupil, the other an empty socket”), see also Lance, supra note 5, at 8 (“Blinded shortly after birth, Nosair Abdel Rahman had resorted to the Koran by the age of eleven.”), Mary B. W. Tabor, Informer’s Ex-Wife Said He Warned of Terrorism, N.Y. Times, Sept. 28, 1993, at B2 (reporting that Salem “said that the day after the explosion [he] was upset and told [him] that the bombing could have been averted if the F.B.I. had heeded his warnings”).

Nor was in prison on a sentence of 7½ to 22 years for a state conviction on assault and weapons charges stemming from the killing of a “militant Zionist” and former member of the Israeli parliament, Rabbi Meir Kahane, at a November 5, 1990, speech that Kahane made in New York City. 66 There was evidence that projec- tects found in the room where Kahane and others were shots came from Nosair’s gun, but Nosair was acquitted of the murder. 66

In 1991, during Nosair’s state trial, an FBI informant, Emad Eldin Aly Abdou Salem, began to brief friends of Sheik Omar Abdel Rahman, a blind Islamic cleric. 66 Salem met el-Gabrówny at the trial of el-Gabrówny’s cousin Nosair. 68

Abdel Rahman was tried but acquitted in Egypt as an accomplice in the Octo-

ber 6, 1981, murder of President Anwar el-Sadat. 69 He illegally entered the United

States in 1990 and faced a deportation order at the time of the World Trade Center bombing. His followers plotted to assassinate Egypt’s president, Hosni Mubarak, during a March 1993 visit to the United Nations in New York City. Siddig Ibrahim Siddig Ali obtained Mubarak’s itinerary from a source in the Sudanese government. But the plot was foiled when a confidant of Abdel Rahman’s, Abu Mohammed Haggag, informed the Egyptian government of the assassination plan, and Mubarak’s New York trip was canceled.

Siddig Ali and Clement Rodney Hampton-El led paramilitary training on weekends between October 1992 and February 1993. Participants included Amir and Fadil Abdelgani and Tarig Elhassan, as well as the Egyptian informant Haggag. The training was for jihad, perhaps in Bosnia. Hampton-El was observed by the FBI in July 1989 shooting weapons at a public rifle range on Long Island with World Trade Center bombers Abuhamila, Salameh, and Ayyad.

In May 2003, the informant Salem persuaded Siddig Ali to establish a bomb-making safehouse where the FBI had installed surveillance equipment.

The conspirators considered bombing various New York City locations, including the United Nations, the federal building, the FBI headquarters, the diamond district, the Lincoln Tunnel, and the Holland Tunnel.


inspired the assassination of Sadat”), Ali H. Soufan, The Black Banners 47 (2011) ("he was acquitted but expelled from Egypt")

Abdel Rahman was subsequently tried for and acquitted of participating in a plot to overthrow the Egyptian government after el-Sadat’s death. See Egyptian Court Sentences 107 Muslim Militants in a 1981 Revolt, N.Y. Times, Oct. 1, 1984, at A6. He was later included in an arrest of 1,500 Muslim extremists, but he was freed several months later. See Alan Cowell, Castro Fires Fundamentalist Cleric: Pending Hearing on Role in Spyrie, N.Y. Times, Aug. 11, 1989, at A3; Alan Cowell, Egypt Seizes 1,500 in Crackdown on Fundamentalists, N.Y. Times, Apr. 27, 1989, at A3.

Abdel Rahman was convicted, but given a suspended sentence. See James C. McKinley, Jr., Islamic Leader on U.S. Terrorist List Is in Brooklyn, N.Y. Times, Dec. 16, 1990, at 144; McFadden, supra note 15, Mitchell, supra note 60, see also Soufan, supra note 69, at 47 (“The visa was given to him in Sudan by a CIA official.”).

According to the 9/11 Commission, “After it was discovered that Abdel Rahman, the Blind Sheikh, had come and gone almost at will, State initiated significant reforms to its watchlist and visa-processing policies.” The 9/11 Commission Report 95 (2004)


72. Rahman, 189 F.3d at 108.

73. Id.

74. Id. at 107.

75. Id.

76. Id.

77. Id. at 105, see Lance, supra note 5, at 47-49, 74.

78. Rahman, 189 F.3d at 109, see Lance, supra note 5, at 118, Mitchell, Egyptian Informer, supra note 67.


unsuccessfully tried to steal cars to use as both bomb-delivery and getaway vehicles. On June 22 and 23, Mohammed Saleh, who owned two gas stations in Yonkers, provided nearly $300 worth of diesel fuel to Siddig Ali and the Abdelgani’s to use for making bombs.

A couple of hours after midnight on June 24, 1993, the FBI raided the safehouse and arrested Siddig Ali, Amir and Fadil Abdelgani, Elhassan, and Alvarez while they were mixing explosive chemicals. Hampton-El, Saleh, and Khallafalla were arrested at their homes in Flatbush, Yonkers, and Jersey City, respectively.

It was reported that the government allowed Abdel Rahman to remain free pending his deportation appeal because he was not considered a flight risk and the conspiracy evidence against him was weak. But after his evaded federal agents following him on June 30, the government decided to arrest him on an immigration detainee. A negotiated surrender was agreed on for July 3.

On July 14, the indictment against el-Gabrowny was expanded to include bomb conspiracy charges and defendants Siddig Ali, Hampton-El, Amir Abdelgani, Khallafalla, Elhassan, Fadil Abdelgani, Saleh, Alvarez, and two others: Earl Gant and a defendant identified only as “Wahid.” Abdel Rahman, Nosair, Haggag, and Mohammed Abouhalima, the brother of World Trade Center bomber Mahmoud Abouhalima, were added as defendants by superseding indictment on August 25.

Gant, who was considered a minor player in the case, was arrested on July 1, 1993, and released on bail on October 19, he pleaded guilty on April 1, 1994.

80. Rahman, 189 F.3d at 110.
81. Id.; see McFadden, supra note 79.
82. Rahman, 189 F.3d at 110.
83. Id. at 111; see McFadden, supra note 79.
84. Rahman, 189 F.3d at 111; see McFadden, supra note 79.
86. See id.
87. See id.
88. Abdel Rahman was tried in absentia, convicted, and sentenced to seven years in prison in Egypt in 1993 and 1994 in a prosecution for illegal demonstrations and attempts to kill police officers during protests. See Bombing Defendants to Be Tried in Egypt, N.Y. Times, Oct. 22, 1993, at B3; Egyptian Court Sentences Absent Sheikh to Prison, N.Y. Times, Apr. 29, 1994, at B3.
90. Mitchell, Bomb Informer, supra note 67.
92. S.D.N.Y Abdel Rahman Docket Sheet, supra note 62, see Ralph Blumenthal, Defendant in a Bombing Plot Released on Bail, N.Y. Times, Oct. 19, 1993, at B2 (reporting that there was evidence that Gant agreed to obtain explosives but had no real awareness of what they would be used for); Mary B. W. Tabor, 5th Held in Bomb Plot as Tie Is Made to a 1991 Murder, N.Y. Times, July 1, 1993, at B3.
He was sentenced on July 20, 1994, to time served, with three years of supervised release.91

"Wahid" turned out to be Mataraw Ahmed Mohamed Said Saleh, who was arrested on July 22, 1993, and who is not related to codefendant Ahmed Mohamed Saleh.92 Because prosecutors determined that Wahid joined the conspiracy only hours before the government began arresting codefendants, he pleaded guilty and was sentenced on December 19, 1995, to time served, with three years of supervised release.93

Haggag agreed to testify for the government, terrorism charges against him were dropped, and he pleaded guilty to an unrelated insurance fraud scheme in which he tried to collect on a fire he set in a cafe he co-owned.94 The other defendants were tried for seditious conspiracy "to conduct a campaign of urban terrorism," including participation in the bombing of the World Trade Center, the murder of Rabbi Kahane, the plot to assassinate President Murarak, and plans to bomb New York landmarks.95

Famed defender of the unpopular William M. Kunstler and his partner, Ronald L. Kuby, represented el-Gabrowny.96 When the indictment was superseded to include Siddig Ali and others as defendants, Kunstler and Kuby appeared for both el-Gabrowny and Siddig Ali.97 Judge Mukasey sought to ensure that a conflict-of-interest waiver by the defendants was knowing.98

I said I would conduct a hearing at a later date to determine that both defendants understood their right to conflict-free representation, and that in aid of such a determination I would appoint whichever attorneys from the panel of Criminal Justice Act ("CJA") attorneys were scheduled to receive cases that week, for the purpose of advising each defendant of that right independent of any advice received from the Kunstler firm. Kunstler objected, stating immediately in open court, without consulting either defendant, that "[t]hey are perfectly willing to be represented here by me and they are here and they are willing to waive any alleged conflict of interest." (7/15/93 Tr. 17) He added that he did not want any CJA attorney "talking to either one of them." When I noted that neither defendant would be obligated to talk to independent counsel, but only to listen to an explanation of the risks of dual representation, Kunstler responded, "There are no risks here, Judge, except those created by the government." (Id. at 18)

Notwithstanding defense counsel's position, I appointed the two lawyers on duty to accept CJA appointment that day and a succeeding day to act as independent counsel to El-Gabrowny and Siddig Ali, to explain to them the hazards of joint representation.99 [Both defendants said they had understood the explanations of possible conflicts, and both expressed the desire to be represented by the Kunstler firm.100

When the indictment was superseded to include as defendants Nosair, Abdel Rahman, and two others, attorney Michael Warren appeared for Nosair, and another attorney appeared for Abdel Rahman.101

Warren and Kunstler represented Nosair at his state murder trial, and Warren appeared for el-Gabrowny at el-Gabrowny's first appearance following the filing of a criminal complaint and preceding the filing of the indictment.102 Judge Mukasey denied Nosair's application to name Warren as his appointed attorney in this federal trial as an exception to regular Criminal Justice Act procedures.103 Judge Mukasey assigned Nosair a CJA panel attorney.104

91. S.D.N.Y. Abdel Rahman Docket Sheet, supra note 62, see Ronald Sullivan, Minor Figure in Bomb Plot Sentenced to Time Served, N.Y. Times, July 21, 1994, at B4 (reporting that Gant said he thought the explosives he was providing would be used to combat the rape and massacre of Muslims in Bosnia).
93. S.D.N.Y. Abdel Rahman Docket Sheet, supra note 62, see Fried, supra note 92.
96. Judge Mukasey denied Nosair's motion to dismiss some counts against him as double jeopardy because of his prior prosecution in state court for crimes related to the murder of Rabbi Kahane. United States v. Nosair, 854 F. Supp. 251 (S.D.N.Y. 1994). Judge Mukasey also ruled that although participation in the Kahane murder was a triple offense, it could not be prosecuted as part of seditious conspiracy, because Kahane was a private foreign citizen. Rahman, 834 F. Supp. at 258-61.
Abdel Rahman’s attorney announced that he and Abdel Rahman could not agree on a fee; Kunstler and Kuby informed the court that they had accepted Abdel Rahman’s request that they represent him instead.104 The government moved to disqualify the Kunstler firm from representing more than one defendant.105 On November 9, 1993, Judge Mukasey ruled that the firm could either represent el-Gabroney and Siddig Ali, as they had, or Abdel Rahman, but not all three.106 Abdel Rahman opted to represent himself, and the court appointed a panel attorney to assist him.107 By the time the trial commenced, he was represented by Lynne Stewart108 who had represented Aja at Aja’s arraignment in the bombing case.109

On February 8, 1994, Mohammed Abouhalima was released in a sealed proceeding.110 But he was indicted on September 18, 1996, for aiding his brother’s escape.111 He was convicted on May 28, 1997, and sentenced on November 24, 1998, to eight years in prison.112

In June 1994, Siddig Ali obtained substitute counsel to help him try to cooperate with the government, but the government decided in August not to strike a deal.113 The substitute counsel asked to be relieved as Siddig Ali’s attorney, because his knowledge of Siddig Ali’s proffers to the government would constrain


107 Rahman, 837 F. Supp. at 65, 72, see id. at 71 (noting that the court would appoint standby counsel “to conduct cross-examination of any former client of the Kunstler firm who takes the stand at trial, so as to minimize the risk that that client’s privileged communications to the Kunstler firm will influence the cross-examination”), Rahman, 861 F. Supp. at 271 (noting ruling), see also Ralph Blumenthal, Judge Rules That Sheik and Two Other Defendants Cannot Share Lawyer, N.Y. Times, Nov. 11, 1993, at B3.


109 See Bernstein, supra note 67.

110 See Tahor, supra note 6.


116 Id. at 267–68.

117 Id. at 268, 276, 279.


Public attention to this trial was diminished somewhat by the coincident criminal trial of O.J. Simpson for the murder of his wife and her friend. Interview with Michael B. Mukasey, June 25, 2007, see Simpson Case Timeline, L.A. Times, Oct. 3, 1995, at 3 (noting that jury selection in the Simpson trial began on Sept. 26, 1994, opening statements began on Jan. 24, 1995, and the not guilty verdict was announced on Oct. 3, 1995).

Interview with Michael B. Mukasey, United States v. Abdel Rahman: Jury Questionnaire (Jan. 9, 1995), Interview with Michael B. Mukasey, June 22, 2007.

Judge Mukasey has pointed out that a good jury questionnaire should serve to weed out two types of jurors: those who cannot reasonably meet the time commitment for such a trial and those who cannot be impartial knowing all the publicity about the trial or having bias against certain people.

Gross, supra note 31, at 22–23.

122 Interview with Michael B. Mukasey, June 25, 2007.

123 S.D.N.Y. Abdel Rahman Docket Sheet, supra note 62, see Bernstein, supra note 67.


Opening statements commenced on January 30.125 Judge Mukasey found it helpful—necessary even—to charge the jury with applicable law at the beginning of the case, between opening statements and presentation of evidence.122 For example, it was important for the jury to understand up front that seditious conspira-
cy did not necessarily include an intent to overthrow the government.\textsuperscript{125} As was his general practice, Judge Mukasey permitted jurors to take notes.\textsuperscript{126} On February 6, Siddig Ali pleaded guilty, agreed to be a witness for the government, and asked God to forgive him for his acts, which he admitted were wrong.\textsuperscript{127} He was sentenced to 11 years in prison on October 15, 1999, on a finding that he provided the government with extensive assistance in the case.\textsuperscript{128}

Judge Mukasey conducted the nine-month trial four days per week.\textsuperscript{129} A brief experience with five days per week fatigued all participants without moving things along noticeably faster.\textsuperscript{130} Both Arabic and Spanish interpreters were required.\textsuperscript{131}

While the trial was in progress, on April 19, 1995, the federal building in Oklahoma City, including the courthouse, was partially destroyed by a bomb. Judge Mukasey permitted the jurors to consult news of the event, but admonished them not to let it influence them in the trial.\textsuperscript{133}

On October 1, 1995, the jury convicted el-Gabrowny, Hampton-El, both Abdelgani, Khalilallah, Elhassan, Saleh, Alvarez, Abdel Rahman, and Nosair of seditionary conspiracy and other charges, including a guilty verdict for Nosair in Rabbi Kahane’s murder.\textsuperscript{134} On January 17, 1996, Judge Mukasey sentenced Abdel Rahman and Nosair to life in prison and sentenced the other eight defendants as follows: el-Gabrowny to 57 years; Alvarez, Elhassan, Hampton-El, and Saleh to 35 years; Amir Abdelgani and Khalilallah to 30 years; and Fadil Abdelgani to 25 years.\textsuperscript{135}

\textsuperscript{125} Interview with Michael B. Mukasey, June 25, 2007.

\textsuperscript{126} Id.


\textsuperscript{130} Interview with Michael B. Mukasey, June 25, 2007.

\textsuperscript{131} Id.


\textsuperscript{135} Hampton-El, Fadil Abdelgani, Elhassan, and Alvarez testified at trial; the others did not. Michael B. Mukasey, United States v. Abdel Rahman: Jury Instructions (Sept. 29, 1995).

\textsuperscript{136} S.D.N.Y. Abdel Rahman Docket Sheet, supra note 62; see Joseph P. Fried, Shock Sentenced to Life in Prison on Bombing Plot, \textit{N.Y. Times}, Jan. 18, 1996, at 1; Wren, supra note 3; see also http://www.bop.gov (noting life sentences for Abdel Rahman, reg. no. 34892-054, and Nosair, reg. no. 35074-054, and noting release dates of April 22, 2025, for Alvarez, reg. no. 34848-054, December 21, 2023, for Elhassan, reg. no. 34892-054, December 21, 2023, for Hampton-El, reg. no. 34854-054, March 24, 2024, for Saleh, reg. no. 34853-054, October 11, 2019, for

On August 16, 1999, the court of appeals affirmed the convictions and largely affirmed the sentences, remanding for a reconsideration of el-Gabrowny’s sentence.\textsuperscript{137} On remand, Judge Mukasey sentenced el-Gabrowny to 33 years,\textsuperscript{138} which the court of appeals affirmed.\textsuperscript{139}

A Plot to Bomb Airplanes

In the summer of 1994, Yusuf moved to Manila, Philippines.\textsuperscript{139} There, he launched a conspiracy to bomb U.S. airliners serving routes in southeast Asia. To test their methods, Yusuf and Wali Khan Amin Shah bombed a Manila movie theater on December 1, 1994, injuring several moviegoers.\textsuperscript{140} In December, Yusuf planted a nitroglycerine bomb under a passenger seat during the first leg of a Philippine Airlines flight from Manila to Tokyo.\textsuperscript{141} Yusuf exited the plane during a stopover in Cebu, Philippines, and the bomb exploded during the second leg, killing one passenger and injuring several others.\textsuperscript{142}

Amir Abdelgani, reg. no. 34850-054, October 10, 2019, for Khalilallah, reg. no. 34856-054, and April 5, 2015, for Fadil Abdelgani, reg. no. 34849-054.


138 United States v. Elgabrowny, 10 F. App’x 23 (2d Cir. 2001).


140 The 9/11 Commission Report 147 (2004) (noting that the plan became known as the “Bojinka” plot). Yusuf, 327 F.3d at 79-80; see Lance, supra note 5, at 150-36, id. at 181 (“They planned to execute the Bojinka plot right after assassinating the Holy Father, during the week of January 12.”); Dina Temple-Raston, The Jihad Next Door: The Lackawanna Six and Rough Justice in the Age of Terror 24 (2007) (reporting that the plan was to use liquid explosives that would pass through airport metal detectors), see also McDermott & Meyer, supra note 5, at 66 (noting that bojinka is Serbo-Croatian for big noise).

Using nothing more exotic or complicated than airline timetables, they devised a scheme whereby five men could in a single day board twelve flights—one for each of the three men, three each for the other two—assemble and depart their bombs, exit the planes with the timers set to ignite the bombs up to several days ahead, allowing the men to be far away and far from reasonable suspicion by the time they exploded.

McDermott, supra note 9, at 148.

141. The 9/11 Commission Report 147 (2004), Yusuf, 327 F.3d at 79, 81, see Lance, supra note 5, at 152 (describing the injuries at issue), McDermott, supra note 9, at 147, McDermott & Meyer, supra note 5, at 67, Wren, supra note 3.


143. Yusuf, 327 F.3d at 79, 81, Yusuf, 927 F. Supp. 675, see Lance, supra note 5, at 154-55, McDermott, supra note 9, at 148-49, McDermott & Meyer, supra note 5, at 67 (“the pilots heroically managed to land [the plane] with a gaping hole in its fuselage”), McIntyre, supra note 23, Wren, supra note 3.

National Security Case Management Studies (06 23 2013) 19
Yousef and his high school friend, Abdul Hakim Murad, were burning off excess chemicals in their Manila apartment on January 6, 1995, and they accidentally started a fire that resulted in a visit from Philippine police officers and discovery of the plot to bomb planes.\textsuperscript{144}

Philippine authorities arrested Murad on January 7, and he was transported to the Southern District of New York on April 12.\textsuperscript{145} While on route, he confessed that the goal of the bombing plot was to punish the United States and its people for their support of Israel.\textsuperscript{146}

Philippine authorities arrested Shah on January 11, but he escaped.\textsuperscript{147} He was recaptured by Malaysian authorities in December and flown to New York on December 12.\textsuperscript{148}

Yousef fled the Philippines but was turned in by an accomplice to authorities in Islamabad, Pakistan, on February 7, 1995.\textsuperscript{149} He was transported to the Southern District of New York on February 8.\textsuperscript{150} En route, he confessed to an intention to topple one of the World Trade Center towers into the other.\textsuperscript{151}

A jury trial against Yousef, Murad, and Shah for conspiracy to bomb airliners began with jury selection on May 13, 1996.\textsuperscript{152} Yousef asked to address the jury during opening arguments, and Judge Duffy said that if he did he would have to act as his own lawyer throughout the trial.\textsuperscript{153} Yousef and Judge Duffy agreed that he would do this.\textsuperscript{154} All three defendants were convicted on September 5, the fourth day of deliberation.\textsuperscript{155}

A jury trial against Yousef and Ismoil for involvement in the bombing of the World Trade Center began with jury selection on July 15, 1997.\textsuperscript{156} This time, Yousef let a lawyer represent him.\textsuperscript{157} Both were convicted on November 12.\textsuperscript{158}

Judge Duffy sentenced Yousef on January 8, 1998, to 240 years in prison for his participation in the World Trade Center bombing and a consecutive life sentence for his participation in the plot to bomb airliners.\textsuperscript{159} At his sentencing, Yousef proclaimed, “I am a terrorist and I am proud of it.”\textsuperscript{160} Judge Duffy sentenced Ismoil on April 3, 1998, to 240 years in prison, and the judge sentenced him to May 15, 1998, to life plus 60 years.\textsuperscript{161} The court of appeals affirmed the convictions and sentences on April 4, 2003.\textsuperscript{162} On October 8, 2004, Judge Duffy sentenced Shah to 30 years.\textsuperscript{163}

\textsuperscript{144} Yousef, 327 F.3d at 79, 81; see Lance, supra note 5, at 178–80; McDermott & Meyer, supra note 5, at 68 (describing Yousef as ever careless), McKinley, supra note 23, Philip Sharton, Broad Terror Campaign Is Foiled by Fire in Kitchen, Officials Say, N.Y. Times, Feb. 12, 1995, at 1; Temple-Raston, supra note 140, at 24, Wren, supra note 3; see also McDermott, supra note 9, at 146, 152–54 (reporting that the apartment was selected because it was on the route of a planned papal procession).

\textsuperscript{145} Yousef, 327 F.3d at 79, 81, United States v Yousef, 925 F. Supp. 1069 (S.D.N.Y. 1996), see McKinley, supra note 23.

\textsuperscript{146} Yousef, 327 F.3d at 83.

\textsuperscript{147} Id. at 79, 82, see Lance, supra note 5, at 227; James C. McKinley, Jr., F.B.I. Arrests Man in Far East, Charged in Plot to Bomb Planes, N.Y. Times, Dec. 13, 1995, at 5.

\textsuperscript{148} Yousef, 327 F.3d at 79, 82; see Lance, supra note 5, at 227; McKinley, supra note 147.


\textsuperscript{150} Yousef, 327 F.3d at 82; Yousef, 925 F. Supp. at 1065, see S.D.N.Y. Salamch Docket Sheet, supra note 26 (noting Yousef’s “not guilty plea on Feb 9, 1995), see also Johnston, supra note 23, Wren, supra note 3.

\textsuperscript{151} See McDermott & Meyer, supra note 5, at 78–79; Benjamin Weiner, Suspect’s Confession Cited as Bombing Trial Opens, N.Y. Times, Aug. 6, 1997, at B6.

\textsuperscript{152} Yousef, 327 F.3d at 85 (giving the start date as May 29, which was the day of opening arguments), S.D.N.Y. Salamch Docket Sheet, supra note 26 (also noting the filing on Apr. 13, 1995, of an eighth superseding indictment against Yousef, Yasin, and Murad, the filing on June 14, 1995, of a ninth superseding indictment against Yousef, Yasin, and Murad, the filing on Sept. 11, 1995, of a tenth superseding indictment against Yousef, Yasin, Murad, and Ismoil, the filing on Dec. 13, 1995, of eleventh superseding indictments against Yousef, Yasin, Murad, Ismoil, and Shah, and the filing on Feb. 21, 1996, of twelfth superseding indictments against Yousef, Yasin, Murad, Ismoil, and Shah), see Judge Dismisses 75 on Bomb Jury Panel, N.Y. Times, May 14, 1996, at 2 (hereinafter Judge Dismisses 75); Lance, supra note 5, at 227; McDermott & Meyer, supra note 5, at 108–10 (reporting that Yousef’s trial for the airplane plot occurred before his trial for the World Trade Center bombing so that a delay in the airplane trial would not make it more difficult to get testimony from witnesses in the Philippines).

\textsuperscript{153} See Gross, supra note 31, at 5; Christopher S. Wren, Plot of Terror in the Skies Is Outlined by a Prosecutor, N.Y. Times, May 30, 1996, at 3.


\textsuperscript{155} Yousef, 327 F.3d at 85; see Wren, supra note 3.

\textsuperscript{156} Yousef, 327 F.3d at 77–78, 80, S.D.N.Y. Salamch Docket Sheet, supra note 26, see Jury Selection Begins in Trade Center Trial, N.Y. Times, July 16, 1997, at B2.

\textsuperscript{157} See Bomb Suspect to Use Lawyer at 2d Trial, N.Y. Times, Dec. 6, 1996, at 3 (hereinafter Suspect to Use Lawyer).


\textsuperscript{159} Yousef, 327 F.3d at 80, 135, S.D.N.Y. Salamch Docket Sheet, supra note 26; see Benjamin Weisser, "Mastermind Gets Life for Bombing of Trade Center," N.Y. Times, Jan. 9, 1998, at A1; see also http://www.bop.gov (noting a life sentence for Yousef, reg. no. 03911-000).

\textsuperscript{160} The court of appeals denied Yousef’s appeal of the district court’s decision not to appoint habeas corpus counsel under the Criminal Justice Act. United States v. Yousef, 395 F.3d 76 (2d Cir. 2005).

\textsuperscript{161} See Lance, supra note 5, at 284; McDermott & Meyer, supra note 5, at 113; Weisser, supra note 159.

\textsuperscript{162} Yousef, 327 F.3d at 80, 85, 135, S.D.N.Y. Salamch Docket Sheet, supra note 26; see Plot Is Given Life Term for Bombing Plot, N.Y. Times, May 16, 1998, at B5; Benjamin Weisser, Driver Gets 240 Years in Prison for Bombing of Trade Center, N.Y. Times, Apr. 5, 1998, at B2, see also http://www.bop.gov (noting a release date of August 29, 2204, for Ismoil, reg. no. 37802-054, and a life sentence for Murad, reg. no. 37407-054).

\textsuperscript{163} Yousef, 327 F.3d 56; see Benjamin Weisser, Judges Uphold Convictions in ‘93 Bombing, N.Y. Times, Apr. 5, 2003, at D3.

The appeal was heard by Second Circuit Judges Ralph K. Winter, Jr., John Walker, Jr., and José A. Cabranes. Because, by chance, all three judges sat in New Haven, Connecticut, oral argument was held there. Interview with Hon. José A. Cabranes, Nov. 4, 2009. Second Circuit oral
2001 Destruction of the World Trade Center

On June 5, 2008, during the presidency of George W. Bush, five men were arraigned in military tribunals at Guantánamo Bay for the September 11, 2001, attacks: KSM, Mustafa Ahmed al-Hawsawi, Ramzi bin al-Shibh, Walid bin Attash, and Ali Abdul Aziz Ali. ^164^ Eric H. Holder, President Obama’s attorney general, announced on November 13, 2009, that the men would be tried in the Southern District of New York instead. ^165^ Their sealed December 14 indictment was added to the indictment for the 1993 World Trade Center bombing. ^166^ Magistrate Judge James C. Francis IV granted the government’s request to both seal the indictment and keep it off the case’s docket. ^185^ According to the government, knowledge of the specific date the Superseding Indictment was returned may lead the defendants to coordinate with each other in ways that undermine both their security and the security of others. In addition, notice that new charges have been filed against the defendants may lead them to destroy evidence they now possess. ^169^ The defense appropriation act for 2011, however, forbade the use of defense funds to transfer KSM or any other Guantánamo Bay detainee for prosecution in a civilian court, ^169^ so the government obtained a dismissal of the superseding indictment in favor of renewed military tribunal prosecutions. ^170^

Arguments are almost always held in New York. Interview with 2d Ctr. Clerk’s Office Staff, Nov. 6, 2009.


The unsealing of an indictment against KSM was earlier announced at the 1998 sentencing of his nephew Yousef. See Lance, supra note 5, at 283-85, McDermott & Meyer, supra note 5, at 136, Wesser, supra note 159. A sealed indictment against KSM was returned in January 1996. See McDermott, supra note 9, at 165.


---

Challenges: Interpreters

These prosecutions required both Arabic and Spanish interpreters. ^171^

Challenges: Court Security

Security was tight in these trials. One downside of tight security in a criminal prosecution is the message it sends to the jury that the defendants might be dangerous. In the trial for conspiracy to bomb airplanes, Judge Duffy had to dismiss the first 75 prospective jurors because they indicated they would be influenced by heavy court security. ^172^

Challenges: Pro Se Defendants

Perhaps arising from ideological hostility to U.S. institutions, terrorism defend- ants sometimes elect to appear pro se. Sometimes defendants appear pro se because of irreconcilable conflicts with assigned counsel. After their convictions, Salameh, Ayyad, Mahmoud Abouhalima, and Ajaj dismissed their attorneys, and they appeared pro se for sentencing. ^173^ In response to Judge Mukasey’s determination that Kunstler’s law firm could represent either el-Gabrowny and Siddig Ali or Abdel Rahman, but not all three, Abdel Rahman elected to represent himself for a time. ^174^ Abdel Rahman had been successful defending himself pro se in Egypt on conspiracy charges in connection with the 1981 assassination of Egyptian President Anwar Sadat and thus thought he could duplicate those results, Abdel Rahman also wanted to use the trial as a platform from which to convey his views. Ultimately, Abdel Rahman’s close circle of people around him convinced him that he would have little chance of prevailing if he continued through trial pro se and convinced him to accept counsel. ^175^ At Yousef’s first trial, for the plot to bomb airplanes, he appeared pro se so that he could address the jury during opening arguments. ^176^ He was convicted, and he opted for counsel representation at his second trial, for participation in the first bombing of the World Trade Center. ^177^

Challenges: Jury Security

Both Judge Duffy and Judge Mukasey used anonymous juries for the jurors’ protection. ^178^

---

^171^ Interview with Michael B. Mukasey, June 25, 2007.

^172^ See Judge Joorjooosis 75, supra note 152.


^175^ Judge Mukasey told Abdel Rahman that if he behaved improperly, appointed counsel would take over. Interview with Michael B. Mukasey, June 25, 2007.

^176^ Gross, supra note 31, at 4 (reporting on an interview with Judge Mukasey, footnote omitted).

^177^ See id. at 5.

^178^ See Suspect to Use Lawyer, supra note 157.

^179^ Michael B. Mukasey, United States v. Abdel Rahman: Preliminary Voir Dire (Jan. 9, 1995) [hereinafter Mukasey Preliminary Voir Dire], Behind Closed Doors: Secret Justice in Amer-
This process becomes necessary in high-profile cases to protect the security of jurors. The confidential information in that case, mercifully, is something that even the court, and in a sense, the judge, is unaware of. The clerk knows the names of the jurors, the judge and the parties do not. The court tries at all costs to keep that information secret.179

To protect the jurors’ safety and anonymity, they did not report directly to the courthouse but to secret locations from which deputy marshals transported them to court.180

In Judge Mukasey’s case, “the identities of at least two of the jurors became known to some reporters after the case was over. As a result, those reporters camped outside the jurors’ doors to discuss the jury’s deliberations.”181 When an alternate juror’s anonymity became at risk in the last trial, Judge Duffy dismissed the juror.182

Because of the anticipated lengths of the trials, Judge Duffy decided not to sequester the juries.183 Judge Mukasey did not sequester the jurors during his trial until it was time to deliberate, at which time he moved to a seven-days-per-week schedule.184

Both Judge Duffy and Judge Mukasey sought to provide the jurors with extra comforts, such as meals and beverages.185

**Challenge: Classified Evidence**

In the seditious conspiracy trial, the government presented six classified exhibits ex parte to Judge Mukasey, pursuant to the Classified Information Procedures Act (CIPA).186 Judge Mukasey kept the exhibits in a safe while he considered whether

---

179. *Behind Closed Doors*, supra note 178, at 10 (remarks by Judge Mukasey).
180. Mukasey Preliminary Voir Dire, supra note 178, at 10 (remarks by Judge Mukasey).
183. Interview with Meghan Silhan, law clerk to Hon. Kevin Thomas Duffy, July 23, 2007, see Bernsten, supra note 11, Tabor, supra note 44.
184. Interview with Michael B. Mukasey, June 25, 2007

---

Kenya and Tanzania

Bombs exploded outside the United States embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania, on August 7, 1998, killing 224 people, including 12 Americans. Eleven non-American deaths occurred in Tanzania; the other deaths occurred in Kenya.

Nairobi
Pakistan authorities arrested Mohammed Saddiq Odeh on the day of the bombings for traveling with a fraudulent passport, and he quickly became a suspect.

190. An appeal was heard by Second Circuit Judges Wolfinbarger, Newman, and Joseph A. Cabranes for this report, on November 4, 2009, Tim Reagan interviewed Judge Newman in Judge Newman’s Hartford chambers, and Judge Cabranes and his law clerk Matt McKenzie in Judge Cabranes’s New Haven chambers.


The leadership decided that the attacks would occur on Friday, August 7, 1998, at 10:30 a.m., the time of day when Muslims are meant to be in the mosque at prayer. Therefore, al-Qaeda’s theologues argued, anyone killed in the bombing could not be a real Muslim, as he wasn’t at prayer, and so his death would be an acceptable consequence.

Soufan, supra, at 78.


193. Hundreds more would have been killed and hurt but for the extraordinary luck of there having been a filled water truck parked at just that moment in front of the Dar es Salaam embassy.” McDermott, supra note 191, at 177.

194. In re Terrorist Bombings of U.S. Embassies in Africa, 552 F.3d 177, 185 (2d Cir. 2008); In re Terrorist Bombings, 552 F.3d at 104; United States v. Bin Laden, 132 F. Supp. 2d 185; 207 (2001); see Raymond Bonner, Pakistan Arrests Two New Suspects in Embassy Blasts, N.Y. Times, Aug. 19, 1998, at A1; Bonner, supra note 192; Soufan, supra note 191, at 88 (“Pakistan authorities had noticed that the picture on his passport was fraudulent”).

195. In re Terrorist Bombings, 552 F.3d at 185 (noting that one week after detention in Pakistan, Odeh was transferred to Kenyan authorities); see David Johnston, U.S. Says Suspect Does Not Admit Role in Bombings or Ties to Saudi, N.Y. Times, Aug. 18, 1998, at A7.


197. See Johnston, supra note 195, and see In re Terrorist Bombings, 552 F.3d at 182 (noting that al-Owhali’s cooperation was contingent on his being tried in the United States, which he regarded as his enemy, instead of in Kenya, which he did not).


formation leading to his arrest, but he has not been apprehended. In 2009, Saleh Ali Saleh Nabhan, who is believed to be also responsible for the 2002 bombing of an Israeli hotel on the Kenyan coast, was killed in Somalia in a helicopter raid on Al-Shabab.

On September 16, Wadud el-Hage, a naturalized U.S. citizen and resident of Arlington, Texas, who once shared a house with Fazil in Nairobi and who once was Osama Bin Laden’s personal secretary, was arrested immediately after testifying before a grand jury. El-Hage, who also testified before a grand jury about Bin Laden’s activities a year earlier, was charged with making false statements to investigators and the grand jury. On October 7, charges against him were broadened to include conspiracy to kill American citizens.

The U.S. District Court for the Southern District of New York assigned the case to Judge Leonard B. Sand.

On October 24, 2000, el-Hage tried to plead guilty, but the court did not accept his plea, because Judge Sand determined that el-Hage was pleading guilty to avoid the strip searches required every time he came to court rather than because he believed he was guilty.

Dar es Salaam

On September 21, 1998, the government of Tanzania charged Mustafa Mahmoud Said Ahmed and Rashid Saleh Hemed with the bombing of the American embassy in Dar es Salaam. Tanzania dropped charges against Ahmed in March 2004. After a four-year trial, Tanzania’s High Court ruled in 2004 that the evidence did not support a conviction against Hemed.

Khafan Khamis Mohamed was arrested in Cape Town, South Africa, on October 5, 1999, flown to New York, and arraigned on October 8 for participation in the Dar es Salaam bombing. His attorney admitted at trial that K.K. Mohamed helped assemble the bomb. The United States decided to seek the death penalty against him.

South Africa’s Constitutional Court, its highest court, subsequently ruled that it was improper to turn Mohamed over to the United States for a capital trial. Judge Sand ruled that the decision by the South African court did

208. S.D.N.Y. El Hage Docket Sheet, supra note 204, see Benjamin Weiser, Judge Rejects Guilty Plea in Bomb Plot, N.Y Times, Oct 25, 2000, at B1

209. See Bronner, supra note 192, see also James Risen & Benjamin Weiser, Before Bombings, Omens and Fears, N.Y. Times, Jan 9, 1999, at A1 (reporting that in 1997 Ahmed warned the American embassy in Kenya of a bomb plot)


213. United States v. Bin Laden, 156 F. Supp. 2d 359, 362 (S.D.N.Y. 2001) He used fraudulent documents and a false name to request political asylum, and he was arrested when the fraud was discovered. Id.

214. See Hirsch, supra note 191, at 69, 81 (reporting also that Mohamed was known as “K.K.”), Benjamin Weiser, Suspect Admits Helping Make Embassy Bomb, N.Y. Times Feb 6, 2001, at A1 (reporting that Mohamed’s attorney made the concession during opening arguments), see also Bin Laden, 156 F. Supp. 2d at 362-63 (“During interrogations by American officials on October 5 and 6, 1999, Khalfan Mohamed admitted to playing a role in the August 7, 1998, bombing of the American Embassy in Dar es Salaam.”)

215. See Hirsch, supra note 191, at 71, 83, 99 (reporting also that Mohamed was known as “K.K.”), Benjamin Weiser, Suspect Admits Helping Make Embassy Bomb, N.Y. Times Feb 6, 2001, at A1 (reporting that Mohamed’s attorney made the concession during opening arguments), see also Bin Laden, 156 F. Supp. 2d at 362-63 (“During interrogations by American officials on October 5 and 6, 1999, Khalfan Mohamed admitted to playing a role in the August 7, 1998, bombing of the American Embassy in Dar es Salaam.”)

216. United States v. Bin Laden, 126 F. Supp. 2d 239 (S.D.N.Y. 2000) (denying a claim that the death penalty certification was race-based), see Weiser, Faking Illness, supra note 199, Weiser, 2d Death Penalty, supra note 199

217. Bin Laden, 156 F. Supp. 2d at 361 & n.1; see Hirsch, supra note 191, at 228, Benjamin Weiser, South Africa Regrets Its Role in a Defendant’s Extradition, N.Y Times, May 31, 2001, at B4 (reporting that the May 28, 2001, ruling “came too late to do Mr. Mohamed any good”)

208. S.D.N.Y. El Hage Docket Sheet, supra note 204, see Benjamin Weiser, Judge Rejects Guilty Plea in Bomb Plot, N.Y Times, Oct 25, 2000, at B1

209. See Bronner, supra note 192, see also James Risen & Benjamin Weiser, Before Bombings, Omens and Fears, N.Y. Times, Jan 9, 1999, at A1 (reporting that in 1997 Ahmed warned the American embassy in Kenya of a bomb plot)


213. United States v. Bin Laden, 156 F. Supp. 2d 359, 362 (S.D.N.Y. 2001) He used fraudulent documents and a false name to request political asylum, and he was arrested when the fraud was discovered. Id.

214. See Hirsch, supra note 191, at 69, 81 (reporting also that Mohamed was known as “K.K.”), Benjamin Weiser, Suspect Admits Helping Make Embassy Bomb, N.Y. Times Feb 6, 2001, at A1 (reporting that Mohamed’s attorney made the concession during opening arguments), see also Bin Laden, 156 F. Supp. 2d at 362-63 (“During interrogations by American officials on October 5 and 6, 1999, Khalfan Mohamed admitted to playing a role in the August 7, 1998, bombing of the American Embassy in Dar es Salaam.”)

215. See Hirsch, supra note 191, at 71, 83, 99 (reporting also that Mohamed was known as “K.K.”), Benjamin Weiser, Suspect Admits Helping Make Embassy Bomb, N.Y. Times Feb 6, 2001, at A1 (reporting that Mohamed’s attorney made the concession during opening arguments), see also Bin Laden, 156 F. Supp. 2d at 362-63 (“During interrogations by American officials on October 5 and 6, 1999, Khalfan Mohamed admitted to playing a role in the August 7, 1998, bombing of the American Embassy in Dar es Salaam.”)

216. United States v. Bin Laden, 126 F. Supp. 2d 239 (S.D.N.Y. 2000) (denying a claim that the death penalty certification was race-based), see Weiser, Faking Illness, supra note 199, Weiser, 2d Death Penalty, supra note 199

217. Bin Laden, 156 F. Supp. 2d at 361 & n.1; see Hirsch, supra note 191, at 228, Benjamin Weiser, South Africa Regrets Its Role in a Defendant’s Extradition, N.Y Times, May 31, 2001, at B4 (reporting that the May 28, 2001, ruling “came too late to do Mr. Mohamed any good”)
not invalidate Mohamed’s capital prosecution, but Mohamed could offer the decision as mitigating evidence.226

A Larger Plot

Osama Bin Laden was included in a November 4, 1998, superseding indictment,227 but he remained a fugitive until his killing by U.S. forces in 2011.228 Fazul Abdullah Mohammed came to be regarded as the bombings’ mastermind, and he was killed in a firefight in 2011 when he mistakenly came upon a security checkpoint in Mogadishu, Somalia, and tried to flee.229

Mamdouh Mahmoud Salim, Osama Bin Laden’s finance manager, was suspected of organizing the embassy bombings and was arrested in Munich, Germany, on September 16, 1998.220 German authorities handed him over to the U.S. government on December 20 on condition that he not face the death penalty.221 He first appeared before the district court on December 21.222 The government charged him with four broad conspiracy counts.223

Khalid al-Fawwaz, who was reportedly a close friend of Osama Bin Laden’s and who ran Al-Qaeda’s media operations, was arrested by British authorities in September 1998.224 On June 19, 1999, the U.S. government indicted him for having a hand in the 1998 bombings.225 At the United States’ request, British authorities also arrested Ibrahim Hussein Eidarous and Adel Mohammed Abdal Bary on July 11, 1999.226 Britain’s House of Lords ruled on December 17, 2001, that these three suspects could be extradited to the United States.227 Eidarous died of leukemia on July 16, 2008, while under house arrest in London.228 On April 10, 2012, the European Court of Human Rights approved the extradition of al-Fawwaz and Bary.229 The men were flown to New York on October 5.230

Ali A. Mohamed—a former sergeant in the U.S. Army who previously was a major in Egypt’s army and then a CIA asset—was secretly arrested with Al-Qaeda conspiracies in September 1998.231 He was formally indicted on May 19, 1999, after he refused to cooperate in the tracking down of Osama Bin Laden, and


225 See Jacobs, supra note 224.

226 See David Rohde, U.S. Says It Has Fingerprints of Embassy Bombing Suspects, N.Y. Times, July 13, 1999, at A6, Whitlock, supra note 224; see also Soufan, supra note 191, at 98 (“Although we had urged the British to arrest Fawwaz, Bary, and Eidarous in 1996, they had refused.”).


he first appeared in court on May 27. On October 20, 2000, he agreed to plead guilty. He is held in a secret location, and he has never been sentenced. Mohammed Suliman al-Naffi was lured from his home in Sudan and apprehended in Kenya in late 2000 by the United States. He was held in secret for more than four months before charges against him were made public. In early 2003, he pleaded guilty and was sentenced to ten years and one month in prison.

Among the 25 defendants indicted in the U.S. prosecution, many of whom remain fugitives, is Ahmed Khalaf Ghaibani. He was captured in a raid on his home in Pakistan in the summer of 2004 and held in secret CIA prisons until September 2009, when he was transferred to Guantanamo Bay. The U.S. government announced on March 31, 2008, that it would try Ghaibani by military commission, but the following year the government decided to try him in the

Southern District of New York instead. On January 25, 2011, he was sentenced to life in prison for conspiracy to destroy buildings.

A Prison Guard Is Stabbed

On November 1, 2000, Salim stabbed a prison guard with a sharpened comb when the guard escorted Salim back to retrieve some documents from the cell that Salim shared with K.K. Mohamed.

When the defendants met with their attorneys, they were escorted from their cells to the place where they met with the attorneys and were escorted back. Defendant Salim was escorted back by a corrections officer who was well known by that name. Protocol would have called for the inmate, the defendant, to be put into the cell, the cell to be locked, with the corrections officer outside the cell, the defendant still handcuffed. Then the defendant was to put his hands through an opening left for that purpose and the cuffs to be removed.

Well, Officer Louis Pepe didn't follow that protocol and took the handcuffs off Salim while he was still in the cell. Salim had taken a plastic comb and hoisted it into a knife and stabbed the corrections officer and inflicted a permanent brain injury to him.

Because Salim’s attorneys were both witnesses to the stabbing and potential targets, the court discontinued their representation of Salim and severed his prosecution from the other defendants' trial, which was scheduled to begin only two months after the stabbing.


234 Mohamed was not called as a witness at the trial of the other defendants. See Lance, supra note 231, at 6, 304. Benjamin Wesser, Lawyers Seeking to Expose plea Deal in Bombings Case, N.Y. Times, May 6, 2001, at E1.


236 See Wesser, Qaida Member, supra note 235, Wesser, Held Secretly, supra note 235.


238 S.D.N.Y. E.Hage Docket Sheet, supra note 204, see Benjamin Wesser, 10 Years for al Qaida Operative, N.Y. Times, Feb. 25, 2003, at B4 (reporting a sentence of ten years).


242 Ghaibani, 751 F. Supp. 2d at 525, see Glaberson, supra note 240, White & Warrick, supra note 241.
months later.\textsuperscript{247} Both Salim and K.K. Mohamed were transferred to other jails,\textsuperscript{248} but only Salim was charged with the stabbing.\textsuperscript{249} The court assigned the prosecution of Salim for the stabbing to Judge Deborah A. Batts.\textsuperscript{250} Salim pleaded guilty on April 3, 2002, to attempted murder.\textsuperscript{251} Judge Batts sentenced him to 32 years in prison,\textsuperscript{252} but the court of appeals concluded that a terrorism enhancement did not require transnational conduct,\textsuperscript{253} so Judge Batts resentenced Salim to life.\textsuperscript{254} The court of appeals affirmed the life sentence.\textsuperscript{255}

The Main Trial

The trial against Odeh, al-'Owhali, el-Hage, and K.K. Mohamed began with jury selection on January 3, 2001.\textsuperscript{256} With the help of a jury questionnaire, Judge Sanchi screened a jury pool of 1,302 people.\textsuperscript{257} Opening arguments began a month later, on February 5.\textsuperscript{258}

Many survivors of the bombings attended the trial, wearing lapel pins provided by a victims' advocate showing a map of Africa with Kenya and Tanzania highlighted.\textsuperscript{259} The pins helped the deputy marshals identify victims for appropriate seating, but Judge Sand ordered that the pins not be worn after defense counsel argued that they would improperly influence the jurors.\textsuperscript{260} Closing arguments began on May 1,\textsuperscript{261} and the jury began its deliberations on May 10.\textsuperscript{262} All four defendants were convicted of all charges on May 29.\textsuperscript{263} Judge Sand granted al-'Owhali's hearing—the first death penalty hearing in the Southern District of New York since the 1950s—and the jury began to deliberate on his sentence on June 5, 2001.\textsuperscript{264} On June 12, the jury announced that it

---

247. Bin Laden, 160 F. Supp. 2d at 673, Trying Cases, supra note 205, at 12 (remarks by Judge Sand); see Hirsh, supra note 191, at 213; Weisser, Quandary, supra note 245.


249. Bin Laden, 160 F. Supp. 2d at 673, see Weisser, Escape Plan, supra note 245.

250. Although the government did not charge Mohamed with participation in the stabbing, in an effort to persuade his sentencing jury to have him executed, the government argued that he participated in the stabbing. See Weisser, Doctor Details Injuries, supra note 245.


253. Salim, 549 F. 3d at 70, S.D.N.Y. Salim Docket Sheet, supra note 250 (also noting a $472,800 restitution order), see Salim, 287 F. Supp. 2d 250 (finding facts for the sentence calculation); see also Susan Saulye, As Attacker is Sentenced, Victim Vents Disgust and Is Ejected, N.Y. Times, May 4, 2004, at B3 (reporting that Judge Batts had to eject the victim from the court for disruptive behavior).


259. According to Judge Sand, the questionnaire and voir dire caused many jurors to assume that the court would tell them what penalty would go with each crime, and did not make clear that ultimate decisions on the death penalty would be for the jury to make. Interview with Hon. Leonard B. Sand, June 25, 2007.


261. It was reported that initially five jurors were to acquit el-Hage. Benjamin Weisser, A Jury To and Fearsful in 2001 Terrorism Trial, N.Y. Times, Jan. 3, 2003, at 11 [hereinafter, Jury Tow].


was deadlocked, which meant that al-Owhali would be imprisoned for life without the possibility of release. The jury began to deliberate on K.K. Mohamed’s sentence on July 5th and announced a deadlock on July 10th. On October 18, Judge Sand sentenced each of the four defendants to life in prison without the possibility of release. Because of the intervening and nearby attacks on September 11, court security on the day of sentencing was substantially enhanced. The defendants, including Salim, ultimately were sent to serve their sentences at the Administrative Maximum Facility, or “Super Max,” in Florence, Colorado.

New Trial Denied

On January 23, 2002, Judge Kevin Thomas Duffy took over for Judge Sand with respect to further proceedings in prosecutions for the embassy bombings. That same month, prosecutors learned that the United States Marshals Service had many hours of videotape recordings of interviews with the government’s first witness, an informant named Jamal Ahmed al-Fadl, that should have been turned over to el-Hage’s attorneys for preparation of cross-examination. In response to el-Hage’s motion for a new trial, Judge Duffy wrote, “Through a mixture of inaction, incompetence and stonewalling to cover up their mistakes, the United States Marshals Service and the Department of Justice’s Office of Enforcement Operations have seriously jeopardized the convictions of Al-Qaeda terrorist Wadih el-Hage.”

Al-Fadl was in the Witness Security Program, living in a secret location. Prosecutors had arranged for a videoconference connection to al-Fadl, and the Marshals Service had recorded videoconferences with al-Fadl without the prosecutors’ knowledge. Prosecutors received copies of the videotapes from the Marshals Service and provided defense counsel with transcripts, redacting “various portions to protect the identities of certain individuals and to protect operation information that they believed was not subject to discovery.” On October 24, 2003, el-Hage moved for a new trial. Judge Duffy concluded that “although this material would have fueled a significant attack on al-Fadl’s credibility, it would not have directly contradicted the government’s case, and it appears to fall within the general rule that undisclosed impeachment material generally does not warrant a new trial.” The court of appeals affirmed.

All four defendants appealed their convictions, but K.K. Mohamed withdrew his appeal.

After the trial, the New York Times published an article based on interviews with nine of the 12 jurors. The story reported that two jurors sought outside religious guidance on their sentence verdicts, one juror did legal research on the


275. In re Terrorism Bombings, 552 F.3d at 142, Bin Laden, 397 F. Supp. 2d at 474, see Weiser, Quadra Informer, supra note 273.


277. In re Terrorism Bombings, 552 F.3d at 515.


280. In re Terrorism Bombings, 552 F.3d at 101 n.1; 2d Cir Mohamad Docket Sheet, supra note 281 (noting a January 21, 2004, order that the appeal was withdrawn with prejudice), see Benjamin Weiser, 3 Seek Retrial in Bombing of Embassies, N.Y. Times, Jan. 23, 2004, at B4.

281. Weiser, Jury Trial, supra note 263 (reporting that one juror could not be found and two jurors declined interviews).
ternet, and some jurors were aware that the defendants were shackled under the defense table.284 Judge Duffy determined that the article entitled El-Hage to neither a new trial nor an evidentiary hearing.285

On November 24, 2008, the court of appeals affirmed the convictions of Odeh, al-Owhali, and El-Hage.286

A Guantánamo Bay Defendant

Nearly 11 years after the embassy bombings, Ghaithani, the ninth defendant in the third superseding indictment filed on December 16, 1998, was transferred from the detention camp at Guantánamo Bay, Cuba, to the Southern District of New York.287 Ghaithani’s alleged role was to obtain explosives and transport them to Dar es Salaam.288

Ghaithani grew up in Zanzibar, and after the embassy bombings he reportedly became a cook for Osama Bin Laden.289 He was arrested [in August 2004] after a 14-hour gun battle with the Pakistani authorities, in which he received a shrapnel wound.290 He was held in CIA custody until his transfer to Guantánamo Bay in 2006.291

On June 15, 2009, the case was transferred to Judge Lewis A. Kaplan.292 Judge Kaplan determined that the interval between Ghaithani’s indictment and his presentation to the court for prosecution did not violate a Sixth Amendment right to a speedy trial.293 Although the time since his transfer from CIA to military custody implicated his speedy trial right,294 he was not substantially prejudiced by the delay.295

Judge Kaplan also rejected Ghaithani’s argument that the indictment should be dismissed because of his alleged torture by the CIA while in its custody, because if Ghaithani’s allegation is true then “the proper remedy is money damages or criminal prosecution of the offending officers.”296

Jury selection began on September 22.296 Judge Kaplan used a jury questionnaire,297 but he did not want the questionnaire to deprive the court of the benefits of oral voir dire:

While the Court recognizes that eliciting pedigree information about prospective jurors by written questionnaire would be more efficient [than] doing so by oral voir dire, there is much to be said also for doing it orally. Affording an opportunity for prospective jurors to speak orally in the presence of the parties about familiar matters such as their backgrounds, education, employment and families may help make them sufficiently comfortable to be more responsive with respect to more sensitive matters. In any case, it gives the parties more of an impression of the individuals than would questionnaire answers alone.298

Voir dire began on September 29.299 Judge Kaplan appointed counsel to represent one of the jurors, whose employer apparently illegally refused to excuse the juror’s absence from work.300

The trial began on October 12.302 Judge Kaplan reserved some seats in the courtroom for the news media.303 On November 17, the jury found Ghaithani guilty

---

288 Al-Owhali and Odeh’s petitions for writs of certiorari were denied. Odeh v United States, 556 U.S. 1283 (2009).
291 Id.
292 S.D.N.Y. El Hage Docket Sheet, supra note 204.
on one count of conspiracy to destroy buildings but not guilty of the remaining 281 counts, including separate counts of murder for each of the persons killed at the two embassies. 302 Judge Kaplan sentenced Ghailani to life in prison. 303 An appeal was heard on May 8, 2013. 304

**A Challenge to Prison Security Measures**

On December 17, 2007, K.K. Mohamed submitted to the U.S. District Court for the District of Colorado a pro se complaint alleging improper conditions of confinement. 305 Magistrate Judge Boyd N. Boland reviewed the complaint and, on December 27, ordered it filed. 306 On September 29, 2011, District Judge Marcia S. Krieger dismissed most claims, but she ruled that the complaint, as amended, alleged a potentially valid violation of the First Amendment. 307 Pursuant to the prison’s Special Administrative Measures as applied to Mohamed, (1) the prisoner was permitted communication and visitation only with immediate family members and not with nieces, nephews, and in-laws; and (2) his mail could be held for surveillance for up to two weeks if written in English and up to two months if written in other languages. 308

Judge Krieger agreed to appoint pro bono counsel, if a willing attorney could be found. 309 According to Mohamed, an attorney attempted to send him mail in October 2011, but the mail did not reach Mohamed because of security measures. 310 In time, an attorney agreed to represent Mohamed, and the court initially set a discovery deadline of January 11, 2013. 311 A protective order forbids the attorney to use any discovery for any purpose other than litigating the current case. 312

**Extradited Defendants**

Judge Kaplan will preside over the trial of Fawwaz and Bary, the defendants extradited from Britain in 2012. 313 On June 20, 2013, Judge Kaplan denied Fawwaz’s motion to be tried separately. 314

**Osama Bin Laden’s Son-in-Law**

An indictment against Sulaiman Abu Ghayth, one of Osama Bin Laden’s son-in-law, was filed in the case against embassy bombers on March 1, 2013, for conspiracy to kill Americans based on the defendant’s support of Bin Laden in 2001. 315 Judge Kaplan set Abu Ghayth’s trial for January 7, 2014. 316

In 2002, Abu Ghayth was smuggled from Afghanistan into Iran following the 2001 U.S. invasion of Afghanistan. 317 He was kept under house arrest in Iran until his expulsion in 2012. 318 Turkey deported him to Kuwait in February 2013, but U.S. authorities arrested him during a layover in Jordan on February 28. 319

**Challenge: Attorney–Client Contacts**

In detention, the original defendants were cut off from virtually all communications. 320 They were permitted to meet with their attorneys, but the attorneys were prohibited from sharing anything said in the meetings with investigators or experts, which seriously hampered the preparation of a defense. 321 In response to

---


305 Ghailani Judgment, supra note 244; see Finn, supra note 244; Weiser, supra note 244. Ghailani is serving his sentence with the other embassy bombing defendants at the Super Max prison in Florence, Colorado. http://www.bop.gov (reg. no. 02476-748), see Benjamin Weiser, Heftened Security for a Former Detainee, N.Y. Times, June 10, 2011, at A23.

306 Docket Sheet, United States v. Ghailani, No. 11-320 (Cir. Cir. Jan. 28, 2011) (noting that the case was heard by Circuit Judges Pierre N. Leval, Jose A. Cabranes, and Barrington D. Parker, Jr.).


311 Mohammed Opinion, supra note 309, at 32.

312 Motion to Compel at 2, Mohammed, No. 1:07-cv-2697 (D. Colo. Nov. 15, 2011).

313 Order, id. (July 27, 2012).

---


315 S.D.N.Y.: El Hage Docket Sheet, supra note 204.


321 See Weiser, Suspects Isolated, supra note 322, Weiser, Judge to Hear Complaints, supra note 322; Weiser, Rules Violate Rights, supra note 322.
complaints by defense attorneys, Judge Sand visited the jail and approved the detention conditions, except that he ordered that the defendants be permitted to call their families three times a month instead of once.

Attorney-client communications were also impaired by the fact that defense counsel could not discuss classified evidence with their clients because the defendants did not have security clearances. The court of appeals affirmed Judge Sand’s ruling that failure to share classified information with the defendants, as opposed to their cleared counsel, did not violate the Constitution.

Relations between defendants and assigned counsel are often difficult; they were particularly so in this case: “Lawyers don’t often represent somebody who hates them, who, all things being considered, would just as soon kill them. How you maintain an attorney-client relationship under those circumstances is very difficult.”

Although circumstances suggested that Salim meant to do his attorneys harm, Ghailani’s confidence in his military commission attorneys was so great that he asked Judge Kaplan to order the Secretary of Defense to continue their representation of him in New York. Although the Secretary was not a party to the case, Judge Kaplan agreed to consider the motion. Judge Kaplan ruled that although an indigent defendant has a constitutional right to effective assistance of counsel, the indigent defendant does not have a constitutional right to select counsel.

Ghailani’s dissatisfaction with one of his appointed New York attorneys resulted in the court’s dismissing the attorney from the case.

Upon his indictment, the court assigned the federal defender to represent Abu Ghayth, but Abu Ghayth retained, with funds provided by his brother in Kuwait, a lawyer who himself was under federal indictment for tax improprieties. After a colloquy ensuring that Abu Ghayth knowingly accepted the risks of having an attorney who might seek favor for himself with the prosecution, Judge Kaplan approved the substitution.

**Challenge: Interpreters**

For the trial before Judge Sand, both Arabic and Kiswahili interpreters were required.

**Challenge: Mental Health During Detention**

After several months of restrictive confinement, el-Hage angrily criticized Judge Sand during a hearing for not reading a letter el-Hage had prepared that proclaimed his innocence and contended that the United States could have prevented the embassy bombings. Deputy marshals restrained el-Hage when he leapt from his chair in the courtroom and appeared to charge toward the judge. Approximately six months later, a psychiatrist reported that el-Hage’s solitary confinement was seriously impairing his mental health. The government agreed to give el-Hage a cell mate, but the court ruled that his conditions of confinement were largely proper, and el-Hage complained that the cell mate made his cell too crowded.

After the prison guard was stabbed, an incident not involving el-Hage, the prison removed el-Hage’s possessions and privileges. According to his wife, his mental state deteriorated sharply and he stopped recognizing his attorney. However, two court-appointed psychiatrists and a court-appointed psychologist determined that el-Hage was faking mental illness. Judge Sand decided that the


326 In re Terrorist Bombings, 552 F.3d at 115–30, 156, Bin Laden, No. 198-cr-1023, 2001 WL 66393; see Weiss, supra note 286.

327 Tryin’ Cases, supra note 205, at 13 (remarks by Judge Sand).


329 United States v. Ghailani, 686 F. Supp. 2d 279, 285–97 (S.D.N.Y. 2009), id. at 297 (“Ghailani asks this Court to decide only the constitutional effect of the Secretary’s attended action, not the propriety or wisdom of his decision to act in that manner.”)


332 See Benjamin Weiss, Bin Laden’s Son-in-Law Seeks a New Lawyer, but There’s a Snag, N.Y. Times, May 21, 2013, at A18 (also describing the attorney as "an outspoken former Legal Aid Society lawyer with a gray ponytail", who has also handled many terrorism cases over the years"), see also United States v. Cohen, No. 5-12-cr-316 (N.D.D.N.Y. June 14, 2012), Letter, United States v. Abu Ghayth, No. 1-98-cr-1023-26 (S.D.N.Y. May 24, 2013).

333 See Weiss, supra note 332, see also infra,“Prosecution of a Charity.”


337 See In re Terrorist Bombings, 552 F.3d at 149–50, Tryin’ Cases, supra note 205, at 13, see Weiss, Suspect Aways Innocence, supra note 335, Weiss, Suspect Charges, supra note 335.


341 See id.
expert opinions were well founded and that el-Hage was competent to stand trial. 342

During Ghailani’s pretrial phase, he unsuccessfully moved for proscriptions on the strip and visual body cavity searches performed every time he left the detention center for a court appearance. 343 Judge Kaplan found that such searches apply without exception to all inmates at the Metropolitan Correctional Center in Manhattan. 344 Ghailani claimed that he could tolerate these invasions of his dignity until the ninth occasion of the search in which he was required to not only display his bare buttocks but “open himself” to allow a visual rectal cavity inspection. 345 Between the time of search to which he objected and the time of Judge Kaplan’s ruling, Ghailani agreed to come to court to attend a proceeding only once. 346 A psychologist testified that the stress of the searches was exacerbated by post-traumatic stress disorder resulting from enhanced interrogation techniques during his CIA custody, the details of which are classified. 347

Judge Kaplan ruled that the government had made a credible showing that there were no ready alternatives to the search that would provide the same level of security. 348 If stress of the searches triggered a response that made him unable to assist in his defense, then his prosecution would be suspended until he recovered. 349

A week later, by letter apparently prepared by his attorney, Ghailani waived the right to attend a pretrial conference held that day. 350 A week after that, Judge Kaplan issued an order finding that Ghailani has never suffered from post-traumatic stress disorder and his refusal to attend proceedings was motivated in part by an effort to frustrate the prosecution. 351 Ghailani was back in court on the eve of trial for a three-day hearing on his successful motion to suppress a key witness, 352 and he was in court for his trial. 353

---

344. Id. at 510.
345. Id. at 510–11.
346. Id. at 511.
347. Id. & n.11.
348. Id. at 514.
349. Id. at 514–15.
352. S.D.N.Y. El Hage Docket Sheet, supra note 204.
353. See Benjamin Weiser, Inside Qaeda Terror Defense: Evolving Strategy and Emotional Pendulum, N.Y. Times, Jan. 18, 2011, at A18 (“The lawyers pleaded with him to come to court, and ultimately, Mr. Ghailani agreed to attend the trial after [the defense psychologist] helped reduce his anxiety.”)

---

**Challenge: Jury Security**

Judge Sand decided to close jury selection and use an anonymous jury, but not sequester the jury. 354

On Monday, Feb. 5, 2001, the first day of the trial, the 12 jurors and six alternates met at a secret location in Midtown Manhattan and were driven to court by armed federal marshals. Safety concerns were paramount for the jurors, who were not sequestered. The jury room was guarded by marshals and was checked each morning by bomb-sniffing dogs. But there was always the unexpected. One day, jurors said, they were startled when someone climbed through the window. It turned out to be a workman looking to use the bathroom. 355

For the trial against Ghailani, Judge Kaplan granted the government’s motion for an anonymous jury. 356 Deputy marshals shuttled the jurors to and from the courthouse and provided them with breakfast, lunch, and refreshments. 357

**Challenge: Court Security**

In the first trial, persons entering the courtroom had to pass through a metal detector and sign a log book stating their purpose in attending the trial. 358

At a law school presentation, Judge Sand recalled a critical security event: I held a conference before the jury was selected in my regular courtroom, which is a fairly standard size courtroom. The four defendants were seated in the jury box with a marshal on each side. The issue was that one of the defendants, El-Hage, had written a letter that he wanted to send to the media. The government objected, because they thought, “How do we know whether there are codes in that or other things that would not be apparent to us?” And so we were discussing the sending of a paraphrase—not the exact language, but the substance.

While this discussion is going on, El-Hage, seated next to two marshals in the jury box, jumps off the jury box and races toward the back door. Now, I don’t know why he was racing to the back door. I have a suspicion that he was not coming to shake my hand and thank me for the careful attention I was giving to his case. The courtroom was scattered with security officers. You know, you sort of look around and you see them, and they sometimes don’t do a thing. But you know, there was a security officer standing in front of me, shielding me with his body, which I appreciated. There had been a sketch artist who was just in the line of fire between El-Hage and myself. She immediately threw her easel over and ducked. Of course, one of the security officers tackled El-Hage just as he was coming up to the bench. 359

---

354. See Feuer, supra note 257, Gross, supra note 325, at 21–22, Weiser, supra note 256, Weiser, Jury Tor, supra note 263, Benjamin Weiser, Life-and-Death Questions in Embassy Bombings Case, N.Y. Times, June 6, 2001, at 13 (reporting that “even Judge Leonard R. Sand does not know their names”).
355. Weiser, Jury Tor, supra note 263.
356. Order, Ghailani, No. 1:98-cr-1023-9 (S.D.N.Y. June 16, 2010), see Ghailani Preliminary Remarks, supra note 297, at 2, see also Weiser & Myshar, supra note 298 (“the defense lawyers, prosecutors and even the judge have not been told their names”).
358. See Hirsh, supra note 191, at 71.
359. Trapping Cases, supra note 205, at 13 (remarks by Judge Sand).
Because of el-Hage’s actions, the defendants were shackled to the floor under the table. To prevent the jurors from realizing this, the jury was not present when defendants were brought in and out. And, for this trial, there was no “all rise” when the judge entered. Judge Sand believed it was important to conceal as much as possible any extraordinary security measures.

**Challenge: Witness Security**

The informant al-Fadl was formerly Osama Bin Laden’s payroll manager, whom the government had identified prior to his testimony, even to defense counsel, only as CS-1, which stood for “confidential source one.” He had been under U.S. protection in an undisclosed location since 1998 after pleading guilty to a conspiracy charge in a sealed proceeding in the Southern District of New York. In 1996, al-Fadl presented himself at the American embassy in Entebbe as an asset in the fight against al-Qaeda after he was caught embezzling nearly $110,000 from Bin Laden’s organization.

Al-Fadl’s identity was not revealed to defense counsel until four days before his scheduled testimony, and a protective order forbade counsel from revealing his identity to their clients until the day before al-Fadl appeared in court. Judge Sand forbade courtroom artists from sketching al-Fadl’s face.

---

360. Trying Cases, supra note 205, at 14 (remarks by Judge Sand), Interview with Hon. Leonard B. Sand, June 25, 2007, see Gross, supra note 325, at 15 & n.44; Hirsch, supra note 191, at 78
361. Trying Cases, supra note 205, at 14 (remarks by Judge Sand), Interview with Hon. Leonard B. Sand, June 25, 2007; see Hirsch, supra note 191, at 78
363. Interview with Hon. Leonard B. Sand, June 25, 2007
365. Al-Fadl is related by marriage to al-Nafii. See Weiser, Qada theme, supra note 235, Weiser, Held Secretly, supra note 235, Weiser, Qaeda Informer, supra note 273
366. The 9/11 Commission Report 109 (2004), Bin Laden, 397 F. Supp. 2d at 747, see Mark Bowden, The Finish 90 (2012), Bravin, supra note 290, at 202 (describing al-Fadl as “an al Qaeda turncoat who had become the US government’s star informant”); Lance, supra note 231, at 260-65 (describing al-Fadl as a Zelig of terror and reporting that the embezzlement resulted in part from jealousy over el-Hage’s higher compensation from Al-Qaeda); Soufan, supra note 191, at 66-69, 71; Weiser, Qaeda Informer, supra note 273
368. See id.

Judge Kaplan also forbade courtroom artists from sketching a witness’s face. Ghailani moved to suppress evidence from a witness whom Tanzanian authorities arrested in 2006, the FBI questioned, and who was released after the witness agreed to testify against Ghailani. Ghailani argued that finding the witness resulted from coercion during extremely harsh interrogation while Ghailani was in the CIA’s Rendition, Detention, and Interrogation Program. Judge Kaplan ordered an evidentiary hearing on the matter, at which the witness testified. The witness’s identity was initially redacted from Judge Kaplan’s opinion ordering the hearing, but his identity was revealed at the hearing and the opinion was refiled three weeks later without the witness’s name redacted. Judge Kaplan suppressed the witness, and the government elected not to delay the trial by appealing the suppression order.

**Challenge: Religious Accommodation**

An appointed attorney had to be dismissed for mocking his client’s religious beliefs. As Judge Sand reported,

An attorney who was very diligently representing his client was talking to his client. His client explained that if he died as a martyr he would go immediately to paradise and have thirteen virgin brides. The lawyer said, “Can you imagine having thirteen fathers-in-law?” The next morning there is on my desk a motion to replace the attorney. The defendant said, “How can I be represented by a lawyer who mocks my religion?” I granted the application.

Judge Sand carefully timed breaks in the trial to permit prayer at the appropriate times by the Muslim defendants, whose entry to and exit from the courtroom was made cumbersome by their hidden shackles.

---

370. United States v. Ghailani, 743 F. Supp. 2d 242, 247-48, 259-60 (S.D.N.Y. 2010), see Benjamin Weiser, Dispute Over Witness in Embassy Bombing Case, N.Y. Times, Sept. 3, 2010, at A16 (“brief references in declassified papers say he is a Tanzanian named Hussein who sold Mr. Ghailani hundreds of pounds of TNT that was later used to blow up the United States Embassy in Tanzania”)
371. Ghailani, 743 F. Supp. 2d at 248
372. Id. at 261, see Weiser, supra note 370
373. United States v. Ghailani, 743 F. Supp. 2d 261, 274 (S.D.N.Y. 2010), see Weiser, supra note 369
375. See Weiser, supra note 369.
378. See Benjamin Weiser, Prosecutors Will Not Appeal Ruling Barring Key Witness in Trial of Former Dealmaker, N.Y. Times, Oct. 11, 2010, at A19
379. Interview with Hon. Leonard B. Sand, June 25, 2007
380. Trying Cases, supra note 205, at 13 (remarks by Judge Sand).
381. See Hirsch, supra note 191, at 78.
Challenge: Classified Evidence

In order to have access to classified evidence, defense counsel had to have security clearances. Protective orders specified defense attorneys’ responsibilities for protecting government secrets.

Initially the attorneys in the original trial objected to their adversaries’ invading their privacy with background checks, but the government assured the attorneys and the court that background information would not be shared with prosecutors in the case. The court ruled that a security clearance requirement did not violate the defendants’ Sixth Amendment right to counsel, and the court of appeals affirmed.

For the prosecution of Abu Ghayth, the defendant’s retained counsel was under federal indictment for tax improprieties, but co-counsel was eligible for a security clearance.

Judge Sand resolved issues concerning discovery of classified information by conducting ex parte discussions with defense counsel concerning defense strategy and ex parte discussions with prosecutors concerning potentially relevant classified information. Sometimes Judge Sand was able to mediate a substitution for classified information.

The District Court held five in camera CIPA hearings in February 2001. Portions of the February 6, 2001 hearing were conducted ex parte; the others were attended by counsel for both sides. El-Hage’s defense attorneys, in the presence of the government, described in detail the classified material that they anticipated disclosing. The District Court then excused El-Hage’s counsel in order to inquire into the government’s reasons for refusing to declassify these items. After the government completed its presentation and was excused, the District Court recalled El-Hage’s attorneys, inquiring, in the absence of government counsel, into the use that El-Hage’s counsel planned to make of the classified information at issue. Having established that El-Hage’s attorneys wished to use the classified material for cross-examination of a government witness, the District Court suggested that the parties could work together to produce a paraphrased version of the relevant portions. The District Court then recalled the government in order to discuss the merits of this proposal with counsel on both sides.

Sometimes Judge Sand was able to determine that classified information was not as relevant as defense counsel thought it might be. After giving El-Hage’s counsel the opportunity to set forth their theory on the relevance of this information, the District Court explained that—based upon its review of an ex parte submission made by the government—it could represent with confidence that the classified information did not have the significance claimed by counsel.

Judge Sand held, and the court of appeals agreed, that the Fourth Amendment’s warrant requirement does not apply to extraterritorial searches by the U.S. government, but the Fourth Amendment’s reasonableness requirement does apply to extraterritorial searches of U.S. citizens. In 1996 and 1997, as part of an investigation of Al-Qaeda, telephone lines used by El-Hage in Kenya were bugged, and his Nairobi home was searched. To resolve El-Hage’s suppression motion, Judge Sand determined the reasonableness of the searches by ex parte examination of classified evidence instead of hearing evidence in an adversary proceeding. The court of appeals determined that Judge Sand’s method was appropriate.

Judge Kaplan reviewed classified information on Ghailani to determine what had to be produced in discovery to cleared defense counsel. Defense counsel challenged the adequacy of a chart summarizing the nature of 897 classified “CIA reports that the government claims are not themselves discoverable but that contain statements made by the defendant in response to custodial interrogation.” After reviewing 895 of the documents, Judge Kaplan determined that cleared defense counsel were entitled to an augmented chart “indicating, whenever the underlying documents so indicate, the duration of the interview in which a statement was made and whether that interview took place in the defendant’s cell or elsewhere.” Judge Kaplan determined that the defense was entitled to additional information about two of the documents—a summary of each statement referring to the Embassy Bombings sufficient to indicate the substance of the statement, the time when it was made, and to whom—and Judge Kaplan reserved judgment on two documents the government had not yet shown him.

384. See Weiser, supra note 382.
388. In re Terrorist Bombings, 552 F. 3d at 118–19.

National Security Case Management Studies (06-25-2013) 49

Sometimes Judge Sand was able to determine that classified information was not as relevant as defense counsel thought it might be. After giving El-Hage’s counsel the opportunity to set forth their theory on the relevance of this information, the District Court explained that—based upon its review of an ex parte submission made by the government—it could represent with confidence that the classified information did not have the significance claimed by counsel.

Judge Sand held, and the court of appeals agreed, that the Fourth Amendment’s warrant requirement does not apply to extraterritorial searches by the U.S. government, but the Fourth Amendment’s reasonableness requirement does apply to extraterritorial searches of U.S. citizens. In 1996 and 1997, as part of an investigation of Al-Qaeda, telephone lines used by El-Hage in Kenya were bugged, and his Nairobi home was searched. To resolve El-Hage’s suppression motion, Judge Sand determined the reasonableness of the searches by ex parte examination of classified evidence instead of hearing evidence in an adversary proceeding. The court of appeals determined that Judge Sand’s method was appropriate.

Judge Kaplan reviewed classified information on Ghailani to determine what had to be produced in discovery to cleared defense counsel. Defense counsel challenged the adequacy of a chart summarizing the nature of 897 classified “CIA reports that the government claims are not themselves discoverable but that contain statements made by the defendant in response to custodial interrogation.” After reviewing 895 of the documents, Judge Kaplan determined that cleared defense counsel were entitled to an augmented chart “indicating, whenever the underlying documents so indicate, the duration of the interview in which a statement was made and whether that interview took place in the defendant’s cell or elsewhere.” Judge Kaplan determined that the defense was entitled to additional information about two of the documents—a summary of each statement referring to the Embassy Bombings sufficient to indicate the substance of the statement, the time when it was made, and to whom—and Judge Kaplan reserved judgment on two documents the government had not yet shown him.

389. Id. at 119
391. In re Terrorist Bombings, 552 F. 3d at 159–60, Bin Laden, 264 F. Supp. 2d at 269
393. In re Terrorist Bombings, 552 F. 3d at 159, 167, 177
395. Id. at 1
396. Id. at 2
397. Id.

National Security Case Management Studies (06-25-2013) 50
Judge Sand’s and Judge Kaplan’s law clerks had security clearances. It is Circuit Judge Cabranes’ practice to ask his law clerks to seek security clearances, but Circuit Judge Newman has never had a cleared clerk, unless the clerk came with a security clearance as a result of previous employment. It is especially difficult for appellate judges to wait until they have a relevant case to ask their clerks to seek security clearances, because appellate judges are typically assigned to cases only a few weeks in advance of oral argument.

**Challenge: Classified Arguments**

By the time of Ghailani’s prosecution, electronic filing had become widespread in federal courts. Judge Kaplan issued a two-page order explaining how filings containing classified information would be electronically docketed: an unredacted copy of the filing would be filed with the classified information security officer and only a caption page would be filed electronically until a redacted copy could be filed electronically after a security review.

**Challenge: Classified Orders and Opinions**

A discovery order by Judge Kaplan early in the Ghailani prosecution contained details about two classified documents, about which Judge Kaplan determined cleared counsel were entitled to more information. The order was filed with the classified information security officer on November 24, 2009. The security officer arranged for redaction by intelligence agencies: two bulleted paragraphs were redacted from the order, and then the redacted order was filed publicly on December 7.

A second discovery order was filed with the classified information security officer on December 8, and a redacted version was filed publicly on February 4, 2010. Judge Kaplan’s opinion denying relief from strip and visual body cavity searches was filed with the classified information security officer on June 14, determined to contain no classified information, and then filed publicly three days later.

On July 12, Judge Kaplan filed with the classified information security officer an opinion rejecting Ghailani’s speedy trial motion, and the opinion was publicly filed the next day with three slight redactions. Also on July 12, Judge Kaplan filed with the security officer a classified supplement to his opinion discussing Ghailani’s treatment while in CIA custody. The supplement was docketed the next day, and a heavily redacted public version of it was filed two days after that.

On August 17, Judge Kaplan ordered an evidentiary hearing on whether testimony from a government witness should be suppressed because the government learned of the witness through extraordinary interrogation methods. Judge Kaplan’s memorandum opinion ordering the hearing was filed with the classified information security officer on August 18. On September 1, a heavily redacted version of the opinion was filed publicly. Reductions include the name of the witness and appear to include details of Ghailani’s capture, detention, and interrogation. The witness’s identity was revealed at the hearing on the admissibility of his testimony, and a substitute redacted opinion not redacting his name was filed three weeks after the hearing.

On October 6, Judge Kaplan agreed to suppress the witness. A redacted opinion on the matter was filed publicly approximately one week later.

**Challenge: Subpoenaing a Cabinet Officer**

Al-Owhali’s attorneys decided that testimony from Secretary of State Madeleine Albright might be helpful during the penalty phase of al-Owhali’s trial. It was reported, “The lawyers . . . said they want[ed] to question Dr. Albright about her knowledge of the number of Iraqi children dying as a direct consequence of the United States enforcement of United Nations sanctions following the Gulf

---

399 Interview with Hon. José A. Cabranes, Nov. 4, 2009.
401 Interview with 2d Ct. Clerk’s Office Staff, Nov. 6, 2009.
403 Ghailani Discovery Order, supra note 394.
404 S.D.N.Y. El Hage Docket Sheet, supra note 204.
405 Id.; Interview with Dep’t of Justice Litig. Sec. Group Staff, Jan. 7, 2010.
406 S.D.N.Y. El Hage Docket Sheet, supra note 204.

411 United States v. Ghailani, 743 F. Supp. 2d 242, 261 (S.D.N.Y. 2010); see Weiser, supra note 370.
412 S.D.N.Y. El Hage Docket Sheet, supra note 204.
413 Id.
414 Ghailani, 743 F. Supp. 2d 242, see United States v. Ghailani, 743 F. Supp. 2d 261, 281 (S.D.N.Y. 2010) (noting that the witness’s name was classified until approximately the time of the hearing).
416 Ghailani, 743 F. Supp. 2d 261.
418 See Hirsh, supra note 191, at 195-96 (reporting that al-Owhali wanted to prove that “U.S. government actions and al Qaeda actions could be viewed as similarly criminal”). Subpoena for Albright in Bombings Trial, N.Y. Times, Apr. 18, 2001, at B7 (hereinafter Subpoena for Albright).
On December 14, 1999, Ahmed Ressam was detained by customs officials suspicious of his nervousness as he tried to enter the United States by ferry from Canada into Washington with over 100 pounds of explosives in his car.\footnote{424} In Canada, he lived on welfare and petty theft.\footnote{425} In 1998 and 1999, he attended terrorist training camps in Afghanistan.\footnote{426}

Traveling under the name Benni Noris with fraudulent documentation, Ressam rented a car in Vancouver and drove it onto a ferry from Victoria to Port Angeles, Washington.\footnote{427} Ressam's car was the last off the ferry.\footnote{428} Noting that Res-

---


\footnote{420} See *Subpoena for Albright*, supra note 418.

\footnote{421} See Wesser, * supra note 419.

\footnote{422} See Hirsch, supra note 191, at 196.


\footnote{426} See *Trail of a Terrorist*, supra note 424, Soufan, supra note 424, at 141-42.

\footnote{427} Ressam, 679 F.3d at 1072-73, Ressam, 474 F.3d at 598-600.

\footnote{428} Ressam, 679 F.3d at 1071, Ressam, 474 F.3d at 599-600, Ressam, 221 F. Supp. 2d at 1254, see Ressam Complaint, supra note 424, Bock, supra note 424, Trail of a Terrorist, supra note 424, Soufan, supra note 425, at 142; Sundee & Porterfield, supra note 424, Verhovsek & Weiner, supra note 424.

\footnote{429} See Ressam, 474 F.3d at 600, Ressam Complaint, supra note 424, Bock, supra note 424, *Trail of a Terrorist*, supra note 424, Meyer, supra note 424, Soufan, supra note 425, at 142 (“Apparently he thought that the last car off would receive less attention.”), Sundee & Porterfield, supra note 424.
Ressam shared a motel room with another man for three weeks just before his ferry trip.\(^{438}\) Canadian authorities determined that the other man was Abdelmajed Dahoumâne.\(^{434}\) On January 20, 2000, Ressam’s indictment was superseded to add a terrorism charge and to add Dahoumâne as a defendant.\(^{435}\) On April 6, the U.S. embassy in Montreal offered a reward of $5 million for information leading to Dahoumâne’s arrest and conviction.\(^{435}\) Dahoumâne was arrested in Algeria late in 2000.\(^{436}\) On April 1, 2001, the Algerian government announced that it would try Dahoumâne there.\(^{435}\) Dahoumâne pleaded guilty in Algeria.\(^{436}\)

Investigation showed that Ressam had a reservation for one night’s stay at a Seattle motel near the Space Needle and a flight to London the following day.\(^{437}\)

---


440. Tim Reagan interviewed Judge Coughenour for this report in the judge’s chambers on October 3, 2008.


443. See Meyer, supra note 424 (reporting that this was the same bounty offered for Osama Bin Laden), Steve Miletich & Mike Carter, Prizes Found on Bomb Parts, Seattle Times, Apr. 12, 2000, at B1; Reward Offered on Suspected Terrorist, L.A. Times, Apr. 7, 2000, at 6; Sam Skolnik, U.S. Puts $3 Million Bounty for Algerian, Seattle Post-Intelligencer, Apr. 7, 2000, at A1; Vase & Eggem, supra note 442.


447. See Ressam Complaint, supra note 424, Miletich et al., supra note 434, Verhovek & Weiner, supra note 424.
Seattle canceled its millennium New Year's Eve party scheduled for the base of the Space Needle.448 Because of the extensive news coverage in Seattle about "the possibility of a planned bombing of the Space Needle, the signature building of the Seattle skyline," on March 3, 2000, Judge Coughenour granted Ressam's motion to move the trial to Los Angeles.449

It was reported that a substantial factor in Judge Coughenour's ruling was the superior security of Los Angeles's newer courthouse compared to Seattle's old courthouse, designed in the 1920s, where judges rode the same elevators as defendants, jurors, and witnesses.450 In addition, transportation of Ressam between the detention center in Seattle and the courthouse required road closures, but this was not necessary in Los Angeles because of the detention center's proximity to the courthouse.451

A minor international incident erupted in March 2000 as Ressam's attorneys prepared for trial.452 The Western District of Washington's Federal Public Defender's office agreed to accept service on Ressam's behalf of three seizure notices from the Royal Canadian Mounted Police.453 Two attorneys and an investigator traveled to Montreal to investigate the seizures, and they obtained from the court there copies of documents in the related files.454 Apparently, the documents were disclosed to Ressam's attorneys in error, and they were taken back from the attorney.


449. A large crowd gathered the following year "to watch the Space Needle turn into the world's biggest sparkler." The Center of the Celebration, Seattle Post-Intelligencer, Jan. 1, 2001, at B1.


457. Document Return Motion, supra note 456, see Militech, supra note 452.

458. Document Return Motion Response, supra note 454, Document Return Motion, supra note 455.

459. Document Return Motion, supra note 454, see Mike Carter, Ressam Lawyers May Use Secret Files, Seattle Times, Mar. 24, 2000, at B3.


461. See Carter, supra note 458; Sunde, supra note 452.


On April 6, 2001, the jury convicted Ressam on all counts. On the same day, he and 23 others were sentenced by a French judge, before whom Ressam was tried in absentia, to five years in prison for conspiracy to support Islamic militants. Abdelghani Meskini’s Brooklyn telephone number was found when Ressam was arrested. Meskini, who reportedly lived as a con man and thief, was once an Algerian Army officer, and he came to the United States as a stowaway in 1994. Apparently Meskini flew to Seattle on December 11, 1999, to meet Ressam. Because Ressam was a no-show, Meskini flew back to New York on December 16. On the basis of his number’s being in Ressam’s car, the Foreign Intelligence Surveillance Court authorized surveillance of Meskini’s telephone. Meskini was arrested early in the morning on December 30 at his home as a suspected accomplice of Ressam.

On January 6, 2000, a sealed indictment was filed in the Southern District of New York against Mohktar Haouari, a former schoolmate of Meskini’s in Algeria. He was arrested four days later in Montreal; another three days later, the indictment was superseded to add Meskini as a defendant. The court assigned the case to Judge John F. Keenan.

Based in part on surveillance of Meskini’s telephone conversations, Haouari was charged with coordinating Ressam’s bomb plot. Haouari waived extradition proceedings and agreed to be tried in the United States, where he was arraigned on August 14. On March 7, 2001, Meskini pleaded guilty and agreed to cooperate with the prosecution. On January 23, 2004, he was sentenced to six years, with credit for time served. He was released in 2005, his application for the witness protection program was rejected. With the government’s approval, he got a job in Atlanta as a building manager for an apartment complex known to be “a hotbed of criminal activity, where narcotics sales and prostitution occurred openly and persistently.” In October 2010, he was sentenced to two years and seven months for an attempt to acquire an AK-47 assault rifle.

As Ressam’s sentencing date approached, Meskini agreed to cooperate with the prosecution of Haouari, and Ressam’s sentencing was postponed. At Haouari’s trial, on July 3, 2001, Ressam testified that he and accomplices had

---


469 See Booth, supra note 468, Carter, supra note 468, Meyer, supra note 468, Skolnik & Sunde, supra note 468.


471 See Weiser, supra note 470.


473 Haouari, 429 F. Supp. 2d at 676, see Adams, supra note 444, Meyer, supra note 424, Mileitch & Carter, supra note 470, Vise, supra note 472.


478 Haouari Docket Sheet, supra note 476.

479 Tim Reagan interviewed Judge Keenan for this report in the judge’s chambers on November 6, 2000.

480 See John Sullivan, Algerian Arraigned in Explosives Smuggling Case, N.Y Times, Aug. 15, 2000, at B3.


482 Haouari Docket Sheet, supra note 476, see Weiser, supra note 470.

483 See Weiser, supra note 470.


485 Haouari Docket Sheet, supra note 476, see Benjamin Weiser, Millennium Plot’ Terrorists Reimprisoned in Guant, N.Y Times, Oct. 30, 2010, at A16.

planned to bomb Los Angeles International Airport on New Year's Eve. He said he planned to explode a suitcase filled with fertilizer and nitric acid.

In order to keep the witness Rassam separate from the defendant Haouri, each was brought to Judge Keenan's courtroom by a different elevator. There is one other courtroom on the same floor as Judge Keenan's, and separate prisoner elevators serve the two courtrooms. Rassam was brought up in the other courtroom's elevator.

Haouri found Rassam's testimony so upsetting that he repeatedly bashed his head against the counsel table. In time, he knocked himself out. Judge Keenan had to excuse the jury and seek medical attention for the defendant.

One juror, who worked as a waitress, had to be replaced when she recognized at work a journalist covering the trial and struck up a conversation with him about it.

On July 13, the jury acquitted Haouri of aiding and abetting what became known as the millennium bombing plot, but convicted him of conspiracy and fraud. On January 16, 2002, Judge Keenan sentenced Haouri to 24 years in prison. A year later, the court of appeals affirmed the conviction and the sentence.

On July 27, 2005, at the conclusion of Rassam's cooperation with investigations and prosecutions, Judge Coughenour sentenced Rassam to 22 years in prison.

A year and a half later, the court of appeals reversed Rassam's conviction on one count, for carrying explosives while committing a felony, reasoning that carrying explosives did not relate to the felony of signing a false name on a customs declaration. The court remanded the case for resentencing.

On December 7, 2007, the Supreme Court agreed to review the court of appeals' decision. On March 25, 2008, Attorney General Michael B. Mukasey, who, as a judge, had presided over the prosecution of blind Sheikh Omar Abdel Rahman, argued the government's case to reinstate the conviction.

499 Judge Coughenour observed that the gentler approach of Seattle-based investigators was more effective in obtaining Rassam's cooperation than the more aggressive approach of New York-based investigators, who took over during the prosecution of Haouri. Interview with Hon. John F. Coughenour, Oct. 3, 2008, see also Mike Carter, Mystery FBI Agent Revealed, Seattle Times, Nov. 15, 2012, at A1 ("Special Agent Fred Humphries was outspoken in opposing the FBI's decision at the time to turn Rassam over to agents from New York after the attacks, and warned their tough tactics were undoing the cooperation Humphries had coaxed out of the al-Qaeda-trained terrorist").


502 Rassam, 474 F.3d at 604, see Rassam, 679 F.3d at 1078, Shokovsky, supra note 501.

Judge Marsha S. Berzon joined Judge Pamela Ann Rymer's opinion for the court, but Judge Arthur L. Alarcon dissented from the reversal of the conviction and determined that Rassam's sentence was too lenient. Rassam, 474 F.3d at 604-05 (Judge Alarcon, dissenting). Six judges dissented from the court's refusal to rehear the case en banc: United States v. Rassam, 491 F.3d 997 (9th Cir. 2007).


National Security Case Management Studies (06/25/2013)
preme Court agreed with the argument and reinstated the conviction on May 19, 2005. On December 3, Judge Coughenour resented Ressam to 22 years. On February 2, 2010, a three-judge panel of the court of appeals determined that the sentence was too lenient and remanded the case for resentencing by a different judge. Over the dissent of four judges, on March 12, 2012, an 11-judge en banc panel agreed that the sentence was unreasonably lenient, but the en banc panel remanded the case to Judge Coughenour for resentencing. Judge Coughenour resented Ressam on October 24 to 37 years. 

**Challenge: Classiﬁed Evidence**

Invoking the Classiﬁed Information Procedures Act (CIPA), the government asked Judge Coughenour to review classiﬁed documents to determine whether or not they were discoverable. Judge Coughenour reviewed the documents


without the assistance of a law clerk, because there was not time to obtain top secret clearance. The documents were delivered to the judge by a classiﬁed information security ofﬁcer and reviewed by the judge under the security ofﬁcer’s watch. They were stored in a safe to which the ofﬁcer, and not the judge, had access. Judge Coughenour decided that the documents were not discoverable.

**Challenge: Examination of Foreign Witnesses**

The government sought testimony of witnesses in Canada, beyond the court’s subpoena power, who were unwilling to travel to the United States to offer testimony. So, by stipulation of the parties, Judge Coughenour travelled to Canada to preside over video depositions in both Montreal and Vancouver to obtain the testimony. A Canadian court ofﬁcial attended to rule on potential issues of Canadian law. Ressam participated by video conference from his jail cell with the assistance of an Arabic interpreter.

On one occasion, after Judge Coughenour had travelled to Canada for the deposition, a Canadian judge ruled, at a proceeding from which Judge Coughenour was excluded, that the witness did not have to testify.

Some of the witnesses subsequently indicated that they might be willing to testify live at Ressam’s trial, but the parties agreed that either side could substitute deposition video tapes.

**Challenge: Court Security**

At Ressam’s ﬁrst appearance in court in Seattle, on December 17, 1999, “Security was so tight that the courthouse—that everyone—even employees—had to produce a photo identiﬁcation. A phalanx of U.S. marshals also blocked the door to [U.S. Magistrate Judge David] Wilson’s courtroom and armed ofﬁcers patrolled the streets as Ressam was brought to the courthouse.”


512 Id.

513 Id.

514 Judge Coughenour preferred not to have to deal with the lock and combination himself. Interview with Dep’t of Justice, see Group Staff, Jan. 7, 2010.


521 Skolnik & Porterfield, supra note 424.
For Ressam’s trial also, security at the Royalal courthouse in Los Angeles was enhanced, including added patrols, bomb-sniffing dogs, and inspections of cars entering the underground garage.\footnote{522}

**Challenge: Jury Security**

Judge Coughenour was not asked to use an anonymous jury, he has never used one.\footnote{523} But jurors did not report directly to the courthouse; instead they met at a secret location from which they were transported to the courthouse by deputy marshals.\footnote{524}

**Challenge: Witness Security**

On March 29, 2001, Meskini testified at Ressam’s trial.\footnote{525} It was reported that his testifying would require his entering the witness protection program.\footnote{526} He was brought to the courtroom through a side door.\footnote{527}

Judge Coughenour overruled the government’s attempts to protect the identity of another witness, such as taking testimony remotely or behind a screen and withholding background information, and the government decided not to use the witness.\footnote{528}

---

522. See Carter, supra note 464.
524. Id.
527. Miletich, supra note 523.

---

**Mujahdeen Khalq**

*United States v. Afshari*  
(Robert M. Takasugi and David O. Carter, C.D. Cal.)

After a three-year investigation, on three criminal complaints filed in the Central District of California on February 26, 2001, the FBI arrested on February 27 five Iranians and two Iranian Americans at various Los Angeles locations.\footnote{529} They were charged with providing material support to Mujahdeen Khalq, also known as MEK, which the State Department classified as a terrorist organization on October 8, 1997.\footnote{530} MEK arose in the 1960s and 1970s in opposition to the shah of Iran.\footnote{531} It came to be a regular solicitor of donations at airports, including the Los Angeles International Airport, ostensibly for charitable purposes.\footnote{532} The defendants were charged with participating in those solicitation efforts.\footnote{533}

U.S. citizens Mohammad Omidvar and Navid Taj, also known as Najaf Eskoftegi, were granted $25,000 bail.\footnote{534} Iranian Hossein Afshari’s bail was set at $100,000.\footnote{535} The other Iranians—Roya Rahmani, also known as Tahmineh Tahamant, the only woman, Hassan Rezaee, Moustafa Ahmady, and Ali reza Mohammad Moradi—were denied pretrial release.\footnote{536} The grand jury returned an indictment on March 13.\footnote{537} Two days later, Rahmani’s bail was set at $500,000.\footnote{538} In April, bail was set for Rezaee, Ahmady, and Moradi at $60,000 each.\footnote{539}

On June 21, 2002, Judge Robert M. Takasugi dismissed the indictment.\footnote{540} Judge Takasugi determined that the statute authorizing the designation of MEK as a terrorist organization was unconstitutional:

---

531. Afshari, 426 F.3d at 1152; see Nelson, supra note 529.
532. Id.; see Nelson, supra note 529.
534. Afshari Docket Sheet, supra note 529.
535. Id.
536. Id.
538. Afshari Docket Sheet, supra note 529.
539. Id.


On March 10 from 5:00 to 9:00 p.m. and on March 11 from 6:00 p.m. until past midnight, Judge Carter held a status conference with all counsel and defendants in preparation for an April trial. Among the matters covered were the judge’s learning how to pronounce the participants’ names, a review of witnesses to be called, and preparation of a jury questionnaire. On March 17 and 18, Judge Carter heard motions. On April 9, the government filed a third superseding indictment.

Jury selection began on Friday, April 17. Jury questionnaire review continued on Monday and Tuesday, with jury selection to resume on April 29. On the morning of April 29, the parties announced that they were close to a settlement of the case. By 11:31 a.m., the parties were able to put plea agreements on the record. As a precaution, Judge Carter kept the jury at the courthouse during the plea colloquies.

Judge Carter delayed sentencing, because of political efforts to have MEK removed from the list of terrorist organizations. In September 2012, the Secretary of State removed MEK from the terrorist organization list.

On February 19, 2013, Judge Carter sentenced each defendant to three years of supervised release.

Challenge: Classified Evidence

In preparation for trial, the defendants filed a notice that they might introduce classified evidence, and Judge Carter reviewed classified evidence for discoverability.

The court’s contacts with classified information became much more sensitive when Judge Carter determined that for sentencing purposes he needed to know how likely it was that MEK would be removed from the terrorist list. Judge Carter, therefore, determined that he and his law clerks needed access to very sensitive and timely diplomatic and counterterrorism records.

Judge Carter’s law clerks and a court reporter received security clearances allowing them to view top secret sensitive compartmented information (SCI). SCI must be stored in a sensitive compartmented facility (SCIF). The Santa Ana courthouse does not have one, but the courthouse in Los Angeles has one. Classified information designated secret and not SCI could be stored in an approved safe in the Santa Ana courthouse.

Jessica Garrison & David Rosenzweig, Terror Funding Charges Rejected, L.A. Times, June 22, 2002, at 1

541. Lahman, 209 F. Supp. 2d at 1058.

For this report, Tim Reagan interviewed Judge Carter and his law clerks Daniel Galindo and Robert Hudson at the Santa Ana courthouse on October 16, 2012.

547. Id.
549. Third Superseding Indictment, id. (Apr. 9, 2009).
Detroit
United States v. Koubriti (Gerald E. Rosen, E.D. Mich.)

Six days after the September 11, 2001, attacks on the United States, federal agents visited a suspected Detroit apartment residence of Nabil al-Marahb, a suspect in the attacks. Apparently al-Marahb had moved, and the current residents—Karim Koubriti, Ahmed Hannan, and Farouk Ali-Haimoud—consented to a search. Agents found fraudulent identification documents in the name of Youssouf Hmissa, a former roommate, who had asked them to hold the documents for him. Koubriti and Hannan admitted that they knew that the documents were fraudulent. They were arrested that day and charged on the following day; they were indicted on September 27 for possession of false documents. Hmissa, who was arrested in Cedar Rapids, Iowa, also was indicted on September 27. Ali-Haimoud was arrested with Koubriti and Hannan, but he was not indicted until March 27, 2002.

Abdel Ihab Elmaroudi, the alleged ringleader in Chicago, also was indicted on March 27. On August 28, 2002, the government added charges against the defendants for material support of terrorism. The U.S. District Court for the Eastern District of Michigan assigned the case to Judge Gerald E. Rosen.

Hmissa's prosecution was severed from the other defendants' because he agreed to cooperate with the government and testify against them. On September 9, 2005, he was sentenced to six years and six months in prison for document fraud. He was deported to Morocco in 2007.

This case was a high-profile case that had received some national press coverage and a lot of local press coverage. The court selected 280 prospective jurors for the case, and Judge Rosen greeted them on March 18, 2003, with a speech discussing the case on which they might serve and welcoming them to their opportunity to provide civic service.

To select jurors, Judge Rosen worked with the attorneys to prepare a jury questionnaire. Based on answers to this questionnaire, the court and the attorney...
neyes were able to sort the potential jurors into three groups: (1) apparently suitable, (2) possibly suitable, and (3) not suitable. Juries were questioned individually, beginning with those "apparently suitable," in random order, and a jury was selected from the approximately 65–80 potential jurors in that group. On June 3, the jury convicted Koubriti and Elmadoudi of both terrorism and document-fraud charges, convicted Hannan of document-fraud charges only, and acquitted Ali-Haïmoud.

In December 2003, it came to the court's attention that the lead prosecutor in the case had withheld from defense counsel a potentially exculpatory or impeaching document. The defendant moved for a mistrial, but the government maintained that the document was not material. Judge Rosen ordered an investigation, which showed that the withholding of this document was the tip of a misconduct iceberg.

As thoroughly detailed in the Government's filing, at critical junctures and on critical issues, the prosecutor failed in his obligation to turn over the evidence to the Court. Further, the Government's filing also makes abundantly clear, the prosecution materially misled the Court, the jury and the defense as to the nature, character and complexion of critical evidence that provided important foundations for the prosecution's case. Judge Rosen concluded that "the prosecution early on in the case developed and became invested in a view of the case and the Defendants' culpability and role as to the terrorism charges, and then simply ignored or avoided any evidence or information which contradicted or undermined that view."

In a criminal trial over which Judge Arthur J. Tarnow presided, the prosecutor and a government witness were acquitted of wrongdoing. As a result, at the request of both the government and the defense, on September 2, 2004, the court dismissed the terrorism charges against Koubriti and Elmadoudi and ordered a new trial on the fraudulent-document charges against Koubriti, Elmadoudi, and Hannan. The government elected not to pursue further the charges tried.

The government nevertheless filed a fourth superseding indictment against Koubriti and Hannan on December 15, charging them with taking an automobile accident in July 2001 to defraud an insurance company. Hannan pleaded guilty on March 22, 2005, agreeing to a prison term of time served and deportation to Morocco. The court released Koubriti on bond on October 12, 2004. Koubriti unsuccessfully moved to dismiss the fourth superseding indictment as double jeopardy and otherwise a violation of due process. On February 9, 2010, Judge Rosen granted the government's motion to dismiss Koubriti's indictment for successful completion of pretrial diversion.

583. Id.
588. Koubriti, 336 F. Supp. 2d at 680–81; see also id. at 681–82 n.5 (“Having itself reviewed [additional] classified materials, the Court observes that they provide additional and substantial support for the conclusions reached in the Government’s filing.”).
589. Id. at 681, see Hakim, supra note 575 (quoting text).

National Security Case Management Studies (06-25-2013)
Koubriti filed a lawsuit against the Wayne County Jail for improper conditions of confinement, such as excessive security and serving him pork. The district court granted the county summary judgment on claims of insufficient exercise and serving pork, but denied summary judgment on excessive strip searches, and the case settled.

Elmadoudi was sentenced by the U.S. District Court for the District of Minnesota to four years and three months in prison for a separate prosecution for trafficking in fraudulent telephone calling cards, and he was sentenced by the U.S. District Court for the Northern District of Iowa to five years in prison for fraudulent use of Social Security numbers.

an agreement that would save Koubriti from a criminal record and provide him with a path to citizenship.

In their first motion for summary judgment, the defendants noted that "[w]hile incarcerated at the Wayne County Jail, Plaintiff was deemed a level 4 security risk by the U.S. Marshals, and as such, was placed in a 'super max' security cell block. Defendants' Summary Judgment Motion at 1, id. (July 25, 2006).

Between September 17, 2001 until August of 2003, Plaintiff Koubriti was incarcerated in the Wayne County Jail, and under level 4 'super max' security protocol, Plaintiff Koubriti was escorted in his cell for 23 hours per day, and allowed 1 hour per day of exercise. In August of 2003, Plaintiff was released, but was re-incarcerated again in November 2003. From November 2003 until July of 2004, Plaintiff Koubriti was once again incarcerated in the Wayne County Jail and given a level 4 max security risk classification.


Stipulated Dismissals, id. (Aug. 9 and 24, 2007).


In their first motion for summary judgment, the defendants noted that "[w]hile incarcerated at the Wayne County Jail, Plaintiff was deemed a level 4 security risk by the U.S. Marshals, and as such, was placed in a 'super max' security cell block." Defendants' Summary Judgment Motion at 1, id. (July 25, 2006).

Between September 17, 2001 until August of 2003, Plaintiff Koubriti was incarcerated at the Wayne County Jail, and under level 4 'super max' security protocol, Plaintiff Koubriti was escorted in his cell for 23 hours per day, and allowed 1 hour per day of exercise. In August of 2003, Plaintiff was released, but was re-incarcerated again in November 2003. From November 2003 until July of 2004, Plaintiff Koubriti was once again incarcerated in the Wayne County Jail and given a level 4 max security risk classification.

Id. at 2.


Stipulated Dismissals, id. (Aug. 9 and 24, 2007).


United States v. Elmadoudi, 501 F. 3d 935, 937, 940 (8th Cir. 2007) (describing the crime as "shoulder surfing," that is, surreptitiously memorizing other people's calling card and credit card numbers at the Minneapolis-St. Paul airport and then passing the numbers on to other people who used them to pay for telephone calls), cert. denied, 552 U.S. 1120 (2008), Amended Sentencing Judgment, United States v. Elmadoudi, No. 06-cr-262 (D. Minn. Oct. 17, 2006).


Challenge: Jury Security

To protect jurors' security, Judge Rosen implemented "soft sequestration." Jurors did not come directly to the courthouse in the morning. Instead, they assembled at a secret location and were driven to the courthouse in a van. Someone found out about the secret location and called the jury room with a death threat. On the following day, someone called the Detroit News with a death threat concerning the judge. The Marshal changed the jurors' meeting location, used a different-color van to transport them, and beefed up security for Judge Rosen's courtroom.

Another measure Judge Rosen implemented to protect jurors' security was to empanel an anonymous jury. Jury selection was conducted behind closed doors. Judge Rosen released a redacted transcript of the selection process, but only after the trial was over. Judge Rosen noted that it was very important to make sure that even the jury clerk knew that the names and addresses of the jurors were confidential.

Challenge: Sanctioning a Cabinet Officer

The Attorney General of the United States violated a gag order that was stipulated by the parties—indeed, drafted by the government—not once, but twice, which occasioned contempt motions by the defense throughout the trial, which I put off until after the trial. I think I was the first federal judge to be required to issue a public admonishment of the Attorney General of the United States.

On October 23, 2001, Judge Rosen issued a stipulated gag order forbidding public comments about the case that would have a reasonable likelihood of inter-
ferring with a fair trial. Eight days later, Attorney General John Ashcroft incorrectly stated at a press conference that the defendants in the case were “suspected of having knowledge of the September 11th attacks.” In addition, during the trial, the Attorney General commented favorably at a press conference on the credibility of the cooperating codefendant’s testimony.

On the day before the grand jury handed down the second superseding indictment adding terrorism charges for the first time, Fox News announced the forthcoming indictment in detail sufficient to suggest the indictment had been improperly leaked. On the following day, MSNBC News presented improperly leaked evidence against the defendants. The Attorney General’s responsibility for these leaks remained unclear.

The defendants moved for sanctions against the Attorney General on August 28, 2003. On the following day, Judge Rosen ordered the Attorney General “to show cause in writing why he should not be compelled to appear for a hearing to address Defendants’ motion.” In response, the Attorney General stated that he regretted making the statements and acknowledged that they were mistakes, but said that the errors were entirely inadvertent. Because the sanction motion occurred after the trial was over, a civil contempt sanction could not remedy the wrongdoing; the only type of pertinent contempt would be criminal contempt as a punitive sanction. Criminal contempt proceedings against a sitting Cabinet officer would require extraordinary procedures and implicate serious constitutional issues. Because the record did not suggest willful violation of the court’s order, Judge Rosen decided that confronting these difficulties would not be necessary. Because the Attorney General did violate the court’s order on two occasions, however, Judge Rosen decided to formally admonish him.

Challenge: Classified Evidence

In order to investigate claims of prosecutorial misconduct, the court had to review the prosecution’s entire case file, which included classified documents, as well as highly sensitive records maintained at CIA headquarters. Judge Rosen negotiated with the CIA’s general counsel to establish a protocol for the review and use of the CIA’s evidence. Because records of cable traffic could not be brought to Detroit, Judge Rosen traveled to McLean, Virginia, to review them. Review of classified evidence in Detroit required the court to (1) establish a sensitive compartmented information facility (SCIF) and (2) engage in the time-consuming process of obtaining security clearances for both court staff and defense counsel.

A SCIF is a secure room in which documents are stored in independently locked file drawers. The room was created by classified information security officers provided by the Justice Department’s Litigation Security Group, and then the court programmed the codes for access. Only chambers staff with security clearances may enter this SCIF.

If there is any chance that a case will involve classified information, Judge Rosen advised the following:

The first thing that the judge should do is to have a conference with the lawyers and attempt to determine whether classified information is going to be a part of the case. That’s not as easy as it sounds, because sometimes it is unclear whether classified information will be a part of the case. The government may have classified information, but they may not be certain if they are going to use it. So, at the very least, if it looks remote-ly as if classified information may be implicated in the case, the court should discuss this with counsel and have a very open discussion.

618. Koubri, 305 F. Supp. 2d at 728-29, see id. at 733 (“I didn’t initiate the gag order, but I intend to keep it in place until further order of the Court, and I intend to enforce it.”), see also The Prosecutor, supra note 567.


Two days after the news conference, the Justice Department acknowledged that it did not know whether three Arab men now in custody in Michigan had advance knowledge of the terror attacks of Sept. 11.” Don Van Natta, Jr., Justice Dept. Actor Stand on 3 Dreamed, N.Y. Times, Nov. 3, 2001, at B5; see The Prosecutor, supra note 567. More than five years after that, however, government counsel told an appellate panel at oral argument that Elmadouli was accused of supporting terrorists connected with the September 11, 2001, attacks United States v. Elmadouli, 504 F.3d 935, 938 n.3 (8th Cir. 2007).

620. Koubri, 305 F. Supp. 2d at 725, 735-36. See id. at 731, 734-36, supra note 566. supra note 566, at 22 (remarks by Judge Rosen), see The Prosecutor, supra note 567 (noting that Judge Rosen learned from the broadcast that he would precede over the case).


623. Id. at 725 n.1.


625. Koubri, 305 F. Supp. 2d at 725; see also id. at 737.

626. Id. at 737-38, 738, 739, Schmitt, supra note 616.


628. Id. at 726, 742, 752-57.

629. Id. at 726, 748-57.

630. Id. at 725-26, 757-65, see Schmitt, supra note 616, The Prosecutor, supra note 567.


637. See Reagan, supra note 634, at 17-18.


639. Id.

640. Trying Cases, supra note 566, at 3 (remarks by Professor Daniel J. Capra).
Twentieth Hijacker

*United States v. Moussaoui* *(Leonie M. Brinkema, E.D. Va.)*

On September 11, 2001, four hijacked commercial jumbo jets were crashed in New York, Virginia, and Pennsylvania, killing nearly 3,000 people, including 19 suspected hijackers. Two planes crashed into the two towers of the World Trade Center in New York City, and one plane crashed into the Pentagon, each of these planes apparently had five hijackers aboard. The fourth plane crashed near Shanksville, Pennsylvania, after passengers thwarted the hijackers’ plan to strike a strategic target—probably the Capitol. This plane apparently had only four hijackers aboard. Just a few days later, it was reported that Zacarias Moussaoui may have been intended to be the twentieth hijacker.

---

643. Pre-conviction appeals were heard by Fourth Circuit Judges William W. Wilkins, Karen J. Williams, and Roger L. Gregory; a post-conviction appeal was first heard by Judges Williams and Gregory and Fourth Circuit Judge William B. Traxler, Jr., and then reheard by Judges Traxler and Gregory and Fourth Circuit Judge Dennis W. Shedd.


t Trib., Sept. 20, 2001, at 9A (reporting that the French newsmagazine *L’Express* speculated online on September 19, 2001, that Moussaoui might be the twentieth hijacker).

Khalid Shaikh Mohammed wanted even more men, as many as seven or eight per plane. At least half a dozen men selected for the mission never made it into the United States—several had visas denied, others agreed to participate, then withdrew before ever leaving for the United States. At least one man was turfed away by an immigration officer at arrival McDermott, *Perfect Soldiers*, supra note 646, at 204 (footnotes omitted).
Moussaoui could not hijack a plane on September 11, because he was in custody following an arrest in Minnesota on August 16 for an immigration violation. Three days earlier, he had begun instruction at the Pan American Flight Academy. It was initially reported that he aroused suspicion when he expressed an interest in steering a jumbo jet but not in taking off or landing. The Washington Post reported in November, however, that the director of the FBI told federal prosecutors at a closed-door meeting that initial reports of Moussaoui's not wanting to learn how to take off or land were inaccurate, and Moussaoui no longer was thought to be intended as the twentieth hijacker, he was thought to have been intended for a later attack.

Moussaoui was born on May 30, 1968, in the Atlantic coast town of St.-Jean-de-Luz, France, the youngest of four children. He moved to London in 1990, and then moved back to France in 1997. By the time he entered the United States on a student visa, French authorities already suspected him of terrorist ties. In February 2001, he moved to Norman, Oklahoma, for training at the Airman Flight School, where his performance was judged poor.

649 The 9/11 Commission Report 247 (2004) (reporting that the planners of the attacks might have canceled them if they had known about Moussaoui's arrest), Moussaoui, 591 F.3d at 266, Moussaoui, 382 F.3d at 457, Moussaoui, 333 F.3d at 512, United States v. Moussaoui, 282 F. Supp. 2d 486, 483 (E.D. Va. 2003), see Katherine C. Donahue, Slave of Allah 3, 13–16 (2007); Johnston & Shenon, supra note 645; McDermott, Perfect Soldiers, supra note 646, at 226; Peterson, supra note 648; H.L. Pehlivan, Terrorism and the Constitution 192 (2008), Soufan, supra note 646, at 277.


652 Dan Egggen, Yemeni Fugitive Linked to Hijackers, Wash. Post, Nov. 15, 2001, at A20, see Bin al-Shehhi Deposition Opinion at 3, United States v. Moussaoui, No. 01-61-cr-655 (E.D. Va. Mar. 10, 2003), available at 2003 WL 21263699 ("he suggests that he was part of another operation to occur outside the United States after September 11 involving different members of al Qaeda"). Philip Shenon, P.B.I. Chief Says Failed Sept. 11 Hijackers May Remain at Large, N.Y. Times, Nov. 17, 2001, at B5, see also McDermott, Perfect Soldiers, supra note 646, at 204 (reporting that attack planners decided that they would use Moussaoui only as a last resort).

653 The 9/11 Commission reported that Khalid Sheikh Mohammed was between two and six operators per plane. KSM states that at Qaeda had originally planned to use 25 or 26 hijackers but ended up with only the 19. The 9/11 Commission Report 235 (2004).

654 See Daley, supra note 648, 591 F.3d at 42, 104, Schmidt & Romano, supra note 651.

655 See Daley, supra note 648.

During this time, he apparently had contact with Ramzi Muhammad Abdullah Bin al-Shihab, a roommate of Mohamed Atta in Hamburg, Germany. Atta was believed to be the leader of the September 11 attacks and the pilot of the first plane to hit the World Trade Center. Bin al-Shihab apparently warned Moussaoui $14,000, $8,600 of which Moussaoui used for flight school. Ramzi Bin al-Shihab was also known as Ramzi Omar, and he too came to be suspected as the intended twentieth hijacker, but he was repeatedly denied a visa to enter the

In April 1998, Moussaoui was at the same terrorist training camp in Afghanistan as Ahmed Ressam, who is sometimes referred to as the Millennium Bomber United States v. Ressam, 679 F.3d 1069, 1075 (9th Cir. 2012), see Donahue, supra note 649, at 121, 165, see also supra, "Millennium Bomber" (concerning the prosecution of Ressam).


657 "Atta was a finicky, dour man whose chief attributes were obedience and a capacity for detail." McDermott, The Mastermind, supra note 646, at 49. "Where Atta was the dutiful steward, bin al-Shihab was an affable layabout who rarely held a job for more than a few weeks and found university study not worth his effort. A friend in Hamburg said Atta was impossible to like, but bin al-Shihab had charm to spare." McDermott & Meyer, supra note 646, at 140.


662 See McDermott, The Mastermind, supra note 646, at 49, Soufan, supra note 646, at 272. "His real name, he said, had no religious meaning, so he adopted the name of the prophet Mohamed—his success as the second caliph of Islam. Many Americans in Hamburg didn’t even know Omar had another name." McDermott, Perfect Soldiers, supra note 646, at 37.

663 See New Theory, supra note 645, Risen, supra note 658, Shenon, supra note 652, Tagliabue, supra note 659, see also Bruno, supra note 646, at 346 (reporting on an apparent military commission confession “that, as the government alleged, he, too, had aspired to be a twentieth Hijacker”).

Another person designated a twentieth hijacker—Mohammed al-Qutbani—was detained at Guantánamo Bay. See Peter L. Bergen, Man Hunt 95 (2012) ("the man in Qaeda was grieving to be the twentieth hijacker in the months before the 9/11 attacks"). Bravan, supra note 646, at 252–55 (reporting that al-Qutbani was denied entry on August 4, 2011, at the Orlando airport), Jona-
than Hafetz, Habeas Corpus After 9/11 38 (2011); Charlie Savage, William Glaberson & Andrew W. Lehren, Classified Files Offer New Insights Into Detainees, N.Y. Times, Apr. 25, 2011, at A1, Soufan, supra note 646, at 458–59, Steven T. Wac, Kafka Comes to America: Fighting for Justice in the War on Terror 154 (2008). He has been declared “incompetent and unable to assist effec-
United States. He was captured in Karachi, Pakistan, on the eve of the first anniversary of September 11, held in Morocco in secret by the CIA, and eventually transferred to Guantánamo Bay. He is on trial there by military commission.

Unlike the hijackers, who trained on aircraft simulators for a year or more, Moussaoui enrolled in flight school only months before the September 11 attacks.

The government filed an indictment against Moussaoui on December 11, 2001, in the U.S. District Court for the Eastern District of Virginia. Four of the six conspiracy counts exposed Moussaoui to the death penalty, and the court immediately appointed three attorneys to represent him. The court assigned the case to Judge Leonie M. Brinkema.

At his January 2, 2002, arraignment, Moussaoui refused to enter a plea. "In the name of Allah, I do not have anything to plead. I enter no plea. Thank you very much." Judge Brinkema, with the consent of Moussaoui's lawyer, entered a plea of not guilty. Meeting a deadline set by the court, the government announced on March 28 that it would seek the death penalty.

Moussaoui refused to honor the judge by standing when she entered or left the courtroom, so Judge Brinkema arranged proceedings so that she and he would enter and leave the courtroom at the same time.

At a hearing on April 22 concerning Moussaoui's conditions of confinement, the defendant raised his hand and, when recognized by Judge Brinkema, began a 50-minute diatribe on Islam and the U.S. government's conspiracy to kill him. He said that his lawyers did not understand Muslims, so he would like to represent himself, possibly with the assistance of a Muslim lawyer. Judge Brinkema said that he could represent himself if he were adjudged competent to do so, but that she recommended against it and would continue the appointment of his attorneys as backups.

The government filed a superseding indictment on June 19, and at the arraignment six days later Moussaoui tried to plead no contest. Judge Brinkema admonished him that such a plea did not mean what he seemed to think it meant and again entered a plea of not guilty on his behalf.

On June 24, in Ring v. Arizona, the Supreme Court determined that aggravating factors meriting a death sentence must be proved to a jury beyond a reasona-

---


665. E.D. Va. Docket Sheet, supra note 670, Moussaoui, 591 F.3d at 267, see Copeland, supra note 671; Donahue, supra note 649, at 33, 59, 60.

666. E.D. Va. Docket Sheet, supra note 670, Moussaoui, 591 F.3d at 267, see Copeland, supra note 671; Donahue, supra note 649, at 20, Johnston, supra note 671.


668. See Donahue, supra note 649, at 9, 64.


672. See Shenon, id., and Johnston, supra note 670, supra note 679.
ble doubt. So the government filed a second superseding indictment on July 16 to accommodate the requirements of Ring. At the July 18 arraignment on the new indictment, Moussaoui announced, "I, Moussaoui Zacarias, in the interests to preserve my life, enter with full conscience a plea of guilty, because I have knowledge and participated in Al Qaeda."

Judge Brinkema decided to give him a week to reconsider his guilty plea. On July 25, Moussaoui insisted that his support for Al-Qaeda did not include involvement in the September 11 hijackings, and, on instructions from Judge Brinkema that this was inconsistent with a guilty plea, he changed his plea to not guilty.

On January 31, 2003, Judge Brinkema secretly ordered the government to allow Moussaoui’s standby attorneys to interview Bin al-Shih, who was undergoing intensive interrogations overseas. Judge Brinkema postponed the trial indefinitely to permit the government to appeal. The court of appeals stayed the appeal briefly and remanded the case so that the government could consider alternatives to the evidence sought. Judge Brinkema ruled that a government summary of what Bin al-Shih would say if interviewed would be insufficient because of its unreliability, incompleteness and inaccuracy. After oral argument on June 3 before Circuit Judges William W. Wilkins, Karen J. Williams, and Roger L. Gregory, the court of appeals determined on June 26 that it did not have appellate jurisdiction over Judge Brinkema’s order, and the merits of the government’s objection were not so clear as to warrant mandamus.

On August 29, Judge Brinkema ordered the government to provide Moussaoui deposition access to Khalid Sheikh Mohammed (KSM)—regarded as the mastermind of the September 11 attacks—and Mustafa Ahmed al-Hawaswi—regarded as the paymaster for the September 11 attacks—as well. KSM and al-Hawaswi had been captured in Pakistan on February 7. The government refused to comply with the deposition orders, so Judge Brinkema ruled that the government could not argue that Moussaoui had anything to do with the September 11 attacks, and Judge Brinkema ruled that the government could not seek a sentence of death.


696. San Francisco, supra note 649, at 198, 344 (2003), see Donahue, supra note 649, at 34, at 34. KSM had been awaiting the return of an Israeli lawyer who had been killed in the September 11 attacks.


National Security Case Management Studies (06-25-2013)
The same panel that dismissed the appeal of Judge Brinkema’s deposition order determined that this sanction order was appealable.695 Although the court of appeals agreed that the government’s proposed substitutions for detainee depositions were inadequate, in an opinion by Judge Wilkins, the court ordered Judge Brinkema to attempt to craft adequate substitutes.696 Judge Gregory dissented in part on the ground that substitutions for witness depositions would not be sufficient to justify a death sentence.697

As part of the government’s interrogation of the three detainees, it had prepared classified detainee reports for military and intelligence use.698 The government prepared classified summaries of these detainee reports for the use of cleared counsel in Moussaoui’s prosecution.699 The court of appeals did not share Judge Brinkema’s skepticism about the reliability of the detainee reports: the interrogators “have a profound interest in obtaining accurate information from the witnesses and in reporting that information accurately to those who can use it to prevent acts of terrorism and to capture other al Qaeda operatives.”700 Noting that Judge Brinkema judged the summaries accurate reflections of the reports, the court of appeals ruled that the summaries “provide an adequate basis for the creation of written statements that may be submitted to the jury in lieu of the witnesses’ deposition testimony.”701

Meanwhile, on November 14, 2003, Judge Brinkema decided that because of his frequent inappropriate filings Moussaoui could no longer proceed pro se.702 Seventeen months later, on April 22, 2005, one month after the Supreme Court denied his petition for a writ of certiorari, Moussaoui pleaded guilty to a conspiracy to kill Americans, but denied involvement in the September 11 attacks.703

Judge Brinkema bifurcated Moussaoui’s penalty trial into a first phase on whether he was eligible for the death penalty and a possible second phase on whether he merited the death penalty.704 Jury selection began on February 6, 2006.705 The court sent summonses to more than 1,000 residents within the district’s Alexandria division.706 Judge Brinkema used an anonymous jury, and to facilitate juror selection she used a jury questionnaire, which more than 500 potential jurors filled out.707

Opening statements began on March 6.708 The government’s core argument for Moussaoui’s execution was that the tragedies of September 11, 2001, would not have occurred had Moussaoui not lied to authorities following his arrest in August 2001.709 Proceedings were not publicly televised, but they were broadcast to viewing sites in Manhattan, Central Islip, Boston, Philadelphia, Newark, and Alexandria for family members of September 11 victims.710

As the sentencing trial entered its second week, Judge Brinkema learned that a lawyer for the Transportation Security Administration was improperly coaching witnesses who were aviation officials.711 Judge Brinkema ruled that the coached witnesses could not testify.712


704 Moussaoui, 591 F.3d at 275, Leonie M. Brinkema, United States v. Moussaoui: Preliminary Venue Instructions (Feb. 6, 2006), Leonce M. Brinkema, United States v. Moussaoui: Jury Instructions for Penalty Phase Part Two (Feb. 6, 2006), see Donahue, supra note 649, at 33, 65.


706 Interview with Hon. Leonie M. Brinkema, Mar. 26, 2008.

707 Trial Conduct Order 1, Moussaoui, No. 1:01-cr-455 (E.D.Va. Feb 2, 2006), Leonie M Brinkema, United States v. Moussaoui: Jury Questionnaire (Feb 6, 2006), Interview with Hon. Leonie M. Brinkema, Mar. 26, 2008, see Donahue, supra note 649, at 59 ("Beginning on Wednesday, February 15, the potential jurors were to arrive in smaller groups for individual questioning, or voir dire, in order to create a pool of 85 potential jurors."). Id. at 61-62; Jerry Markon, Terrorism Jury Faces slew of Questions, Wash. Post, Nov. 29, 2006, at B1.


"During the trial, Judge Brinkema remarked that fewer people were watching from the off-site courtrooms than anticipated." Donahue, supra note 649, at 174.

711 See Donahue, supra note 649, at 69-70; Stephen Lahatson & Matthew L Wald, Lawyer Thrust Into Spotlight After Mistry in Terror Case, N.Y. Times, Mar. 15, 2006, at A1, Neil A

695 Moussaoui, 382 F.3d at 462-63.


698 Moussaoui, 382 F.3d at 483-89 (Judge Gregory, concurring in part and dissenting in part), see Markon, supra note 696, Pohlian, supra note 649, at 226-27.

699 Moussaoui, 382 F.3d at 458 n.5.

700 Id.

701 Id. at 478.


703 Plea Statement, Moussaoui, No 1:01-cr-455 (E.D. Va Apr. 22, 2005), Moussaoui, 382 F.3d at 272, United States v. Moussaoui, 483 F.3d 220, 223-24 n.1 (4th Cir. 2007), see Donahue, supra note 649, at 31; Neil A. Lewis, Moussaoui Tells Court He’s Guilty of a Terror Plot, N.Y
The trial continued and jurors began to deliberate on Wednesday, March 29. After a weekend break, on Monday, April 3, the jurors unanimously agreed that Moussaoui lied to federal agents knowing that people would die as a result. On Monday, April 24, the jury began to deliberate on Moussaoui’s penalty, returning a verdict of life in prison on Wednesday, May 3. After interviews with two anonymous jurors, The Washington Post reported that Moussaoui’s life was spared by a single juror’s vote.

Surprised that the jury spared his life, and more confident as a result in the possibility for a fair trial in an American court, Moussaoui moved on May 8 to withdraw his guilty plea. Judge Brinkema denied his motion. The court of appeals affirmed on January 4, 2010: “the finality of the guilty plea, entered knowingly, intelligently, and with sufficient awareness of the relevant circumstances and likely consequences, stands.”

Challenge: Attorney Appointment

Judge Brinkema initially appointed the Federal Public Defender and a private attorney to represent Moussaoui. The relationship between Moussaoui and his appointed attorneys was strained at best, and Moussaoui almost immediately began demanding to proceed pro se, but with the assistance of Muslim counsel. Moussaoui identified a Muslim attorney in Texas with whom he wanted to consult, but this attorney never made an appearance, never sought admission to the court’s bar, and never consented to the screening required for the security clearance that would be needed to represent Moussaoui in court.

Moussaoui’s relations with his appointed private attorney were more problematic than his relations with the Federal Defender’s office, so Judge Brinkema appointed another private attorney. “Although Moussaoui initially refused to...

According to Moussaoui’s affidavit, 16. I was extremely surprised when the jury did not return a verdict of death because I knew that it was the intention of the American justice system to put me to death.

17. I had thought that I would be sentenced to death based on the emotions and anger toward me for the deaths on September 11 but after reviewing the jury verdict and reading how the jurors set aside their emotions and disgust for me and focused on the law and the evidence that was presented during the trial, I came to understand that the jury process was more complex than I assumed.

18. Because I now see that it is possible that I can receive a fair trial even with Americans as jurors and that I can have the opportunity to prove that I did not have any knowledge of and was not a member of the plot to hijack planes and crash them into buildings on September 11, 2001, I wish to withdraw my guilty plea and ask the Court for a new trial to prove my innocence of the September 11 plot.

Moussaoui Affidavit at 3, Motion to Withdraw Plea, supra, see Donahue, supra note 649, at 167.

720 Order Denying Plea Withdrawal, Moussaoui, No. 1:01-cr-455 (E.D. Va May 8, 2006), Moussaoui, 591 F.3d at 278, see Donahue, supra note 649, at 102, 167, Lewin, supra note 719, Markon, supra note 719, Pohlman, supra note 649, at 247.

721 Moussaoui, 591 F.3d at 307, see Docket Sheet, United States v. Moussaoui, No. 06-4944 (4th Cir. May 15, 2006) [hereinafter 4th Cir. May 15, 2006, Docket Sheet]


Tim Reagan attended the September 25, 2009, reharing, interviewed Judge Gregory for this report in the judge’s chambers that same day, and interviewed Judge Shedd by telephone on September 12, 2009.

722 Moussaoui, 591 F.3d at 267. 723 Id. 724 Id. at 269. 725 Id.
communicate with any of his appointed counsel, he later testified that he began communicating with [the second private attorney] because [that attorney] was polite to him.  

**Challenge: Pro Se Defendant**

A court-appointed psychiatrist determined that Moussaoui was a fanatic, but not mentally incompetent to stand trial or waive his right to counsel. On June 13, 2002, Judge Brinkema granted Moussaoui’s motion to represent himself, keeping appointed attorneys as standby. Because of his pro se status, Moussaoui was eventually given three cells to accommodate his access to documents in this case.

As a result of his disruptive filing behavior, however, Judge Brinkema withdrew the privilege of self-representation in November 2003.

**Challenge: Court Security**

Security was enhanced at Moussaoui’s arraignment. He arrived before 6:00 a.m., while it was still dark. Deputy marshals surrounded the courthouse, and extra metal detectors were stationed at the courtroom. Although the outside air was frigid, members of the news media and the public—there were several dozen of the former and almost none of the latter—were not allowed into the building until shortly before the hearing. At subsequent appearances also, extra deputy marshals guarded the courthouse. It was reported that the courthouse had never seen such a level of security.

On Friday, April 22, 2005, at the hearing concerning Moussaoui’s conditions of confinement where Moussaoui asked to proceed pro se, security at the Alexandria Federal District Court was extremely tight. Two dogs and their handlers patrolled the street outside the courthouse, sniffing people’s briefcases and purses for explosive devices. People entering the courthouse passed through a nuclear materials detector positioned just outside the doors. Up on the seventh floor, Courthouse 700 was closed off until 1:30 p.m. . . . At precisely 1:30 p.m. the guards let people take the elevators up from the second floor. The lawyers, press, family members of 9/11 victims, and the curious began to file in, again passing through another security checkpoint. DIs were checked, briefcases were x-rayed, people walked through metal detectors, men pulled their pant legs up to show that they had nothing hidden in their socks. At exactly 3:30 p.m. Judge Brinkema and Zacarias Moussaoui both entered the courtroom. Proceedings began.

**Challenge: Jury Security**

Judge Brinkema used an anonymous jury. Jurors assembled in a secret location and were driven to the courthouse. The court set up a special room for the jurors to eat lunch away from the public. They were never permitted to be in the building unsupervised.

Judge Brinkema observed that it is important to work cooperatively with the Marshal while maintaining ultimate responsibility.

**Challenge: Classified Evidence**

Classified materials require extraordinary procedures, but Judge Brinkema tries to keep procedures as normal as possible. She requires all of her law clerks and other staff members to qualify for top-secret security clearances. Because Moussaoui’s standby attorneys would need access to classified evidence to prepare his defense, Judge Brinkema issued a protective order, which provided that defense access to classified information would require appropriate security clearances and the signing of a memorandum of understanding requiring that classified secrets be kept secret forever.

Moussaoui himself was not supposed to have access to classified information. But, in June and July of 2002, the government inadvertently included

---

726. Id. at 271 n. 6.
730. Order Vacating Pro Se Status, supra note 702, Moussaoui, 591 F.3d at 271, United States v. Moussaoui, 382 F.3d 453, 460 n. 6 (4th Cir. 2004).
731. See Copeland, supra note 671; Johnston, supra note 671.
732. See Copeland, supra note 671; see also Brooke A. Masters, *Alexandria's Logistical Juggling Act*, Wash. Post, Mar 14, 2002 (“High-risk prisoners are being transported between the jail and the courthouse at night or in the early morning, and the streets are shut down to minimize the risks.”)
733. See Johnston, supra note 671.
734. See Masters, supra note 732.
735. See Libby Copeland & Richard Leiby, *The Moussaoui Circus Extends Its Run*, Wash. Post, July 26, 2002 (“This is the most security we’ve ever had to use here at the courthouse since it opened in 1996,” said John Clark, acting U.S. Marshal for the Eastern District of Virginia.”)
736. Id.
737. Donahue, supra note 649, at 32.
738. Trial Conduct Order 1, supra note 707, see Markon, supra note 707.
740. Id.
741. Id.
742. Id.
743. Id.
744. Id.

As the Government strenuously argues, the defendant’s repeated prayers for the destruction of the United States and the American people, admission to being a member of al Qaeda, and
classified materials among documents produced to Moussaoui. 47 On August 22,
the government wrote to Judge Brinkema stating that two documents produced to
Moussaoui had mistakenly not been classified and asking that a “walled-off FBI
team” search Moussaoui’s cell to retrieve the documents. 54
Judge Brinkema denied the FBI search.

[...]

But Judge Brinkema did permit the Marshal Service, in consultation with the clas-
sified information security officer, to search Moussaoui’s cells for the two docu-
ments plus an additional five that the government identified in the interim as im-
properly produced. 51 Of the seven searched for, five were found. 51 By the fol-
lowing week, the government presented to Judge Brinkema a list of 43 improperly
produced documents. 72 Many of the documents were prepared by FBI agents
who were brought into September 11 investigations without sufficient training in
handling and labeling classified information. 53 Eventually, the documents were
retrieved and properly classified. 72

pledged allegiance to Osama Bin Laden are strong evidence that the national security could
be threatened if the defendant had access to classified information.

Id. at 2. See Liptak, supra note 703, Philip Shenon, U.S. Gave Secrets to Terror Suspect, N.Y.
Times, Oct. 27, 2002, at A1

Standing counsel, but not Moussaoui, also were granted access to “sensitive security in-
formation,” which is secret—but not classified—information related to transportation security. See 49
C.F.R. § 1520.5(a) (2011). Tom Jackman, Moussaoui’s Access to Documents Limited, Wash. Post,

ment Retrieval Unsealing Order, Moussaoui, No. 01-cr-455 (E.D. Va Sept. 26, 2002), available
at 2002 WL 32001771; Interview with Hon. Leonce M. Brinkema, Jan. 5, 2007, see Shenon, supra
note 746.

These documents [redacted] were inadvertently produced as unclassified documents, in elec-
tronic form, to defense counsel and Mr. Moussaoui on June 12, 2002 [redacted] and June 7,
2002 [redacted]. On July 29, 2002, in accordance with the Court’s order on hard-copy dis-
covery, a paper copy of these documents was delivered to Mr. Moussaoui.


750 Interview with Dep’t of Justice Litig. Sec. Group Staff, Feb. 3, 2010, see Letter (Aug. 29,
Order, supra note 747.

751 Interview with Hon. Leonce M. Brinkema, Jan. 5, 2007, see Aug. 29, 2002, Letter, supra
note 750; Shenon, supra note 746.

752 See Letter (Sept. 5, 2002), attached to Classified Document Retrieval Unsealing Order,
supra note 747; Shenon, supra note 746.

753 See Dan Eggen, FBI Failed to Classify Reports Before Moussaoui Had Them, Wash. Post,

754 Classified Document Retrieval Unsealing Order, supra note 747, at 1.

In part to accommodate the disruption to Moussaoui’s trial preparation caused
by the searches for improperly produced documents, Judge Brinkema pushed
back the trial date six months. 755

Challenge: Classified Arguments

Eastern District of Virginia

Moussaoui’s appointed standby attorneys had security clearances; to ensure that
they did not inadvertently put classified information into the public record, Judge
Brinkema established a procedure in which they submitted filings to the classified
information security officer, who was given 48 hours to identify any classified
information that had to be redacted from the public record. 756 These filings could
not be shared with Moussaoui, who did not have a security clearance, until they
had been reviewed by the security officer. 757 Unredacted filings containing class-
ified information were filed with the security officer rather than the clerk. 758 The
government was responsible for classification reviews of its filings. 759

Fourth Circuit

The court of appeals’ clerk’s office anticipated that it was likely to eventually re-
cieve an appeal in Moussaoui’s case, and classified information would be part of
the court record. 760 So the clerk’s office worked with the classified information
security officers to (1) create a sensitive compartmented information facility
(SCIF)—an especially secure storage facility suitable for storing sensitive comp-
artmented information and other classified information—and (2) begin the pro-
cess of obtaining security clearances for several staff members. 761

The court’s judges meet in regular session in Richmond six times a year. There
were safes in the court’s SCIF for the Moussaoui case, with separate drawers
allocated to each judge. 762 Cleared court staff members could bring classified
documents from the SCIF to judges’ Richmond chambers for review while the

755 Order Rescheduling Trial, United States v. Moussaoui, No. 01-cr-455 (E.D. Va Sept
30, 2002), available at 2002 WL 32001785; see Philip Shenon, Judge Agrees to New Delay in

756 Classified Filing Order, Moussaoui, No. 01-cr-455 (E.D. Va Oct. 3, 2002), see
Motions).

757 Classified Filing Order, supra note 755, at 2, see Moussaoui Motions, supra note 756.

758 Classified Filing Order, supra note 755, at 2–3.

759 Id. at 2; see Moussaoui Motions, supra note 756.

760 One 71-page government brief had 50 blank (redacted) pages, 15 partially redacted pages,
three full pages of text, and three head and end pages. Government Response Brief, Moussaoui,
No. 01-cr-455 (E.D. Va Jan. 13, 2003), see Pohlman, supra note 649, at 194.

761 Id.; Interview with Dep’t of Justice Litig. Sec. Group Staff, Feb. 3, 2010, see Robert
Timothy Reagan, Keeping Government Secrets: A Pocket Guide on the State-Secrets Privilege,
the Classified Information Procedures Act, and Classified Information Security Officers 22–23
(Federal Judicial Center, 2d ed. 2013) (describing SCIFs).

762 Interview with 4th Cir. Clerk’s Office Staff, Feb. 26, 2008, Interview with Dep’t of Jus-
judges were in Richmond.\textsuperscript{763} Judge Gregory’s home chambers are in Richmond, so cleared court staff members can bring him classified documents from the Richmond SCIF even when the court is not in session. Judge Gregory frequently visited the SCIF himself to retrieve documents.\textsuperscript{764} He observed that although it is convenient to have the documents stored near his chambers, he still must keep them within view at all times while they are out of the SCIF.\textsuperscript{765}

Judge Wilkins had chambers in Greenville, South Carolina, and the courthouse there has a SCIF.\textsuperscript{766} Judge Williams had chambers in Orangeburg, South Carolina, which is approximately 50 miles south of Columbia. Either classified information security officers brought classified documents to her chambers in Orangeburg for her review while they were there, or she traveled to Columbia, where the FBI has a SCIF.\textsuperscript{767} Judge Shedd’s chambers are in Columbia, so he can review files at the FBI SCIF there or at the court in Richmond during a session.\textsuperscript{768}

In the appeal of Judge Brinkema’s order that Moussaoui be permitted to depose Bin al-Shibh, the briefs were filed with the classified information security officer under seal.\textsuperscript{769} Some information about their contents, however, was reported in the \textit{Washington Post}.\textsuperscript{770} In the appeal of Judge Brinkema’s sanction for the government’s refusal to produce deponents for depositions, complete briefs were filed with the classified information security officer under seal and redacted briefs were filed in the public record.\textsuperscript{771}

While Moussaoui was proceeding pro se, he filed several documents with the court of appeals.\textsuperscript{772} Typically, the documents were construed as attempted appeals, which were reviewed and dismissed.\textsuperscript{773} Moussaoui would give a document for the court of appeals to the jail where he was detained, and the jail would pass it on to a classified information security officer who notified the court.\textsuperscript{774} The court docketed it as filed with the classified information security officer, who had it reviewed for classified information and then sent a redacted copy to the court for public filing.\textsuperscript{775} Sometimes the government’s response would be accompanied by instructions to cleared court staff members to do some of the redacting themselves.\textsuperscript{776}

For a petition to rehear en banc the ruling on Judge Brinkema’s discovery sanction, full briefs were filed in the court’s Richmond SCIF, and redacted copies were sent to each judge.\textsuperscript{777} Some judges opted to review the full briefs in Richmond, and some judges opted to rely on the redacted briefs.\textsuperscript{778} The court denied the petition.\textsuperscript{779}

The appeal of Moussaoui’s guilty plea also included classified briefing.\textsuperscript{780} Judge Gregory observed that the most difficult issue presented to an appellate judge by the presence of classified information in a case is the difficulty of obtaining law clerk assistance.\textsuperscript{781} Judge Gregory does not have a career law clerk, and security clearances take such a large fraction of a temporary law clerk’s tenure to acquire that he relies on a court of appeals staff attorney, who has a security clearance, to help him with matters involving classified information.\textsuperscript{782}

In August 2009, the court worked with the classified information security officer to establish a larger SCIF in Richmond, suitable for working and meeting in addition to storage.\textsuperscript{783}

\textbf{Challenge: Closed Proceedings}

Closed proceedings in district courts are not common, but they do occur, especially in cases involving classified information. Closed proceedings in appellate courts are more rare.\textsuperscript{784} All four oral arguments before the court of appeals included a public session and a closed session at which classified information could be discussed.\textsuperscript{785} At the public session, a classified information security officer and a CIA officer attended to monitor the proceeding in case it needed to be interrupted to prevent disclosure.

\textbf{Citation:}\n
\textsuperscript{763} Interview with 4th C\textsuperscript{r}. Clerk’s Office Staff, Feb. 26, 2008.

\textsuperscript{764} Interview with Hon. Roger L. Gregory, Sept. 25, 2009.

\textsuperscript{765} Id.


\textsuperscript{767} Interview with 4th C\textsuperscript{r}. Clerk’s Office Staff, Feb. 26, 2008.

\textsuperscript{768} Interview with Hon. Dennis W. Shedd, Sept. 3, 2009.

\textsuperscript{769} Docket Sheet, United States v. Moussaoui, No. 03-4162 (4th C\textsuperscript{r}. Feb. 12, 2003) [hereinafter 4th C\textsuperscript{r}. Clerk’s Office Staff, Feb. 26, 2008.

\textsuperscript{770} Interview with Hon. Dennis W. Shedd, Sept. 3, 2009.

\textsuperscript{771} Docket Sheet, United States v. Moussaoui, No. 03-4162 (4th C\textsuperscript{r}. Feb. 12, 2003) [hereinafter 4th C\textsuperscript{r}. Clerk’s Office Staff, Feb. 26, 2008.

\textsuperscript{772} Interview with 4th C\textsuperscript{r}. Clerk’s Office Staff, Feb. 26, 2008

\textsuperscript{773} Id.

\textsuperscript{774} Id.

\textsuperscript{775} Id.

\textsuperscript{776} Id.

\textsuperscript{777} Id.

\textsuperscript{778} Id.

\textsuperscript{779} 4th C\textsuperscript{r}. Clerk’s Office Staff, supra note 771, at 20 (noting the denial of rehearing on October 13, 2004).

\textsuperscript{780} 4th C\textsuperscript{r}. Clerk’s Office Staff, supra note 771, at 20 (noting the denial of rehearing on October 13, 2004).

\textsuperscript{781} 4th C\textsuperscript{r}. Clerk’s Office Staff, supra note 771, at 20 (noting the denial of rehearing on October 13, 2004).

\textsuperscript{782} Id.

\textsuperscript{783} Id.; Interview with 4th C\textsuperscript{r}. Clerk’s Office Staff, Feb. 26, 2008, and Sept. 1, 2009, Interview with Dep’t of Justice Litig. Sec. Group Staff, Feb. 3, 2010.

\textsuperscript{784} 4th C\textsuperscript{r}. Clerk’s Office Staff, supra note 771, at 20 (noting the denial of rehearing on October 13, 2004).

\textsuperscript{785} 4th C\textsuperscript{r}. Clerk’s Office Staff, supra note 771, at 20 (noting the denial of rehearing on October 13, 2004).

\textsuperscript{786} National Security Case Management Studies (06-25-2013)
of classified information. At these public sessions, no interruption was necessary.

In the appeal of Judge Brinkema’s order that Moussauoi be permitted to depose Bin al-Shihhi, a motion panel of the court of appeals initially granted the government’s motion to seal the oral argument. But on a motion by news media to hold the oral argument in open court, the panel that would ultimately hear the appeal decided to bifurcate the argument: a public oral argument was held followed by a closed oral argument concerning classified information. The closed proceeding was transcribed by Judge Brinkema’s court reporter, who had a security clearance. The court ordered that a redacted transcript of the closed argument be made available to the public within five business days of the court reporter’s submission of the transcript to the government, which was required within 24 hours of the argument. A redacted transcript of the closed arguments on Tuesday, June 3, 2003, was released to the public on Thursday, June 12.

Challenge: Classified Opinion

Many opinions issued by the district court and the court of appeals in this case were redacted. Judge Gregory observed that in the appeal of Judge Brinkema’s discovery sanction the majority’s opinion and Judge Gregory’s separate opinion came back from the redaction process looking like Swiss cheese. In the opinion issued by the court, redactions appear as white space equal in size to the amount of text redacted; in West’s published version, the expression “[Redacted]” replaces redacted text, regardless of quantity.

Challenge: Terrorist Communications

Once Moussauoi declared in court that he wished to proceed pro se, he began to file with the court handwritten documents that the court regarded as motions. The court initially filled these documents under seal. On a Friday, the day after the court granted Moussauoi’s request to proceed pro se, Judge Brinkema ordered Moussauoi’s filings served on the government, which was required to advise the court by Monday morning whether it objected to the unsealing of the filings. The government announced that it did not object to the unsealing, so Judge Brinkema ordered the filings unsealed and ordered future pro se filings sealed only until 4:00 p.m. on the workday following the filing to provide the government with an opportunity to object.

Two months later, the government expressed concern that Moussauoi’s filings might include coded messages to confederates. Judge Brinkema determined that Moussauoi’s filings included improper material.

The defendant’s pleadings have been replete with irrelevant, inflammatory and insulting rhetoric, which would not be tolerated from an attorney practicing in this court. Because he has been warned numerous times that such writing would have to stop, the defendant may no longer hide behind his pro se status to avoid being held to appropriate pleading practice. Further, we find that the record supports the United States’ concern that the defendant, who is charged with conspiracy to commit acts of terrorism transcending national boundaries among other offenses, is attempting to use the court as a vehicle through which to communicate with the outside world in violation of the Special Administrative Measures governing the conditions of his confinement.

Judge Brinkema ordered that “any future pleadings filed by the defendant, pro se, containing threats, racial slurs, calls to action, or other irrelevant and inappropriate language will be filed and maintained under seal.” She sealed several, but not all, recent filings. She declined Moussauoi’s suggestion that the court engage in the burdensome task of redacting inappropriate language from the filings instead of sealing them. “If he desires his pleadings to be publicly filed, the defendant must limit his writings to appropriate requests for relevant judicial relief.”

On motion from news media, and after observing that “the defendant has filed fewer pleadings and has significantly toned down his inappropriate rhetoric,” Judge Brinkema modified her order so that all pro se filings would be sealed for ten days to give the government an opportunity “to advise the Court in writing whether the pleading should remain under seal or be unsealed with or without redactions.”

785 Interview with Dep’t of Justice Litig. Sec. Group Staff, Sept. 28, 2009.
790 Moussauoi, 65 F. App’x 881.
792 Interview with Hon. Roger L. Gregory, Sept. 25, 2009, see United States v. Moussauoi, 382 F.3d 455 (4th Cir. 2004).
794 Pro Se Order, supra note 728, at 1.
The Court will also conduct its own review of the defendant’s pro se pleadings, and will redact any insulting, threatening or inflammatory language which would not be tolerated from an attorney practicing in this court. Should the defendant’s pleadings again become replete with inappropriate rhetoric, we will return to categorical sealing. 805

Moussaoui was granted access to a videotape of an Al-Jazeera interview with the captured Bin al-Shibh, but the tape produced apparently was blank. 803 Judge Brinkema ordered the “inexcusable error” corrected immediately, but also ordered Moussaoui’s motion to correct the error to remain under total seal, because it was “replete with irrelevant and inflammatory rhetoric, including messages to third parties and a prayer for the destruction of the United States.” 804

American Taliban
United States v. Lindh (T.S. Ellis III, E.D. Va.)

On November 25, 2001, at the Qala-i-Jhangi prison near Mazar-e-Sharif, Afghani-

stan, CIA officer Johnny “Mike” Spann interviewed a captured Taliban fighter who was an American citizen: John Phillip Walker Lindh. 807 Spann became the first American casualty of the war in Afghanistan when he was killed in a prisoner uprising later that day. 807 Lindh 808 was shot in the upper thigh during the uprising, and he denied involvement in Spann’s death. 809 Lindh and several dozen other surviving Taliban troops were recaptured on December 1 when the Northern Alliance flooded them out of a basement. 801 Lindh was charged in a criminal complaint filed on January 15, 2002, with conspiracy to kill American citizens and with providing support to terrorists, including Al-Qaeda. 811 He arrived in the Eastern District of Virginia for trial eight days later. 812 An indictment filed on February 5 added related charges as well as a

803 Sept. 27, 2002, Pro Se Filings Sealing Order, supra note 802, at n.1.
805 Videotape Production Order, supra note 804

National Security Case Management Studies (06-25-2013)
firearms charge. The court assigned the case to Judge T.S. Ellis III. Lindh pleaded not guilty on February 13. Judge Ellis denied Lindh’s motion to transfer the case to a district that did not include so many persons directly affected by the September 11, 2001, terrorist attacks.

Lindh was born in February 1981 in the District of Columbia as the second of three children born to Marilyn Walker and Frank Lindh, who subsequently moved the family to California and ultimately separated. John Walker Lindh was raised a Catholic, but he decided to convert to Islam at 16, taking the name Suleyman. At 18, he moved to Yemen to study Arabic, and then he moved to Bannu, Pakistan, to attend a madrasa.

Adopting the name Abdul Hamid, he reportedly volunteered to fight with the Taliban, because he did not know Pashto or Urdu, the local languages, he was assigned to fight with troops financed by Osama Bin Laden. He arrived on the Taliban’s front line on September 6, 2001.

Tim Reagan interviewed Judge Ellis for this report in the judge’s chambers on September 5, 2007.

A photo taken during Lindh’s captivity showed him naked and blindfolded, strapped to a stretcher. Another photo showed American soldiers posing with a handcuffed and blindfolded Lindh, an obscenity written across the blindfold. Other photos apparently were destroyed.

Lindh’s parents hired prominent San Francisco attorney James Brosnahan to defend him. To protect Brosnahan’s law firm’s employees from harm, Brosnahan kept the firm’s name off of the case.

Spann’s family attended Lindh’s plea hearing, telling reporters that they blamed Lindh for Spann’s death. But the government acknowledged at a hearing two months later that there was no evidence that Lindh killed or shot at any American citizen, including Spann.

On July 15, 2002, Lindh pleaded guilty to the felony of fighting for the Taliban. All other charges were dropped, and Lindh pleaded guilty to a new charge of carrying grenades while committing a felony. On October 4, Judge Ellis imposed the statutory maximum of consecutive ten-year terms on each charge, a sentence to which the parties had agreed. Lindh tearfully admitted making a mistake by joining the Taliban. Judge Ellis gave Lindh credit for time served, beginning December 1, 2001.

**Challenge: Protected National Security Information**

Early in the prosecution, the government determined that it had to disclose to the defendant “reports of interviews of detainees captured in Afghanistan and elsewhere who may have knowledge of al Qaeda or who may have been members of


815 E.D. Va. Docket Sheet, supra note 811; see Masters, supra note 814.


817 See Heffelfinger, supra note 806, at xii-xv; Kunkle, supra note 806; Loeb, supra note 810, Evelyn Nieves, A U.S. Convert’s Path from Suburbania to a Gory Jail for Taliban, N.Y. Times, Dec. 4, 2001, at B1; Romero & Temple-Raston, supra note 807, at 13, 15, Sanchez, supra note 807.

818 See Eggen & Masters, supra note 806 (reporting that Lindh took the name Suleyman al-Farsi); Heffelfinger, supra note 806, at xvi-xvii ("He asked that the name on his [high-school] diploma be changed to Suleyman al-Lindh, though he never picked it up"); Kunkle, supra note 806; Loeb, supra note 810; Nieves, supra note 817 (reporting that Lindh took the name Suleyman al-Lindh); Romero & Temple-Raston, supra note 807, at 16 (reporting that “Suleyman” is equivalent to “Solomon”); Sanchez, supra note 807.

819 See Eggen & Masters, supra note 806, Heffelfinger, supra note 806, at xvi-xvii, Loeb, supra note 810; Romero & Temple-Raston, supra note 807, at 17-19 (reporting that the Lindh determined that Yemen was the best place in the world to learn classical Arabic); Sanchez, supra note 807.

820 See Eggen & Masters, supra note 806, Loeb, supra note 810; Nieves, supra note 817; Romero & Temple-Raston, supra note 807, at 22-23, 138 (reporting that Lindh undertook military training to fight the Northern Alliance, not Al-Qaeda training, which was to fight civilians); Sanchez, supra note 807.

821 See Heffelfinger, supra note 806, at xiii, Romero & Temple-Raston, supra note 807, at 24.

822 See Brooke A. Masters, U.S. Soldiers Posed with Bound Lindh, Wash. Post, Apr. 13, 2002, at A5; Romero & Temple-Raston, supra note 807, at 111 & fig. 5.

823 See Masters, supra note 822; Romero & Temple-Raston, supra note 807, at 114 (reporting that the obscenity was “sh t head”).

824 See Masters, supra note 822; Romero & Temple-Raston, supra note 807, at 114.

825 See Eggen & Masters, supra note 806; Romero & Temple-Raston, supra note 807, at 94, 111-14, 136-37.


827 See Masters, supra note 814; Romero & Temple-Raston, supra note 807, at 140-41 (reporting that the government brought Spann’s family to the courthouse.


829 United States v. Lindh, 227 F. Supp. 2d 565, 566 (E.D. Va. 2002); E.D. Va. Docket Sheet, supra note 811; see Jackman, supra note 807, Kunkle, supra note 806; Neil A. Lewis, Admiring the Fugitive from Taliban, American Agrees to 20-Year Term, N.Y. Times, July 16, 2002; Romero & Temple-Raston, supra note 807, at 188.

830 Lindh, 227 F. Supp. 2d at 566, see Jackman, supra note 807, Lewis, supra note 829.


832 See Apologistic Lindh, supra note 831; Romero & Temple-Raston, supra note 807, at 189.

833 Lindh, 227 F. Supp. 2d at 572, see http://www.bop.gov (noting a release date of May 23, 2019, reg. no. 45426-083).
that organization and who are housed primarily at Guantanamo Bay, Cuba.\textsuperscript{834} The reports were regarded as "unclassified information vital to national security."\textsuperscript{835} The government submitted to the court ex parte and in camera both an unredacted set of reports and a set with proposed redactions, omitting agent and case identifiers and information concerning other detainees not relevant to the defense.\textsuperscript{836}

Judge Ellis granted the government’s motion for a protective order.\textsuperscript{837}

[Given the nature of al Qaeda and its activities, and the ongoing federal law enforcement investigation into al Qaeda, the identities of the detainees, as well as the questions asked and the techniques employed by law enforcement agents in the interviews are highly sensitive and confidential. Additionally, the intelligence information gathered in the course of the detainee interviews may be of critical importance to national security, as detainees may reveal information leading to the identification and apprehension of other terrorist suspects and the prevention of additional terrorist acts. Thus, a protective order prohibiting the public dissemination of the detainee interview reports will, in this case, serve to prevent members of international terrorist organizations, including al Qaeda, from learning, from publicly available sources, the status of, the methods used in, and the information obtained from the ongoing investigation of the detainees.]

Judge Ellis rejected the government’s proposal that defense investigators and expert witnesses be pre-screened before information contained in the redacted reports could be disclosed to them.\textsuperscript{838} Judge Ellis determined that having investigators and witnesses sign a memorandum of understanding would suffice.\textsuperscript{839}

By signing such a memorandum of understanding, a defense investigator or expert would declare under penalty of perjury under the laws of the United States that she or he had (i) read and understood the protective order pertaining to these unclassified documents and materials and (ii) agreed to be bound by the terms of the protective order, which would remain binding during, and after the conclusion of these proceedings.\textsuperscript{840}

On motion, and without objection from the defendant, Judge Ellis subsequently modified the protective order to require of persons seeing the reports a "brief, basic background investigation, performed by law enforcement personnel independent of the prosecution team and reporting directly to the Court through the Court Security Officer."\textsuperscript{841}

Judge Ellis determined that showing the reports to a detainee witness, however, would additionally require notice to the government and court approval "to assure that the Court is fully apprised of the risks attendant to disclosure of unclassified protected information to a specific detainee."\textsuperscript{842}

**Challenge: Classified Evidence**

In order to determine what evidence the government had to produce to the defendant, Judge Ellis had to review a substantial amount of classified material.\textsuperscript{843} It was stored in the court’s sensitive compartmented information facility (SCIF).\textsuperscript{844}

Judge Ellis’s career law clerk has a top-secret security clearance, so she can assist the judge with reviews of classified information.\textsuperscript{845} The chambers has a rule requiring classified documents to be within eyesight at all times.\textsuperscript{846} Even a law clerk’s brief trip outside chambers requires taking the classified documents securely along.\textsuperscript{847} But classified materials are never taken home.\textsuperscript{848}

**Challenge: Interviewing Guantánamo Bay Detainees**

Defense counsel sought to interview Guantánamo Bay detainees.\textsuperscript{849} Judge Ellis denied counsel face-to-face access to the detainees, but established a procedure allowing counsel to submit questions to "firewall" attorneys, who passed them on to the detainees.\textsuperscript{850}

Firewall attorneys included attorneys from the Department of Justice and the Department of Defense "who are separate and independent from the attorneys who represent the government" in the case, including two assistant U.S. attorneys from another district.\textsuperscript{851}

Defense counsel submitted questions for each detainee to the firewall attorneys.\textsuperscript{852} The firewall attorneys could object to any questions, and the court would

---

\textsuperscript{835} Id. at 742.
\textsuperscript{836} Id. at 2.
\textsuperscript{837} Later in the case, Judge Ellis agreed with the government that a set of additional detainee reports did not need to be disclosed to the defense. United States v. Lindh, No. 1:02-cr-37, 2002 WL 1974284 (E.D. Va. June 17, 2002).
\textsuperscript{838} Lindh, 198 F. Supp. 2d at 744.
\textsuperscript{839} Id. at 742.
\textsuperscript{840} Id. at 742–43, see id. at 743 (noting that the “defendant will be at liberty to disclose information from the redacted interview reports to investigators and expert witnesses who are not pre-screened by, or known to, the government”).
\textsuperscript{841} Id. at 742–43.
\textsuperscript{842} United States v. Lindh, No. 1:02-cr-37, 2002 WL 1974184 (E.D. Va. May 6, 2002).
\textsuperscript{843} This type of court security officer is now known as a classified information security officer. See Robert Timothy Reagan, Keeping Government Secrets: A Pocket Guide on the State-Secrets Privilege, the Classified Information Procedures Act, and Classified Information Security Officers 21–22 (Federal Judicial Center, 2d ed. 2013).
\textsuperscript{844} Lindh, 198 F. Supp. 2d at 743.
\textsuperscript{845} Interviews with Hon. T.S. Ellis III, Sept. 5, 2007.
\textsuperscript{846} Id.; see Reagan, supra note 842, at 22–23 (describing SCIFs).
\textsuperscript{847} Interview with Hon. T.S. Ellis III, Sept. 5, 2007.
\textsuperscript{848} Id.
\textsuperscript{849} Id.
\textsuperscript{851} Justice Department prosecutors felt the Pentagon nearly had sabotaged the cases of Lindh and Zacarias Moussaoui by blocking access to Guantánamo detainees who were potential witnesses. The Defense Department would not acknowledge any summons from a federal court directed to Guantánamo:” Bravo!, supra note 812, at 121.
\textsuperscript{852} Lindh, 2002 WL 1298601, at *1–2, Interview with Hon. T.S. Ellis III, Sept. 5, 2007; see Masters, supra note 809.
\textsuperscript{853} Lindh, 2002 WL 1298601, at *1 & n.1.
\textsuperscript{854} Id. at *1.
resolve any objections on sealed noticed filings. Approved questions were submitted to interrogators who interwove the questions into the interrogations. Soon thereafter, the firewall attorneys prepared written summaries, and defense counsel could submit follow-up questions. Soon thereafter, the firewall attorneys submitted to defense counsel video recordings of the interviews.

Judge Ellis monitored the procedure to ensure that it protected Lindh’s rights to a defense.

**Challenge: Witness Security**

Lindh pleaded guilty on a day the court was prepared to take testimony from a covert agent in a hearing on Lindh’s motion to suppress his confession. To protect the witness by shielding the witness’s identity, Judge Ellis worked with the classified information security officers and the Marshal Service to make adjustments to the courtroom. The courtroom was outfitted with special draperies and screens. The witness box was shielded from the public, as was the path to the door through which prisoners often are brought—a door that would be used in this case for the witness.

The plan was for the defendant and his counsel to sit in the jury box so that they could see the witness, but the draperies shielded the witness from the public’s view. The courtroom was equipped with an electronic device that would distort the witness’s voice, but the words would be audible to the parties and the public.

---

854 Id.
855 Id.
856 Id.
857 Id.
858 Id.; see Masters, supra note 809.
859 Interview with Hon. T.S. Ellis III, Sept. 5, 2007, see Jackman, supra note 807; Lewis, supra note 829; Romero & Temple-Raston, supra note 807, at 188, 192 (reporting that a condition of the plea agreement was that Lindh accept the agreement before the suppression hearing).
862 United States v. Rosen, 520 F. Supp. 2d 786, 795 n.15 (E.D. Va. 2007) (“the court indicated that it would allow a clandestine government intelligence agent to appear at an evidentiary hearing under an assumed name, and the courtroom would be arranged in such a way that the government, the defendant and defense counsel would see and confront the agent, while others in the courtroom would be able to [hear], but not [see] the agent.”), Interview with Hon. T.S. Ellis III, Sept. 5, 2007.

---

875 Scheduling Order, id. (June 21, 2013).
Dirty Bomber

Jose Padilla was born in Brooklyn to Puerto Rican parents. On May 8, 2002, upon his landing at O'Hare International Airport in Chicago on a trip from Pakistan, federal authorities arrested him on a material witness warrant arising from a grand jury investigation of the September 11, 2001, attacks. Padilla was flown to Manhattan for detention and possible grand jury testimony.

On June 10, at a press conference in Russia, Attorney General John Ashcroft announced that the government was holding in custody an enemy combatant who had been apprehended at O'Hare on suspicion of planning to build and detonate a “dirty bomb,” which is a bomb made up of radioactive material and conventional explosives. The detainee was Padilla, and the government had transferred him the previous day to the high-security Consolidated Naval Brig in Charleston, South Carolina. As a result of this transfer, Padilla was denied access to counsel.

Padilla had been scheduled to appear on June 11 before the Southern District of New York's chief judge Michael B. Mukasey for a hearing on his motion to vacate the material witness warrant. A material witness warrant may not be used simply as a substitute for indefinite detention. When it was clear Padilla would not testify against his cohorts, he was transferred on order of the President to military custody as an unlawful combatant.

As a result of Padilla's change in status from material witness to enemy combatant, the government vacated the warrant. Padilla's attorney filed a habeas corpus petition on his behalf. Judge Mukasey ruled that she had standing to do so.


879. Padilla, 233 F. Supp. 2d at 572–73, see Padilla, 678 F.3d at 751, Eggen & Schmidt, supra note 876, Hafetz, supra note 877, at 47, Herzog, supra note 877, Newman, What the F—, supra note 877, at 362, Rosen & Shenon, supra note 876, US Announces Arrest of Alleged Al-Qaeda Terrorist, Morning Edition (NPR radio broadcast June 10, 2002), see also Soufan, supra note 877, at 408 (reporting that the Attorney General was misinformed. "While Padilla was a committed terrorist set on trying to harm America, he was a brain transplant away from making a bomb, and there was no unfolding plot."); Clive Stafford Smith, Eight O'Clock Ferry to the Windward Side 49–50 (2007) (arguing that the allaged dirty bomb plot was "almost certainly a fantasy"). But see Terry McDermott & Josh Meyer, The Hunt for KSM 144 (2012) (reporting that Khalid Sheikh Mohammed "sent José Padilla, the hapless American son of Puerto Rican immigrants, back to the United States to research the possibility of building a dirty bomb and blowing up apartment buildings after filling them with gas."); id. at 187.

880. Padilla, 542 U.S. at 431–32, Padilla, 678 F.3d at 751, Lebron, 670 F.3d at 545, Padilla, 423 F.3d at 390; Padilla, 552 F.3d at 700, Padilla, 233 F. Supp. 2d at 569, see Eggen & Schmidt, supra note 876, Gibbons, supra note 877, at 304–05, Pohman, supra note 877, at 76–77, Rosen & Shenon, supra note 876.

881. Padilla, 678 F.3d at 751, Padilla, 233 F. Supp. 2d at 574, see Newman, Modern Day Struggle, supra note 877, at 336.

882. Padilla, 352 F.3d at 700, Padilla, 233 F. Supp. 2d at 571, see Eggen & Schmidt, supra note 876, Gibbons, supra note 877, at 304–05, Rosen & Shenon, supra note 876, see also Soufan, supra note 877, at 408 (noting that Judge Mukasey had signed the warrant).

Judge Mukasey had appointed counsel to represent Padilla in his material witness case. In May 2002, it seemed that the smell of the debris and smoke from the demise of the Twin Towers had just cleared. I received a call from the courtroom deputy to the Honorable Michael B. Mukasey, then chief judge of the U.S. District Court for the Southern District of New York. He asked me to appear in court the following week for an assignment representing a grand jury material witness who was being held in connection with the grand jury sitting to investigate 9/11.
that as Padilla’s next friend and denied the government’s motion to transfer the habeas case to the District of South Carolina.

Judge Mukasey ruled that the President had the power to detain Padilla as an enemy combatant, but he also ruled that Padilla had a right to consult counsel and pursue a habeas corpus petition challenging the grounds for the detention. The government would have to show only “some evidence” to support its determination that Padilla was an enemy combatant. On reconsideration, Judge Mukasey upheld his original ruling on access to counsel. At the government’s request, a month later, Judge Mukasey certified the issue for interlocutory appeal.

Over the dissent of Judge Richard C. Wesley, Judges Rosemary S. Pooler and Barrington D. Parker, Jr., determined Padilla’s detention to be unlawful: “Padilla’s detention was not authorized by Congress, and absent such authorization, the President does not have the power under Article II of the Constitution to detain as an enemy combatant an American citizen seized on American soil outside a zone of combat.” The court ordered Padilla released from military custody, and the court acknowledged that he could be held as a material witness or for criminal prosecution.

On June 28, 2004, the Supreme Court reversed, holding that Padilla should have brought his habeas corpus petition in the District of South Carolina, where he was held. On the same day, however, the court held that former nationals apprehended abroad and held at the Guantanamo Bay Naval Base in Cuba could challenge their detention through habeas corpus.

The court resolved a third case that day: a habeas corpus petition by Yaser Hamdi, who, like Padilla, was an American citizen held as an enemy combatant in a naval brig. But Hamdi was apprehended in Afghanistan. No opinion was endorsed by a majority of the court, but only Justice Thomas thought that Hamdi could be detained indefinitely without a meaningful opportunity to contest the factual basis for that detention before a neutral decisionmaker.

Approximately four weeks before the Supreme Court issued its opinion in Padilla’s case, the government released newly declassified information on Padilla. It was reported that Padilla admitted to attending a terrorist training camp, but his interest in a dirty bomb plot was only a ruse to avoid combat in Afghanistan.

On July 2, 2004, Padilla’s New York attorney filed a habeas corpus petition on his behalf in the District of South Carolina. The court assigned the case to Judge Henry F. Floyd. On February 28, 2005, Judge Floyd declared Padilla’s


887 Padilla, 233 F. Supp. 2d at 569, 578–79, 610, see Pohlman, supra note 877, at 84–85; Weiser, supra note 886.


889 Padilla, 233 F. Supp. 2d at 570, 605–10; see Pohlman, supra note 877, at 85; Weiser, supra note 886.


894 Padilla, 352 F.3d at 699, 724.

On June 28, 2004, the Supreme Court reversed, holding that Padilla should have brought his habeas corpus petition in the District of South Carolina, where he was held. On the same day, however, the court held that former nationals apprehended abroad and held at the Guantanamo Bay Naval Base in Cuba could challenge their detention through habeas corpus.

The court resolved a third case that day: a habeas corpus petition by Yaser Hamdi, who, like Padilla, was an American citizen held as an enemy combatant in a naval brig. But Hamdi was apprehended in Afghanistan. No opinion was endorsed by a majority of the court, but only Justice Thomas thought that Hamdi could be detained indefinitely without a meaningful opportunity to contest the factual basis for that detention before a neutral decisionmaker.

Approximately four weeks before the Supreme Court issued its opinion in Padilla’s case, the government released newly declassified information on Padilla. It was reported that Padilla admitted to attending a terrorist training camp, but his interest in a dirty bomb plot was only a ruse to avoid combat in Afghanistan.

On July 2, 2004, Padilla’s New York attorney filed a habeas corpus petition on his behalf in the District of South Carolina. The court assigned the case to Judge Henry F. Floyd. On February 28, 2005, Judge Floyd declared Padilla’s
military detention improper. On September 9, a unanimous panel of the U.S. Court of Appeals for the Fourth Circuit reversed, determining that the 2001 Authorization for Use of Military Force Joint Resolution gave the President the authority to indefinitely detain even U.S. citizens as enemy combatants.

While Padilla’s petition to the Supreme Court for a writ of certiorari was pending, on November 17, 2005, the government indicted him in the Southern District of Florida, adding him to a terrorism conspiracy case pending for nearly two years against four other defendants. The case had been assigned to Judge Marcia G. Cooke.

For this report, Tim Reagan interviewed Judge Floyd, his law clerks Jeff Brown and Chase Samples, and the judge’s judicial assistant Cindy Chapman on November 19, 2009, in Spartanburg, South Carolina, where Judge Floyd has his chambers.


The court of appeals denied the government’s motion to transfer Padilla to civilian authority in Florida. A short time after our decision issued on the government’s representation that Padilla’s military custody was indeed necessary in the interest of national security, the government determined that it was no longer necessary that Padilla be held militarily. Instead, it announced, Padilla would be transferred to the custody of federal civilian law enforcement authorities and criminally prosecuted in Florida for alleged offenses considerably different from, and less serious than, those acts for which the government had militarily detained Padilla.

The Supreme Court, however, granted the government’s request to transfer Padilla. In light of Padilla’s removal from military detention, the court later denied his petition for a writ of certiorari.

First indicted on January 8, 2004, Adham Amin Hassoun was a Lebanese-born Palestinian charged with raising money and recruiting persons for jihad training. He and Padilla became friends when they both attended a Fort Lauderdale mosque in the 1990s. Added by superseding indictment on September 16, 2004, Mohamed Hesham Youssef was charged as one of Hassoun’s recruiters; he was in custody in Egypt on other charges. Kifah Wael Jayyousi and Kassem Daher were named in a sealed material support complaint filed on December 1, 2004. The complaint was unsealed on March 30, 2005, when Jayyousi was apprehended in Detroit on his return from Qatar. Jayyousi was born in Jordan. Daher was a Canadian citizen in overseas custody.
and Daher were added to the pending indictment on April 7, 2005.\textsuperscript{920} Yousef and Daher remain fugitives.\textsuperscript{921}

Even after Padilla was added to the indictment, there was no charge pertaining to a dirty bomb.\textsuperscript{922} The dirty bomb issue never arose at all in the case.\textsuperscript{923} But there was the following allegation: “On or about July 24, 2000, Padilla filled out a ‘Musjahideen Data Form’ in preparation for violent jihad training in Afghanistan.”\textsuperscript{924}

The government claimed that it was found in Afghanistan among dozens of other applications late in 2001.

Hassoun and Jayyousi, the only two defendants in local custody, were held in solitary confinement because they were terrorism suspects; they complained of improper detention practices: not being permitted family visits on weekends when family members did not have to work; not being permitted family visits in the evenings, which meant that out-of-town family members had to pay for overnight lodging; not being permitted long-distance telephone calls to family members at times when the family members would be awake, severe mail delays; and various inconveniences in meetings with attorneys.\textsuperscript{925} Judge Cooke denied the defendants’ motion to be relieved of solitary confinement, but she said she would “hold the government’s feet to the fire.”\textsuperscript{926}

A few months later, deciding that he was not a flight risk, Judge Cooke granted Jayyousi’s request for bail, setting the bond at $1.3 million and imposing electronic monitoring.\textsuperscript{927}

On August 18, 2006, Judge Cooke dismissed the first count of the 11-count indictment—a charge that the defendants conspired to murder, kidnap, and main persons in a foreign country—as impermissibly multiplicitous of other counts.\textsuperscript{928}

The court of appeals reversed.\textsuperscript{929}

On January 4, 2007, the New York Times printed a front-page story based in part on discovery that Padilla’s attorneys improperly provided to the newspaper.

Tens of thousands of conversations were recorded. Some 230 phone calls from the core of the government’s case, including 21 that make reference to Mr. Padilla, prosecutors said. But Mr. Padilla’s voice is heard on only seven calls. And on those seven, which were obtained from a participant in the case, Mr. Padilla does not discuss violent plots.\textsuperscript{930}

Padilla’s attorneys said that the error resulted from a person in the federal defender’s office not understanding the operable protective order, and Judge Cooke reprimanded the attorneys.\textsuperscript{931}

Jury selection began on April 16, 2007.\textsuperscript{932} Judge Cooke had decided that the court should send out 3,000 jury duty letters for the trial.\textsuperscript{933} Jurors were selected from a pool of approximately 300.\textsuperscript{934} Voire dire lasted four weeks.\textsuperscript{935} Judge Cooke decided to use a jury questionnaire.\textsuperscript{936} On May 8, 2007, the jury was selected from a culled pool of 88 potential jurors.\textsuperscript{937}

After about three weeks of testimony, it was discovered that one of the jurors was not a U.S. citizen.\textsuperscript{938} The jury summons was meant for his son, who had the same name.\textsuperscript{939} Another juror was excused because of injuries suffered when he tried to prevent a break-in of his daughter’s car.\textsuperscript{940} Another juror’s sister died, but she asked only for an early dismissal on Friday so that she could attend a memorial service in North Carolina on Saturday.\textsuperscript{941}

\textsuperscript{920} Nov. 17, 2005, Indictment, supra note 907, see Jack Dolan, Third Suspect Faces Terror Charges, Miami Herald, Apr. 9, 2005, at 4B.


\textsuperscript{922} See Padilla v. Yoo, 678 F.3d 748, 751 (9th Cir. 2012), see also Polhill, supra note 877, at 133, Weaver, supra note 907.

\textsuperscript{923} Trying Cases, supra note 907, at 7 (remarks by Judge Cooke), Interview with Hon. Marcia G. Cooke, Oct. 8, 2009.

\textsuperscript{924} Nov. 17, 2005, Indictment, supra note 907, see Jayyousi, 657 F.3d at 1093, Weaver, supra note 911.

\textsuperscript{925} See Jay Weaver, We Found at Qaeda Inquiry, U.S. Says, Miami Herald, Jan. 13, 2006, at 2B, see also Jayyousi, 657 F.3d at 1093.

\textsuperscript{926} Joint Motion, Hassoun, No. 0:04-cr-60001 (S.D. Fla. June 15, 2005) [hereinafter Joint Motion], see Jay Weaver, Two Men Claim Prison Abuse, Miami Herald, June 18, 2005, at 1B.

\textsuperscript{927} Order, Hassoun, No. 0:04-cr-60001 (S.D. Fla. Sept. 21, 2005) [hereinafter Order], see Jay Weaver, Judge Bars Confine of Two Terror Suspects, Miami Herald, Sept. 17, 2005, at 1B.

\textsuperscript{928} Order, Hassoun, No. 0:04-cr-60001 (S.D. Fla. Jan. 25, 2006), see Weaver, supra note 911.
The jury convicted all three defendants on August 16, 2007, one day after beginning deliberations. On January 22, 2008, Judge Cooke sentenced Padilla to 17 years and four months, Hashioun 15 years and eight months, and Javyssu to 12 years and eight months. The court of appeals, over a dissent, affirmed the convictions but remanded Padilla’s case for a harsher sentence.

During his criminal prosecution in Florida, Padilla filed civil suits challenging his conditions of confinement while designated an enemy combatant. On February 17, 2011, Judge Richard Mark Gergel dismissed a 2007 action for nominal damages that Padilla and his mother filed in the District of South Carolina against the government. The court originally assigned the action to Judge Floyd, but the action was transferred to Judge Gergel when he joined the bench. The court of appeals affirmed on January 23, 2012. The designations of persons and groups as special threats to national security may be subject to a variety of checks and to habeas corpus proceedings. But they are not reviewable by the judiciary by means of implied civil actions for money damages.

On January 4, 2008, Padilla and his mother filed an action against Boalt Hall law professor John Yoo, claiming that mistreatment of Padilla while in custody resulted from improperly drafted legal opinions that Yoo wrote when he worked for the Justice Department’s Office of Legal Counsel. The court assigned the case to Judge Jeffrey S. White, who denied Yoo’s motion to dismiss. The court of appeals, however, determined that Professor Yoo was entitled to qualified immunity, because the rights of suspected terrorists held in military detention as enemy combatants were not beyond debate, and it was not clearly established at the time that Padilla’s treatment qualified as torture.

Challenges: Attorney–Client Contacts

Padilla was transferred from New York to South Carolina without notice to his attorney. Once Padilla was designated an enemy combatant, the government denied him access to counsel, arguing that access to counsel would interfere with Padilla’s interrogation and that Padilla might use contacts with counsel to communicate with other terrorists. Judge Mukasey ruled this restriction improper.

A[access to counsel need be granted only for purposes of present facts to the court in connection with this petition if Padilla wishes to do so, no general right to counsel in connection with questioning has been hypothesized here, and thus the interference with interrogation would be minimal or nonexistent.]

Judge Mukasey characterized concerns about using the attorney as a communication conduit to terrorists “gossamer speculation.” There is no reason that military personnel cannot monitor Padilla’s contacts with counsel, so long as those who participate in the monitoring are insulated from any activity in connection with this petition, or in connection with a future criminal prosecution of Padilla, if there should ever be one.” Further, there is nothing to suggest that a member of the court’s Criminal Justice Act panel, such as Padilla’s attorney, “would ever be inclined to act as conduits for their client, even if he wanted them to do so.”

---


944. See Jay Weaver, Padilla Codefendant Tries to Kill Himself, Miami Herald, Dec. 4, 2007, at B3.


946. Jayouso, 657 F. 3d at 1119–20 (opinion by Judge Joel F. Dubina, joined by Judge William H. Pryor, Jr.), cert. denied, ___ U.S. ___, 133 S. Ct. 29 (petition by Padilla), ___ U.S. ___, 133 S. Ct. 29 (petition by Hafsoun), and ___ U.S. ___, 133 S. Ct. 29 (2012 petition by Jayouso), see Jayouso, 657 F. 3d at 1119–35 (dissenting opinion by Judge Rosemary Barkett, who would have suppressed Padilla’s statements before he was read his Miranda rights, who would have suppressed lay opinion testimony, and who determined that Padilla’s sentence was reasonable), see also Padilla, 678 F.3d at 751; Lizette Alvarez, Sentence for Terrorist Is Too Short, Court Rules, N.Y. Times, Sept. 20, 2011, at A12, see also http://www.bnpa.gov (noting release dates of September 15, 2011, for Jayouso, reg. no. 39551-039, and October 10, 2011, for Hafsoun, reg. no. 39553-004).


Unwilling to allow Padilla access to counsel, the government filed a motion to reconsider, violating local rules by filing the motion late and submitting a supporting affidavit without leave of court. The government argued that access to counsel would interfere with the psychological pressure on Padilla employed as part of the interrogation process and access to counsel was furthermore unnecessary because the court could rely on the government’s evidence alone to decide Padilla’s habeas corpus petition. Judge Mukasey was not persuaded.

Because the court of appeals ordered Padilla released, it did not reach the issue of his right to counsel, and the government continued to deny him counsel access until his case was pending before the Supreme Court, at which time the government argued that that legal issue was moot.

In Florida, Hassoun and Jayyousi complained of insufficient access to counsel; Judge Cooke ordered that they be permitted two 15-minute telephone calls with their attorneys each week. During these legal telephone calls the [Federal Detention Center] officials shall stay a reasonable distance away from the Defendant to allow for sufficient privacy. As trial approached, Judge Cooke ordered the detention center to provide a bigger conference table for meetings between the defendants and their attorneys.

**Challenge: Mental Health During Detention**

One month before the scheduled commencement of trial, Padilla’s attorneys filed a motion to determine whether their client was competent to stand trial. “He appears to be incapacitated by post traumatic stress disorder, stemming from the circumstances surrounding his time at the Naval Brig and, as a result of this incapacitation, is unable to assist his attorneys by providing relevant information to his defense.”

Special administrative measures for Padilla’s detention (SAMS) made his psychiatric evaluation difficult, so Judge Cooke had the evaluation conducted in her courtroom. Judge Cooke was not present for the evaluation.

Judge Cooke found Padilla competent to stand trial.

For Padilla’s scheduled December 3, 2012, resentencing, Padilla was transferred from the Supermax facility in Florence, Colorado, to Florida. Padilla’s attorney requested a delay in sentencing for the benefit of Padilla’s mental health. While in Florence, Jose’s family, who are of limited means, only have been able to visit him on one occasion. The undersigned is clearly concerned about Jose’s mental health and believes that multiple family visits, prior to the resentencing, will be beneficial to his mental health.

Judge Cooke delayed sentencing until April 8, 2013, on which day two sealed docket entries were entered in the case.

**Challenge: Classified Arguments**

In response to Padilla’s habeas corpus petition in New York, the government submitted both a public redacted declaration describing evidence supporting the designation of Padilla as an enemy combatant and an ex parte, in camera classified unredacted declaration. Judge Mukasey reviewed the classified declaration to assess the validity of the government’s denial of Padilla’s access to counsel. The only information in the redacted declaration not in the public declaration was the identity of sources and some circumstantial evidence corroborating facts in the redacted declaration. The classified declaration did not refer to conduct by Padilla not described in the redacted declaration.

Judge Mukasey ruled that it was proper to deny Padilla access to the classified declaration unless Padilla rebutted the facts in the redacted declaration justifying his designation as an enemy combatant and fairness demanded his access to the unredacted declaration, at which time the government could elect to withdraw the unredacted declaration instead of granting Padilla access to it, if the government so wished.
The government also presented in camera an ex parte unredacted declaration to support its motion to reconsider Judge Mukasey’s granting Padilla access to counsel. The court of appeals reviewed both unredacted declarations, but it did not rely on them.

In the Eleventh Circuit appeal by Padilla, Hassoun, and Jayoussi, the court instructed the parties to give notice whether classified matters would be presented at oral argument. None was. Much of the information that was classified during the district court case, such as statements made while Padilla was designated an enemy combatant, had been declassified by the time of the appeal. Hassoun’s appellate brief included some still-classified information.

**Challenge: Witness Security**

To show chain of custody for Padilla’s alleged Mujahideen Data Form, the government offered testimony from the CIA agent who found it. The government asked that the witness’s identity be protected by use of (1) a pseudonym; (2) light disguise (which “may involve the witness wearing a wig, eyeglasses or minor facial hair”); (3) a separate entrance; (4) a prohibition on sketch artists “recording the witness’ likeness”; and (5) a prohibition on “questioning the witness in a manner that would expose either his classified identity, the classified identities of other covert CIA personnel, or the specific location of the covert CIA site in Quandahar, Afghanistan where the witness worked.

At trial, the witness wore black-rimmed glasses and a closely cropped beard. He came to the courtroom from the basement by way of the prisoner elevator.

**Challenge: Court Security**

For Padilla’s Miami trial, federal deputy marshals were brought in from around the country. An extra metal detector was set up outside Judge Cooke’s courtroom.

**Challenge: Jury Security**

To shield potential jurors from the public during jury selection, the court erected a screen in the courthouse lobby. The jury was semi-sequestered. Their identities were known to the court and the parties, but identifying information was not presented in open court or otherwise made public. Jurors did not report directly to the courthouse, each reported to a specific secret location—one on the north side of town and one on the south side—from which they were shuttled to the courthouse. Instead of going their own way for lunch, they always ate together. Once a week or so, the deputy marshals took them out for lunch.

Restrooms on the courtroom’s floor were reserved for use by jurors and court staff only. Cubicle walls were used to screen off a rest area outside the jury room, a table and chairs were set up outside a porch, and extra games and magazines were brought in.

**Challenge: Classified Evidence**

District of South Carolina

Padilla’s attorneys wanted his habeas petition decided on legal grounds rather than factual grounds, so evidence was never an important issue in the case. However, this could not be known with certainty at the outset, so Judge Floyd’s two law clerks and his judicial assistant obtained security clearances. Judge Floyd sits in Spartanburg, but he anticipated a possible evidentiary hearing at the larger courthouse in Charleston, about 200 miles away. For this reason, a courtroom deputy and a court reporter there obtained security clearances. As it happened, oral arguments were held in Spartanburg, and they did not refer to classified information.

Judge Floyd examined some classified evidence at a sensitive compartmented information facility (SCIF) at the courthouse in Charleston, but there was no need for his staff to do so.
Southern District of Florida

All defense attorneys in the criminal case received security clearances. There was already a SCIF in the basement of the courthouse, and defense attorneys could review classified information in this room.

More than two years after Padilla’s indictment, Judge Cooke granted him access to classified evidence created during his military confinement. Although it is common to grant defense attorneys access to classified evidence relevant to a prosecution, it is very unusual for courts to grant access to terrorism defendants. Both Judge Cooke and defense attorneys viewed classified videos of Padilla’s interrogation in the basement SCIF.

All of Judge Cooke’s staff received security clearances for this case. The last of her cleared law clerks left in 2009, but her permanent staff—her assistant, courtroom deputy, and court reporter—all retained top secret clearances. During this case, Judge Cooke did not use interns, because they would not have security clearances.

Challenge: FISA Evidence

FISA warrants resulted in evidence against each of the defendants. On February 14, 2006, Hassoun moved the court to undertake a careful review of all applications for electronic surveillance of defendant Hassoun conducted pursuant to the Foreign Intelligence Surveillance Act ("FISA"), as well as applications for such surveillance of any third-party target which intercepted defendant, and to hold a hearing under Franks v. Delaware, 438 U.S. 154 (1978), and, as a result, suppress all intercepts of defendant Hassoun derived from illegally authorized FISA surveillance.

Judge Cooke referred the matter to Magistrate Judge Stephen T. Brown, who "examined in camera every application from which the Government has indicated that it derived evidence that will be used in its case against the Defendants." Judge Brown found that each individual application contained probable cause that the subject of the surveillance was "an agent of a foreign power." The Court additionally found that with respect to any target who is a "United States person," the probable cause finding(s) were not based solely on activities which are protected under the First Amendment.

On April 4, 2007, Judge Cooke affirmed Judge Brown’s findings: "Although the Magistrate Judge carefully reviewed the FISA applications and other materials that are the subject of the instant motions, I also reviewed the applications. On review, I agree with Magistrate Judge Brown." When she was not looking at them, Judge Cooke stored the warrant applications in an approved safe in her chambers.

Judge Cooke was also called upon to review an evidentiary substitute for classified evidence, as provided by the Classified Information Procedures Act (CIPA). An agent of the intelligence agency with authority over the evidence brought the original evidence to the classified information security officer, who delivered it to Judge Cooke in chambers for her private review in her office while the agent and the security officer waited outside her door.

1009 Id.
1012 Id.
1013 Id.
1014 Id.
1015 Tying Cases, supra note 907, at 8 (remarks by Judge Cooke); Interview with Hon. Marcia G. Cooke, Oct. 8, 2009.

National Security Case Management Studies (06.25.2013)
Foreign Intelligence Surveillance Act
Litigation

Robert Timothy Reagan
Federal Judicial Center

The Foreign Intelligence Surveillance Act

The Foreign Intelligence Surveillance Act (FISA) was signed by President Carter on October 25, 1978.¹ The eleven sections of FISA’s title I became chapter 36, sections 1801 through 1811, of the U.S. Code’s title 50 on war and national defense. FISA’s title II included conforming amendments, and title III concerned the effective date.

FISA provides for court orders authorizing “electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information [involving] the acquisition of communications of [a] United States person.”² Foreign powers include foreign governments, foreign factions, and international terrorists.³ Use of FISA-derived evidence in court requires notice to the person against whom the evidence is used.⁴

FISA orders are issued by a FISA court, sometimes referred to as the Foreign Intelligence Surveillance Court or FISC, that originally consisted of seven district judges from seven circuits appointed by the Chief Justice for nonrenewable seven-year terms.⁵

Physical Searches

In 1980, President Carter’s second attorney general, Benjamin Civiletti, adopted a policy of seeking FISA court permission for some physical searches in service of foreign intelligence, searches that are sometimes called black bag jobs.⁶ William French Smith, President Reagan’s first attorney general, submitted a black bag petition to the FISA court on June 3, 1981, asking the court to deny the petition and rule that the court did not have jurisdiction over such petitions.⁷ Presiding Judge George L. Hart, Jr., District of the District of Columbia, acceded to the

². FISA § 102(b), 50 U.S.C. § 1802(b) (2011).
³. Id. § 101(a), 50 U.S.C. § 1801(a).
⁴. Id. § 106(a), 50 U.S.C. § 1806(a).
government’s request in the court’s first public opinion.\(^8\) Expressing a judgment in which all judges on the court concurred, Judge Hart observed that the text of FISA applied only to electronic surveillance.\(^9\)

In 1994, FISA was amended to extend the FISA court’s jurisdiction to include physical searches for foreign intelligence purposes.\(^10\) The new provisions became FISA’s title III,\(^11\) and provisions on effective dates became title IV.

**FISA Expansion**

In 1998, the FISA court’s jurisdiction was further expanded to include pen registers, trap and trace devices, and business records, creating new titles IV\(^12\) and V\(^13\) and moving effective date provisions to title VI.\(^14\)

The USA PATRIOT Act was signed by President Bush on October 26, 2001.\(^15\) It relaxed the standard for issuing a FISA order from “the purpose of the surveillance is to obtain foreign intelligence information” to require that only “a significant purpose” be foreign intelligence.\(^16\) The act also expanded the FISA court from seven to 11 district judges, of whom at least three must reside within 20 miles of D.C.\(^17\) (The FISA Amendments Act of 2008 clarified that the 11 judges must come from “at least” seven circuits.\(^18\))

Section 215 of the Patriot Act expanded FISA’s title V for business records to include “any tangible things.”\(^19\) Before the Patriot Act, FISA provided for FISA court orders issued to the FBI “authorizing a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility to release records in its possession for an investigation to gather foreign intelligence information or an investigation concerning international terrorism.”\(^20\) The Patriot Act authorized the FISA court to assist the FBI by issuing “an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.”\(^21\)

---

9. *Id.*
12. *Id.* §§ 1841–1846 (subchapter III, on pen registers and trap and trace devices).
13. *Id.* §§ 1861–1862 (subchapter IV, on business records).
FISA imposes on the government a requirement for “minimization procedures” to protect persons from unnecessary violations of privacy. Over the years, the FISA court exercised oversight over minimization procedures:

In order to preserve both the appearance and the fact that FISA surveillances and searches were not being used sub rosa for criminal investigations, the Court routinely approved the use of information screening “walls” proposed by the government in its applications. Under the normal “wall” procedures, where there were separate intelligence and criminal investigations, or a single counter-espionage investigation with overlapping intelligence and criminal interests, FBI criminal investigators and Department prosecutors were not allowed to review all of the raw FISA intercepts or seized materials lest they become defacto partners in the FISA surveillances and searches. Instead, a screening mechanism, or person, usually the chief legal counsel in an FBI field office, or an assistant U.S. attorney not involved in the overlapping criminal investigation, would review all of the raw intercepts and seized materials and pass on only that information which might be relevant evidence. In unusual cases such as where attorney-client intercepts occurred, Justice Department lawyers in [the Office of Intelligence Policy and Review] acted as the “wall.” In significant cases, involving major complex investigations such as the bombings of the U.S. Embassies in Africa, and the millennium investigations, where criminal investigations of FISA targets were being conducted concurrently, and prosecution was likely, this Court became the “wall” so that FISA information could not be disseminated to criminal prosecutors without the Court’s approval. In some cases where this Court was the “wall,” the procedures seemed to have functioned as provided in the Court’s orders; however, in an alarming number of instances, there have been troubling results.

In November of 2000, the Court held a special meeting to consider the troubling number of inaccurate FBI affidavits in so many FISA applications.

In virtually every instance, the government’s misstatements and omissions in FISA applications and violations of the Court’s orders involved information sharing and unauthorized disseminations to criminal investigators and prosecutors.

Following the attacks of September 11, 2001, the government proposed relaxed minimization procedures, but all seven members of the court agreed that some of the changes were “designed to enhance the acquisition, retention and dissemination of evidence for law enforcement purposes, instead of being consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.” One of the court’s concerns was that the government would be able to circumvent probable cause requirements for criminal investigations by characterizing the investigations as for foreign intelligence. So the court modified the submitted minimization procedures.

FISA requires the Chief Justice to appoint three district or circuit judges to a FISA court of review to hear government appeals from FISA court rulings. Hearing its very first appeal, the court of review overruled the FISA court’s modi-

22. Id. §§ 1801(h) 1821(4) (2011).
24. Id. at 623.
25. Id. at 624 (quotation marks omitted).
26. Id. at 625–27.
fications to the government’s minimization procedures.28 “The FISA court’s decision and order not only misinterpreted and misapplied minimization procedures it was entitled to impose, but as the government argues persuasively, the FISA court may well have exceeded the constitutional bounds that restrict an Article III court.”29

**Warrantless Wiretaps**

On December 16, 2005, the *New York Times* reported that President Bush had secretly authorized in 2002 a program of surveillance that excluded the FISA court from surveillance approval, although the surveillance included international communications with people in the United States.30 *USA Today* reported on May 11, 2006, that telephone companies were cooperating with government surveillance in possible violation of FISA.31 Civil suits against the government and against telephone companies followed these revelations, and most of the suits were consolidated by the Judicial Panel on Multidistrict Litigation before District Judge Vaughn R. Walker in the Northern District of California.32 Judges were divided in these cases on whether the plaintiffs had standing to challenge the government program.

In an action against the government filed in the Eastern District of Michigan, District Judge Anna Diggs Taylor ruled before the cases were consolidated that the program was unconstitutional and a violation of FISA.33 On appeal, Circuit Judge Ronald Lee Gilman agreed both that the plaintiffs had standing and that their suit had merit,34 but he was outvoted by Circuit Judges Alice M. Batchelder

---


29. Id. at 731.


31. Leslie Cauley, *NSA Has Massive Database of Americans’ Phone Calls*, USA Today, May 11, 2006, at 1A.


34. ACLU v. NSA, 467 F.3d 590, 683, 720 (6th Cir. 2006) (Judge Gilman, dissenting).
and Julia Smith Gibbons, who determined that the plaintiffs’ claims were too speculative to afford them standing.35

Judge Walker dismissed most of the consolidated suits against the government as generalized grievances insufficient to afford the plaintiffs standing.36 Circuit Judges M. Margaret McKeown, Harry Pregerson, and Michael Daly Hawkins, however, all agreed that the plaintiffs did have standing.37

One case against the government had exceptional facts. The government froze the assets of the Al-Haramain Islamic Foundation, a charity headquartered in Ashland, Oregon, on February 19, 2004.38 On September 9, the Treasury Department designated the charity a global terrorist organization.39 The Ashland charity was affiliated with the Al-Haramain Islamic Foundation in Saudi Arabia, which was the charitable arm of the Muslim World League, an organization founded in 1962.40 As part of the charity’s challenge to the freezing of its assets and its designation as a terrorist organization, the government mistakenly produced to the charity’s attorneys a top secret document that apparently is evidence of surveillance pursuant to President Bush’s secret surveillance program.41 Relying on the top secret document, the attorneys filed a civil action in the District of Oregon on February 28, 2006.42

District Judge Garr M. King ruled that the document was protected by the state secrets privilege, so it could not be entered into evidence to support the attorneys’ case, but the attorneys’ memories of the document’s contents could not be expunged, so they could rely on those.43 On interlocutory appeal, certified by Judge King and accepted by the court of appeals, Judges McKeown, Pregerson, and Hawkins reversed Judge King’s “commendable effort to thread the needle,” holding that the plaintiffs’ memories of the top secret document were also covered by the state secrets privilege.44 The court of appeals remanded the case for a determination of whether FISA’s remedies for improper surveillance preempted the

35. Id. at 653 (opinion for the court); id. at 692 (Judge Gibbons, concurring in the judgment).
37. Jewel v. NSA, 673 F.3d 902 (9th Cir. 2011).
38. Al Haramain Islamic Found. v. United States Dep’t of Treasury, 686 F.3d 965, 970–71, 973 (9th Cir. 2012); Al Haramain Islamic Found. v. United States Dep’t of Treasury, 585 F. Supp. 2d 1233, 1245 (D. Or. 2008).
40. United States v. Sedaghaty, 728 F.3d 885, 893 (9th Cir. 2013); see Chris Heffelfinger, Radical Islam in America 57–59 (2011).
44. Al-Haramain Islamic Found. v. Bush, 507 F.3d 1190, 1204–05 (9th Cir. 2007).
state secrets privilege.\textsuperscript{45} By the time of remand, the case had been consolidated with the cases before Judge Walker,\textsuperscript{46} who determined that FISA did preempt the state secrets privilege, “but only in cases within the reach of its provisions.”\textsuperscript{47}

FISA’s section 110 provides civil remedies for violations of FISA.\textsuperscript{48} Judge Walker determined, however, that the court of appeals unequivocally ruled that the plaintiffs could not rely on the top secret document to establish standing to seek those remedies.\textsuperscript{49} In 2010, Judge Walker awarded the plaintiffs summary judgment, because they presented as unrebutted evidence numerous public government statements implying that the charity had been surveilled and the government did not show that the surveillance was authorized by FISA.\textsuperscript{50} On appeal, Judges McKeown, Pregerson, and Hawkins concluded that section 110 had not waived the government’s sovereign immunity.\textsuperscript{51}

Congress amended FISA to provide the telephone companies with retroactive immunity in the consolidated cases before Judge Walker.\textsuperscript{52} The Intelligence Reform and Terrorism Prevention Act of 2004 moved FISA’s title VI on effective dates to title VII and added a new title VI on requirements for reporting FISA court statistics to Congress.\textsuperscript{53} The FISA Amendments Act of 2008 substituted a new title VII providing “additional procedures regarding certain persons outside the United States.”\textsuperscript{54} Subject to FISA court approval or exigent circumstances, “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.”\textsuperscript{55} A new title VIII granted the telephone companies retroactive civil immunity.\textsuperscript{56}

On January 10, 2007, while the warrantless wiretap litigation was pending, the FISA court issued two negotiated classified orders that resulted in the govern-

\textsuperscript{45} Id. at 1205–06.
\textsuperscript{47} In re NSA Telecomm. Records Litig., 564 F. Supp. 2d 1109, 1115–25 (N.D. Cal. 2008).
\textsuperscript{49} In re NSA, 564 F. Supp. 2d at 1134.
\textsuperscript{50} In re NSA Telecomm. Records Litig., 700 F. Supp. 2d 1182 (N.D. Cal. 2010).
\textsuperscript{51} Al-Haramain Islamic Found. v. Obama, 705 F.3d 845 (9th Cir. 2012).
ment’s no longer circumventing the FISA court in the surveillance program at issue. 57

The new FISA Court orders are innovative and complex and it took considerable time and work for the Government to develop the approach that was proposed to and ultimately accepted by the Court. As a result of the new orders, any electronic surveillance that was conducted as part of the [terrorist surveillance program] is now being conducted subject to the approval of the FISA Court. 58

The Electronic Frontier Foundation filed an action under the Freedom of Information Act (FOIA) on February 27 in the District of the District of Columbia seeking disclosure of the orders. 59 Judge Thomas F. Hogan ruled on August 14 that the orders satisfied the national defense, statutory, and law enforcement FOIA exemptions. 60

On August 9, the ACLU filed a motion directly with the FISA court for public release of the orders. 61 On August 16, the court’s Presiding Judge Colleen Kollar-Kotelly, District of the District of Columbia, ordered the government to respond to the motion. 62 FISA Court Judge John D. Bates, District of the District of Columbia, determined on December 11 that the FISA court had supervisory power over its records, so it had jurisdiction to hear the ACLU’s motion, contrary to the government’s position on that issue. 63 Judge Bates denied the ACLU its requested relief. 64 “Other courts operate primarily in public, with secrecy the exception; the FISC operates primarily in secret, with public access the exception.” 65

Upon Judge Walker’s February 28, 2011, retirement, the court assigned the warrantless wiretap cases to Judge Jeffrey S. White. 66 On July 8, 2013, Judge White ruled that FISA displaced the state-secrets privilege in two remaining cas-


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.

Second Privacy Board Report, supra note 31, at 17.


64. Id. at 497.

65. Id. at 488.

Foreign Intelligence Surveillance Act Litigation

es—a case originally filed in Brooklyn on May 17, 2006, and a case filed in San Francisco on September 18, 2008—and that potentially valid constitutional claims remained. An action originally filed in Manhattan on January 17, 2006, was dismissed by the Ninth Circuit’s court of appeals on June 10, 2013, in light of a February 26 standing ruling by the Supreme Court in Clapper v. Amnesty International USA. An action originally filed in Atlanta on January 20, 2006, was voluntarily dismissed on March 5, 2010.

Statutory Enhancement of Surveillance Authority

President Bush signed the Protect America Act on August 5, 2007. The act was a six-month modification of FISA that excluded from FISA’s coverage electronic “surveillance directed at a person reasonably believed to be located outside of the United States.” The act specified a procedure for the FISA court to enforce a directive by the Director of National Intelligence or the Attorney General to a communication service provider for compensated assistance in “the acquisition of foreign intelligence information” concerning “persons reasonably believed to be located outside the United States.”

The FISA Court of Review’s Second Published Opinion

On August 22, 2008, the FISA court of review, in its second published opinion, affirmed an order of compliance issued by the FISA court. Reviewing the constitutionality of the directives, the court held “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 lo-

cated outside the United States.” The court determined that the directives satisfied the Fourth Amendment’s reasonableness requirement.

Yahoo! complied with the directives. On June 14, 2013, it filed a motion with the FISA court to make public the lower court’s opinion and to make public Yahoo!’s identity. Presiding Judge Reggie B. Walton, District of the District of Columbia, after consultation with the other FISA court judges, issued an order on July 15 that the government review the opinion for redaction of classified information. In response to the motion, the government stated that Yahoo!’s identity could be declassified and that the government had no objection to publication of unclassified portions of the opinion and the case file.

**Challenges to the FISA Amendments Act**

The ACLU initiated litigation on the FISA Amendments Act on the day that the act was signed.

The ACLU filed a motion with the FISA court for access to the court’s rulings on the constitutionality of the act’s provisions. On August 27, 2008, Judge Mary A. McLaughlin, Eastern District of Pennsylvania, denied the motion.

The ACLU also filed an action in the Southern District of New York challenging the act’s constitutionality. Judge John G. Koeltl ruled that the plaintiffs lacked standing because they could only claim that their communications might be monitored as a result of the amendments. A panel of the U.S. Court of Appeals for the Second Circuit determined that the plaintiffs did have standing and remanded the action for a determination of constitutionality. En banc rehearing was denied by a vote of six to six. In *Clapper*, however, the Supreme Court ruled that Judge Koeltl was correct that the plaintiffs lacked standing because their grievance was too speculative.

---

79. *In re Directives*, 551 F.3d at 1012; see Second Privacy Board Report, supra note 31, at 90.
80. *In re Directives*, 551 F.3d at 1012–15.
81. Id. at 1008.
89. Amnesty Int’l USA v. Clapper, 638 F.3d 118 (2d Cir. 2011).
90. Amnesty Int’l USA v. Clapper, 667 F.3d 163 (2d Cir. 2011).
Concerns by Senators Wyden and Udall

On May 26, 2011, Senators Ron Wyden and Mark Udall warned that the Justice Department’s secret interpretation of surveillance authorized by the Patriot Act did not comport with the act’s text and would trouble citizens. On June 22, Charlie Savage, a reporter for the New York Times, submitted a FOIA request to the Department for a report referenced by Senators Wyden and Udall. The reporter and the Times filed a complaint to enforce the request in the Southern District of New York on October 5.

On October 26, the ACLU filed an action in the same district to enforce a May 31 FOIA “Request for the release of any and all records concerning the government’s interpretation or use of Section 215” of the Patriot Act, which amended FISA’s title V on business records and other tangible things. The case was immediately referred to Judge William H. Pauley as related to the Times case, over which Judge Pauley was presiding.

After an in camera review of the report, Judge Pauley ruled on May 17, 2012, that it was properly withheld. In 2013 and 2014, the government released to the ACLU additional documents concerning section 215.

On July 20, 2012, Wired posted online a story that the FISA court had ruled on at least one occasion that the government had applied the FISA Amendment Act unconstitutionally. The report derived from a July 20 letter to Senator Ron Wyden from the Office of the Director of National Intelligence granting the senator permission to make three statements, including that “on at least one occasion the Foreign Intelligence Surveillance Court held that some collection carried out pursuant to the [FISA] Section 702 minimization procedures used by the government was unreasonable under the Fourth Amendment.” According to the letter,

The text that you have asked us to review concerns classified opinions of the Foreign Intelligence Surveillance Court (FISC). . . . However, . . . the Director of National Intelli-

gence (DNI), has determined, as an exercise of his discretion, “that the public interest in disclosure outweighs the damage to the national security that might reasonably be expected from disclosure.” Accordingly, the DNI has taken the exceptional step of declassifying your proposed text and the other information contained in this letter.102

The Director’s office asked the Senator to report also, “The government has remedied these concerns and the FISC has continued to approve the collection as consistent with the statute and reasonable under the Fourth Amendment.”103

On August 30, the Electronic Frontier Foundation filed a FOIA complaint in the District of the District of Columbia to enforce a July 26 FOIA request for any FISA court opinion supporting Senator Wyden’s statement.104 In an April 1, 2013, motion for summary judgment, the government argued that it was properly withholding from the plaintiff a FISA court order otherwise responsive to the FOIA request, and only the FISA court could authorize its publication anyway.105 On May 21, the plaintiff sought from the FISA court permission for the government to release the order.106 On June 12, Presiding Judge Walton determined that FISA court rules did not prohibit disclosure of the order.107

Judge Bates’s Concerns

The FOIA court order at issue in the Electronic Frontier Foundation’s FOIA action was an October 3, 2011, opinion by FISA Court Presiding Judge Bates.108 The government publicly released a redacted version of the opinion on August 21, 2013.109 FISA’s section 702, enacted as part of the FISA Amendments Act of

102. Id. at 1–2.
103. Id. at 2.

Foreign Intelligence Surveillance Act Litigation

2008, provides for FISA court approval of surveillance programs “targeting... persons reasonably believed to be located outside the United States to acquire foreign intelligence information.”110 Judge Bates held that aspects of some NSA surveillance violated the Fourth Amendment’s reasonableness requirement.111

The Court’s review of the targeting and minimization procedures submitted with the April 2011 Submissions is complicated by the government’s recent revelation that 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 [multi-communication transactions or MCTs], including communications that are neither to, from, nor about targeted facilities...

...In sum, NSA’s collection of MCTs results in the acquisition of a very large number of Fourth Amendment-protected communications that have no direct connection to any targeted facility and thus do not serve the national security needs underlying the Section 702 collection as a whole. Rather than attempting to identify and segregate the non-target, Fourth-Amendment protected information promptly following acquisition, NSA’s proposed handling of MCTs tends to maximize the retention of such information and hence to enhance the risk that it will be used and disseminated.112

Judge Bates expressed concern that the government’s clarifying revelation while the application for Judge Bates’s approval was pending was “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.”113

On November 30, Judge Bates ruled that “the government has adequately corrected the deficiencies identified in the October 3 Opinion.”114

Presiding over the Electronic Frontier Foundation’s FOIA action, Judge Amy Berman Jackson reviewed Judge Bates’s unredacted opinion and ordered the government to provide additional justifications for some redactions.115 The government responded by removing some redactions; Judge Jackson determined that the less redacted opinion complied with FOIA.116

110. FISA § 702(a); 50 U.S.C. § 1881(a) (2011); see Second Privacy Board Report, supra note 31, at 1 (“Under the... 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 [footnote omitted] located outside the United States.”).
112. Id. at 15.
Litigation Following Snowden’s Revelations

In January 2013, Edward Snowden, who worked in Hawaii for an NSA contractor, contacted documentarian Laura Poitras, who lived in Berlin, because he was interested in disclosing what he believed to be improper surveillance practices.117 Poitras brought into the loop journalists Glenn Greenwald, a reporter for the London Guardian living in Rio de Janeiro, and Barton Gellman, formerly a reporter for the Washington Post, living in New York.118 Snowden turned to Poitras after Greenwald’s cool response to Snowden’s December 2012 efforts to interest him.119

On June 1, Poitras and Greenwald flew to Hong Kong to meet Snowden.120 The Guardian insisted that one of its veteran journalists, Ewan MacAskill, accompany the other two.121 Snowden transferred to the journalists files containing classified information about NSA surveillance programs.122 The impact of Snowden’s revelations resulted in his being the first runner-up as Time magazine’s person of the year for 2013.123 The Guardian and the Washington Post won public-service Pulitzer Prizes.124

---


118. Glenn Greenwald, No Place to Hide 10–16 (2014); see Andrews et al., supra note 117, at 154, 164, 196–97; Auletta, supra note 117, at 52; Gurnow, supra note 117, at 33–40.


120. Greenwald, supra, note 118, at 24–33 (noting that they arrived Sunday night, June 2); see Auletta, supra note 117, at 52; Gurnow, supra note 117, at 40–41; Harding, supra note 119, at 6–13, 78–83.


In June 2013, the FISA court created a public docket website for selected matters brought by private parties.\textsuperscript{125} On June 10, the ACLU filed a motion with the FISA court for release of orders approving the newly disclosed surveillance programs,\textsuperscript{126} and the ACLU filed a civil action in the Southern District of New York on the following day challenging the constitutionality of the programs.\textsuperscript{127} The New York court assigned the case there to Judge Pauley as related to the 2011 FOIA actions by the \textit{New York Times} and the ACLU.\textsuperscript{128} On November 20, 2013, FISA Court Judge F. Dennis Saylor IV, District of Massachusetts, ordered the government to explain why no part of a February 19 opinion by the FISA court could be released.\textsuperscript{129} On December 20, the government submitted to Judge Saylor a proposed redacted opinion for public release.\textsuperscript{130} After discussions with court staff on January 23, 2014, the government agreed on February 6 to release a less redacted opinion.\textsuperscript{131}

Because of FOIA actions by the ACLU and the Electronic Frontier Foundation, the Director of National Intelligence released 1,040 pages of documents, including several FISA court documents, on November 18, 2013.\textsuperscript{132} Two long and redacted opinions granted "authority for the [NSA] to collect information regarding e-mail and certain other forms of Internet communications under the pen register and trap and trace provisions of [FISA]."\textsuperscript{133} In the press release, the Director

---

\textsuperscript{125} http://www.fisc.uscourts.gov/public-filings (remodeled approximately May 1, 2014); see Peter Wallsten, Carol D. Leonnig & Alice Crites, \textit{Rare Scrutiny for a Court Used to Secrecy}, Wash. Post, June 23, 2012, at A1.


\textsuperscript{128} Assignment Notice, ACLU, No. 1:13-cv-3994 (S.D.N.Y. June 14, 2013), D.E. 2; see N.Y. Times Co. v. United States Dep’t of Justice, 872 F. Supp. 2d 309 (S.D.N.Y. 2012); Section 215 of the Patriot Act—FOI, supra note 98.


stated that the surveillance program granted authority by these opinions had been discontinued for lack of effectiveness pursuant to an evaluation begun in 2011. 134

The first opinion is 87 pages by Judge Kollar-Kotelly, with a redacted date of issue. 135 The Washington Post, however, concluded, “Although the date was blanked out, the opinion appeared to be the order that placed the NSA’s Internet metadata program under court supervision in July 2004, according to an NSA inspector general report leaked this year by former NSA contractor Edward Snowden.” 136 According to Judge Kollar-Kotelly, “This application seeks authority for a much broader type of collection than other pen register/trap and trace applications and therefore presents issues of first impression. For that reason it is appropriate to explain why the Court concludes that the application should be granted as modified herein.” 137

“[B]ased on the plain meaning of the applicable definitions, the proposed collection involves a form of both pen register and trap and trace surveillance.” 138 Additionally, Judge Kollar-Kotelly found that “such an interpretation would promote the purpose of Congress in enacting and amending FISA regarding the acquisition of non-content addressing information.” 139 The surveillance program comports with the Fourth Amendment because “there is no reasonable expectation of privacy under the Fourth Amendment in the metadata to be collected.” 140 Additionally, “The weight of authority supports the conclusion that Government information-gathering that does not constitute a Fourth Amendment search or seizure will also comply with the First Amendment when conducted as part of a good-faith criminal investigation.” 141

On the expiration of Judge Kollar-Kotelly’s authorization of the email metadata surveillance program, Judge Bates considered an “application to reinitiate in expanded form” such surveillance. 142 In his 117-page opinion, Judge Bates discussed many violations of surveillance restrictions that the government had disclosed. 143 “The history of material misstatements in prior applications and non-compliance with prior orders gives the Court pause before approving such an expanded collection.” 144 So, Judge Bates’s approval of the surveillance came with some modifications. 145

136. Nakashima & Miller, supra note 132.
138. Id. at 16–17.
139. Id. at 18.
140. Id. at 59.
141. Id. at 66.
143. Id. at 9–22.; see Devlin Barrett, Surveillance Court Judge Criticized NSA “Overcollec-
144. Bates PR/TT Opinion, supra note 133, at 72.
145. Id. at 117.
The Director of National Intelligence released another approximately 1,000 pages of FISA court records on August 11, 2014,\(^{146}\) apparently as a result of a FOIA action brought by the Electronic Privacy Information Center on December 9, 2013,\(^{147}\) that concerned the NSA’s discontinued pen register and trap and trace program.

On June 18 and 19, 2013, respectively, Google and Microsoft sought permission from the FISA court to disclose aggregate statistics on FISA orders that they had received.\(^{148}\) Yahoo!, Facebook, and LinkedIn filed similar motions in September.\(^{149}\) Apple joined the litigation as an amicus curiae in November.\(^{150}\) On January 27, 2014, the government settled the motions by granting permission to the carriers to report the number of FISA orders received in bands of 250, or in bands of 1,000 if broken down into category of FISA order.\(^{151}\)

---


The Electronic Privacy Information Center filed a petition for a writ of mandamus with the Supreme Court on July 8, 2013, seeking review of a leaked FISA court order requiring Verizon to provide the NSA with telephony metadata for all communications in which at least one party is within the United States. On July 19, the day that the leaked order expired, the Director of National Intelligence reported that the FISA court had renewed authorization for NSA’s “telephony metadata collection program.” The Supreme Court denied mandamus review on November 18.

The Electronic Frontier Foundation had filed a FOIA complaint in the Northern District of California on October 26, 2011, to enforce a June 2 FOIA request for records concerning the government’s interpretation of the Patriot Act’s section 215, which amended FISA’s title V on tangible things. In response to that suit and the ACLU’s 2011 FOIA suit in the Southern District of New York, and in light of Snowden’s revelations, the government released on September 10, 2013, 14 previously classified documents, with redactions. Eight of the documents are FISA court orders—a 2006 order by Judge Malcolm J. Howard, Eastern District of North Carolina, a 2008 opinion by Judge Walton, and six 2009 orders and opinions by Judge Walton—and two of the documents are government submissions to the FISA court.

The released documents illustrate the FISA court’s supervision, through its business records or BR docket, of telecommunication metadata surveillance. They also include concerns by Judge Walton that government surveillance was departing from approved procedures:

In summary, since January 15, 2009, it has finally come to light that the FISC’s authorizations of this vast collection program have been premised on a flawed depiction of

---


how the NSA uses BR metadata. This misperception by the FISC existed from the inception of 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 systematically violated that it can fairly be said that this critical element of the overall BR regime has never functioned effectively.\textsuperscript{157}

The Court is deeply troubled by the incidents [disclosed by the government], which have occurred only a few weeks following the completion of an “end to end review” by the government of NSA’s procedures and processes for handling the BR metadata, and its submission of a report intended to assure the Court that NSA had addressed and corrected the issues giving rise to the history of serious and widespread compliance problems in this matter and had taken the necessary steps to ensure compliance with the Court’s orders going forward.\textsuperscript{158}

\[T\]he Court … continues to be concerned about the likelihood that these queries could reveal communications of United States person users of the telephone identifier who are not the subject of FBI investigations.\textsuperscript{159}

A version of one document released on March 28, 2014, with considerably fewer redactions than in the September 2013 release, revealed Judge Walton’s specific concerns about the NSA’s general counsel’s oversight of pen register and trap and trace surveillance:

The court is gravely concerned … that NSA analysts, cleared and otherwise, have generally not adhered to the dissemination restrictions proposed by the government, repeatedly relied upon by the Court in authorizing the collection of the PR/TT metadata, and incorporated into the Court’s orders in this matter [redacted] as binding on NSA. Given the apparent widespread disregard of these restrictions, it seems clear that NSA’s Office of General Counsel has failed to satisfy its obligation to ensure that all analysts with access to information derived from the PR/TT metadata “receive appropriate training and guidance regarding the querying standard set out in paragraph c. above, as well as other procedures and restrictions regarding the retrieval, storage, and dissemination of such information.” Docket No. PR/TT [redacted] Order at 11 (emphasis added).\textsuperscript{160}


On January 15, 2009, the Department of Justice notified the Court in writing that the government has been querying the business records acquired pursuant to Docket ER 08-13 in a manner that appears to the Court to be directly contrary to the [court’s] Order and directly contrary to the sworn attestations of several Executive Branch officials.


\textsuperscript{158} Order at 4, In re FBI Application, No. BR 09-13 (FISA Ct. Sept. 25, 2009), available at 2009 WL 9150896.

\textsuperscript{159} Order at 6, In re FBI Application, No. BR 09-15 (FISA Ct. Nov. 5, 2009), available at 2009 WL 9150915.

On January 17, 2014, the Director of National Intelligence released 24 redacted orders in 20 BR cases before the FISA court in 2006 through 2011. The orders are periodic approvals of a program to collect “all call detail records or ‘telephony metadata’” for periods typically a few days short of 90 days, ranging from 84 days to 89 days, but sometimes for shorter periods—42, 57, or 64 days—and once for a longer period—115 days. The orders do not cover the period from July 10, 2009, to February 26, 2010. In addition to Judges Howard, Kollar-Kotelly, Walton, and Bates, orders were signed by Judges Frederick J. Scullin, Jr., Northern District of New York; Robert C. Broomfield, District of Arizona; Nathaniel M. Gorton, District of Massachusetts; Roger Vinson, Northern District of Florida; and James B. Zagel, Northern District of Illinois.

The FOIA action in the Northern District of California remains pending before Judge Yvonne Gonzalez Rogers, who decided on June 13, 2014, that she would review in camera and ex parte five FISA court orders and opinions “to assure that the agency is complying with its obligations to disclose non-exempt material.” The evidence in the record shows that some documents, previously withheld in the course of this litigation and now declassified, had been withheld in their entirety when a disclosure of reasonably segregable portions of those documents would have been required.

Smith and Jones

On September 17, 2013, the FISA court released a public redacted version of an August 22 opinion by FISA Judge Claire V. Eagan, Northern District of Oklahoma, holding in an ex parte application for surveillance authorization that the FBI’s obtaining a large volume of telephony metadata was consistent with the Fourth Amendment as interpreted by the Supreme Court in 1979 in Smith v. Maryland.

In Smith, the Supreme Court held by a vote of five to three that installation and use of a pen register, to record the numbers dialed on a specific telephone, was not a search because it did not violate reasonable expectations of privacy.


163. Id. at 2.


In 1975, a robbery victim reported “threatening and obscene phone calls from a man identifying himself as the robber.”\textsuperscript{166} Michael Lee Smith was identified as a suspect, so “the telephone company, at police request, installed a pen register at its central offices to record the numbers dialed from the telephone at [his] home.”\textsuperscript{167} Writing on behalf of himself, Chief Justice Burger, and Justices White, Rehnquist, and Stevens, Justice Blackmun reasoned, “All subscribers realize . . . that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.”\textsuperscript{168} In dissent, Justice Stewart responded, “The telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment.”\textsuperscript{169} He concluded, “I think that the numbers dialed from a private telephone—like the conversations that occur during a call—are within the constitutional protection recognized in \textit{Katz} [v. \textit{United States}].”\textsuperscript{170} Justice Marshall, also in dissent, and joined by Justice Brennan, observed, “Privacy is not a discrete commodity, 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.”\textsuperscript{171}

On October 18, the FISA court released a public redacted October 11 opinion by FISA Judge Mary A. McLaughlin, Eastern District of Pennsylvania, that adopted Judge Eagan’s analysis.\textsuperscript{172} Judge McLaughlin also addressed the Supreme Court’s 2012 case, \textit{United States v. Jones}.\textsuperscript{173}

In \textit{Jones}, Justice Scalia concluded for the court, in an opinion joined by Chief Justice Roberts and Justices Kennedy, Thomas, and Sotomayor, that installation of a GPS tracking device on a vehicle to monitor the vehicle’s movements is a Fourth Amendment search because it is a trespass onto property.\textsuperscript{174}

Concurring, Justice Sotomayor observed, “Of course, the Fourth Amendment is not concerned only with trespassory intrusions on property.”\textsuperscript{175} Respecting \textit{Smith}, she observed further,

\begin{itemize}
\item \textsuperscript{166} \textit{Id}. at 737.
\item \textsuperscript{167} \textit{Id}
\item \textsuperscript{168} \textit{Id}. at 742.
\item \textsuperscript{169} \textit{Id}. at 746 (Justice Stewart, dissenting).
\item \textsuperscript{170} \textit{Id}. at 747; see \textit{Katz} v. \textit{United States}, 389 U.S. 347 (1967).
\item \textsuperscript{171} \textit{Smith}, 442 U.S. 749 (Justice Marshall, dissenting).
\item \textsuperscript{173} McLaughlin Opinion, \textit{supra} note 172, at 4–6; see \textit{United States v. Jones}, 565 U.S. ___, 132 S. Ct. 945 (2012).
\item \textsuperscript{174} \textit{Jones}, 565 U.S. at ___, 132 S. Ct. at 949–50.
\item \textsuperscript{175} \textit{Id}. at ___, 132 S. Ct. at 954 (Justice Sotomayor, concurring).
\end{itemize}
It may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This 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.\footnote{176} Concurring in the judgment, Justice Alito wrote for himself and Justices Ginsburg, Breyer, and Kagan that they “would analyze the question presented in this case by asking whether respondent’s reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove.”\footnote{177} Respecting older precedents, Justice Alito observed, “In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical.”\footnote{178}

Judge McLaughlin decided that the concerns expressed by the concurring justices in \textit{Jones} did not suggest a conclusion in the telephony surveillance applications, because non-content metadata are not the same as location information.\footnote{179} On December 18, 2013, Judge McLaughlin granted a motion by the Center for National Security Studies to submit an amicus curiae brief on whether FISA authorizes the collection of telephony metadata in bulk.\footnote{180} Judge Zagel endorsed the analyses of Judges Eagan and McLaughlin in a June 19, 2014, FISA court opinion.\footnote{181}

\textbf{Motions for FISA Court Records}

On November 7, 2013, the ACLU filed a motion with the FISA court “to unseal its opinions addressing the legal basis for the ‘bulk collection’ of data by the United States government under the Foreign Intelligence Surveillance Act.”\footnote{182} ProPublica filed a similar motion on November 12.\footnote{183} On December 5, Presiding Judge Walton granted permission for the Reporters Committee for Freedom of the Press and 25 other media organizations to file an amicus curiae brief.\footnote{184}

\footnotesize
\begin{itemize}
\item \footnote{176}{\textit{Id.} at \underline{2}, 132 S. Ct. at 957 (citations omitted).}
\item \footnote{177}{\textit{Id.} at \underline{2}, 132 S. Ct. at 958 (Justice Alito, concurring in the judgment).}
\item \footnote{178}{\textit{Id.} at \underline{2}, 132 S. Ct. at 963.}
\item \footnote{179}{McLaughlin Opinion, supra note 127, at 5.}
\end{itemize}
Conflicting Rulings on Surveillance Constitutionality

On June 6, Larry Klayman and two other persons filed a class action challenging the newly disclosed surveillance methods in the U.S. District Court for the District of the District of Columbia against the government and Verizon.\(^{185}\) Five days later, an overlapping collection of four individuals filed a similar action against the government and ten other telecommunication companies.\(^{186}\) On December 16, Judge Richard J. Leon granted the plaintiffs a preliminary injunction against bulk metadata collection.\(^{187}\)

Judge Leon found that the plaintiffs had standing, because “[t]he Government . . . describes the advantages of bulk collection in such a way as to convince me that plaintiffs’ metadata—indeed everyone’s metadata—is analyzed, manually or automatically.”\(^ {188}\) Judge Leon found the metadata collection constituted an unreasonable search, despite the Supreme Court’s 1979 decision in Smith:

In Smith, the Supreme Court was actually considering whether local police could collect one person’s phone records for calls made after the pen register was installed and for the limited purpose of a small-scale investigation of harassing phone calls. The notion that the Government could collect similar data on hundreds of millions of people and retain that data for a five-year period, updating it with new data every day in perpetuity, was at best, in 1979, the stuff of science fiction.

. . . I cannot imagine a more “indiscriminate” and “arbitrary invasion” than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval. Surely, such a program infringes on “that degree of privacy” that the Founders enshrined in the Fourth Amendment. Indeed, I have little doubt that the author of our Constitution, James Madison, who cautioned us to beware “the abridgment of freedom of the people by gradual and silent encroachments by those in power,” would be aghast.\(^ {189}\)

Moreover, “the Government does not cite a single instance in which analysis of the NSA’s bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time-sensitive in nature.”\(^ {190}\)

---


188. Id. at 26–29.

189. Id. at 33, 42 (citation omitted).

190. Id. at 40.
Judge Leon stayed his injunction pending appeal. Judge Pauley issued a conflicting opinion on December 27. Judge Pauley’s opinion includes two important observations: (1) “The Government acknowledged that it has collected metadata for substantially every telephone call in the United States since May 2006.” (2) “This blunt tool only works because it collects everything. Such a program, if unchecked, imperils the civil liberties of every citizen.” Judge Pauley determined that Smith compelled a decision in favor of the government.

On June 3, 2014, Judge B. Lynn Winmill dismissed a complaint filed in the District of Idaho alleging that comprehensive metadata collection violates the Fourth Amendment. Judge Smith relied on Smith, circuit law, and Judge Pauley’s decision. Judge Winmill urged, however, that “Judge Leon’s decision should serve as a template for a Supreme Court opinion.”

Rulings remain pending elsewhere.

On July 16, 2013, a collection of 18 organizations, including the First Unitarian Church of Los Angeles, Greenpeace, the California Association of Federal


196. ACLU, 959 F. Supp. 2d at 735.

197. Id. at 730.

198. Id. at 749–52.


An appeal is pending. Docket Sheet, Smith v. Obama, No. 14-35555 (9th Cir. July 1, 2014); Order, id. (July 14, 2014) (granting a motion to expedite the appeal and ordering the answering brief filed by October 2, 2014).


201. Id. at ___ (p.8 of opinion filed at D. Idaho No. 2:13-cv-257, D.E. 27).
Firearms Licensees, and the National Organization for the Reform of Marijuana Laws, filed a complaint against the government in the Northern District of California alleging "an illegal and unconstitutional program of dragnet electronic surveillance." Judge White accepted the case as related to the warrantless wiretap litigation.

Senator Rand Paul filed an action in the District of the District of Columbia challenging bulk surveillance on February 18, 2004. Another action was filed in El Paso on February 5.

Data Retention

In a January 3, 2014, FISA court order, Judge Hogan specified that the metadata authorized for collection by his order must be destroyed within five years of collection. On March 7, Judge Walton denied a February 25 motion by the government to extend the five-year limit to permit the government to comply with evidence-preservation obligations in the civil suits challenging the legality of broad metadata surveillance. "Extending the period of retention for these voluminous records increases the risk that information about United States persons may be improperly used or disseminated." Further, there is no indication that any of the plaintiffs have sought discovery of this information or made any effort to have it preserved . . . .

Plaintiffs in the San Francisco surveillance challenge before Judge White responded to Judge Walton’s Friday decision with a Monday motion for a temporary restraining order enjoining the government “from destroying any evidence relevant to the claims at issue in this action, including but not limited to prohib-

---


210. Id. at 8–9.
ing the destruction of any telephone metadata or ‘call detail’ records.” Judge White ordered a response from the government by 2:00 that afternoon, and then ordered the data retained, pending further hearing on the issue set for March 19.

On Wednesday, March 12, Judge Walton issued an order permitting the government to comply with Judge White’s order. Judge White issued a permanent preservation order on March 21.

Judge Walton scolded the government for failing to inform him of preservation orders remaining in effect from the multidistrict warrantless wiretap litigation that had been transferred to Judge White; the existence of these orders was brought to Judge Walton’s attention by the plaintiffs in Judge White’s cases.

“As the government is well aware, it has a heightened duty of candor to the Court in ex parte proceedings.” In response to Judge Walton’s order that the government explain its behavior, the government acknowledged on April 2 that it should have behaved differently, with “the benefit of hindsight,” but it “has always understood [the warrantless wiretap litigation] to be limited to certain presidentially authorized intelligence collection activities outside FISA.” The government advised, “no additional corrective action on the part of the Government or this Court is necessary.” A deputy assistant attorney general provided additional clarifying information one week later.

Meanwhile, on March 20, Judge Rosemary M. Collyer denied Verizon’s challenge to the legality of Judge Hogan’s January 3 telephony metadata surveillance order, concluding, “this Court finds Judge Leon’s analysis in Klayman to be unpersuasive.”

217. Id. at 8.
218. Id. at 9–10.
220. Id. at 2.
The Privacy and Civil Liberties Oversight Board

The Privacy and Civil Liberties Oversight Board, "an independent bipartisan agency within the executive branch established by the Implementing Recommendations of the 9/11 Commission Act of 2007," issued a report on January 23, 2014, concluding that surveillance authorized by the FISA court violated FISA. Although the Privacy Board was established in 2007, all five members were not appointed by the President and confirmed by the Senate until May 7, 2013, shortly before the Snowden revelations. The report analyzed the legality of surveillance conducted pursuant to FISA’s title V on business records and other tangible things, as expanded by section 215 of the Patriot Act.

There are four grounds upon which we find that the telephone records program fails to comply with Section 215. First, the telephone records acquired under the program have no connection to any specific FBI investigation at the time of their collection. Second, because the records are collected in bulk—potentially encompassing all telephone calling records across the nation—they cannot be regarded as "relevant" to any FBI investigation as required by the statute without redefining the word relevant in a manner that is circular, unlimited in scope, and out of step with the case law from analogous legal contexts involving the production of records. Third, the program operates by putting telephone companies under an obligation to furnish new calling records on a daily basis as they are generated (instead of turning over records already in their possession)—an approach lacking foundation in the statute and one that is inconsistent with FISA as a whole. Fourth, the statute permits only the FBI to obtain items for use in its investigations; it does not authorize the NSA to collect anything.

In addition, we conclude that the program violates the Electronic Communications Privacy Act. That statute prohibits telephone companies from sharing customer records


224. First Privacy Board Report, supra note 223, at 3–4; see Jeremy W. Peters, G.O.P. Delays On Nominees Raise Tension, N.Y. Times, May 12, 2013, at A1; see also 42 U.S.C. § 2000ee(h)(1) ("The Board shall be composed of a full-time chairman and 4 additional members, who shall be appointed by the President, by and with the advice and consent of the Senate.").

Members of the Board shall be selected solely on the basis of their professional qualifications, achievements, public stature, expertise in civil liberties and privacy, and relevant experience, and without regard to political affiliation, but in no event shall more than 3 members of the Board be members of the same political party.

42 U.S.C. § 2000ee(h)(2); see First Privacy Board Report, supra note 223, at 3.

225. First Privacy Board Report, supra note 223, at 8; see Second Privacy Board Report, supra note 31, at 2.
with the government except in response to specific enumerated circumstances, which do not include Section 215 orders.\footnote{Id. at 10; see Electronic Communications Privacy Act, Pub. L. 99-508, 100 Stat. 1948 (1986), relevant sections as amended, 18 U.S.C. §§ 2701–2712 (2012).}

Two board members dissented from the majority’s conclusion that the section 215 surveillance program violates FISA.\footnote{227. First Privacy Board Report, supra note 223, at 208–18.}


“[T]he Board has found no evidence of intentional abuse.”\footnote{229. Second Privacy Board Report, supra note 31, at 2.}

The board concluded that section 702 could be used constitutionally:

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.

... [Some features of the program, however,] 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.\footnote{230. Id. at 96–97.}

New Notices to Criminal Defendants

In 2013, the Justice Department revised its policy on notice to criminal defendants of FISA surveillance to bring its behavior in line with representations previously made by the Solicitor General to the Supreme Court in \textit{Clapper}.

The issue in \textit{Clapper} was standing to challenge the constitutionality of FISA’s section 702, which is section 1881a of the U.S. Code’s title 50. The plaintiffs argued “that they should be held to have standing because otherwise the constitutionality of §1881a could not be challenged.”\footnote{231. Clapper v. Amnesty Int’l USA, 568 U.S. , , , , 133 S. Ct. 1138, 1154 (2013).}

The Court observed that “if the Government intends to use or disclose information obtained or derived from a §1881a acquisition in judicial or administrative proceedings, it must provide advance notice of its intent, and the affected person may challenge the lawfulness of the acquisition.”\footnote{232. Id.} Solicitor General Donald B. Verrilli, Jr., said in his reply brief, “the government must provide advance notice of its intent to use information obtained or derived from Section 1881a-authorized surveillance against a person in
judicial or administrative proceedings and that person may challenge the underlying surveillance.233

On learning, subsequent to the Snowden revelations, that Justice Department practice did not conform to the government’s representations in Clapper, Solicitor General Verrilli persuaded the department that the proper course was to provide defendants with section 702 surveillance notice.234 On December 24, 2013, the Justice Department informed Senators who had inquired about the issue,

Based on a recent review, the Department has determined that information obtained or derived from Title I FISA collection may, in particular cases, also be derived from prior Title VII FISA collection, such that notice concerning both Title I and Title VII should be given in appropriate cases with respect to the same information. Based on this determination, the government has provided notice concerning Section 702-derived information in two criminal cases.235

On October 17, 2013, the ACLU filed a complaint in the Southern District of New York based on a March 29, 2013, FOIA request for “records related to the government’s use of evidence derived from surveillance authorized by the FISA Amendments Act.”236 Judge Robert W. Sweet has held the case in abeyance pending settlement negotiations.

Historically, federal courts have frequently reviewed FISA evidence concerning criminal defendants to determine whether any of the evidence was discoverable as helpful to the defense,238 and whether any FISA evidence should be suppressed.239 Courts have also found prosecutions based on FISA evidence to be constitutional.240


According to the *New York Times* on February 26, 2014, the government had filed section 702 notices in three cases.\(^\text{241}\)

**Jamshid Muhtorov**

The FBI arrested Jamshid Muhtorov at Chicago’s O’Hare airport on January 21, 2012, interrupting his trip to Turkey.\(^\text{242}\) He was indicted in the District of Colorado, and the court assigned his case to Judge John L. Kane.\(^\text{243}\)

The government filed a section 702 notice on October 25, 2013.\(^\text{244}\) Briefing by the parties is in process.\(^\text{245}\)

**Mohamed Osman Mohamud**

Mohamed Osman Mohamud was convicted on January 31, 2013, of an attempt to use a weapon of mass destruction for attempting to detonate a car bomb, which was a fake provided by the FBI in a sting, at Portland, Oregon’s November 26, 2010, Christmas tree lighting ceremony.\(^\text{246}\) Judge Garr M. King presides over the case.\(^\text{247}\)


240. Ning Wen, 477 F.3d at 897–99; United States v. Duka, 671 F.3d 329, 242–47 (3d Cir. 2011); United States v. Abu-Jhaad, 630 F.3d 102 (2d Cir. 2010), aff’d 531 F. Supp. 2d 299 (D. Conn. 2008); United States v. Stewart, 590 F.3d 93, 126–29 (2d Cir. 2009); *Isa*, 923 F.2d 1300; United States v. Posey, 864 F.2d 1487, 1490–91 (9th Cir. 1989) (noting, “As an initial matter, we think it clear that appellant may not make a facial challenge to the FISA without arguing that the particular surveillance against him violated the Fourth Amendment.”); United States v. Pelton, 835 F.2d 1067, 1074–75 (4th Cir. 1987); *Cavanagh*, 807 F.2d 787; Duggan, 743 F.2d at 71–76; *Belfield*, 692 F.2d at 148–49; *Mahamud*, 838 F. Supp. 2d at 888–89; *Warsame*, 547 F. Supp. 2d at 992–97; *Mubayid*, 521 F. Supp. 2d at 135–41; United States v. Benkahla, 437 F. Supp. 2d 541, 554–55 (E.D. Va. 2006); United States v. Nicholson, 955 F. Supp. 588 (E.D. Va. 1997); *Falvey*, 540 F. Supp. 1306; *see Damraj*, 412 F.3d at 625 (“FISA has uniformly been held to be consistent with the Fourth Amendment”); *Johnson*, 952 F.2d at 573 (noting, “We suspect . . . that appellants have waived this claim for purposes of their appeal.”).


245. Docket Sheet, *id.* (Jan. 23, 2012); *see Transcripts at 8–9, id.* (Nov. 15, 2013, filed Dec. 20, 2013), D.E. 487 (noting Judge Kane’s amenability to participation by amici curiae).

On November 19, 2013, before Mohamud had been sentenced, the government filed a section 702 notice. On June 24, Judge King denied Mohamud’s motions for a new trial.

Clearly a lot of time has passed, but otherwise suppression and a new trial would put defendant in the same position he would have been in if the government notified him of the § 702 surveillance at the start of the case. Moreover, the government has apparently changed its practice in making this type of notification, so dismissal is not needed as a deterrence.

Judge King rejected various constitutional challenges to FISA’s new title VII, section 702 in particular. Respecting separation of powers, “[r]eview of § 702 surveillance applications is as central to the mission of the judiciary as the review of search warrants and wiretap applications.” With respect to the Fourth Amendment, “§ 702 surveillance falls within the foreign intelligence exception to the warrant requirement.” Mohamud’s “communications were collected incidentally during intelligence collection targeted at one or more non-U.S. persons outside the United States.” Acknowledging the issue as presenting “a very close question,” Judge King concluded that a warrant was not required for the examination of evidence incidentally collected on Mohamud. Finally, I made a careful de novo, ex parte review of the § 702 applications and conclude the certification required by 50 U.S.C. § 1881a(g)(2)(A) [FISA § 702(g)(2)(A)] was in place. I also find that the government agents followed appropriate targeting and minimization procedures. Thus I conclude the § 702 surveillance at issue here was lawfully conducted.

Mohamud’s sentencing is set for October 1.

251. Id. at ___. (p.18 of opinion filed at D. Or. No. 3:10-cr-475, D.E. 517); see Savage, supra note 249 (“The constitutionality of the 2008 law had never been tested in court before Judge King’s ruling.”).
253. Id. at ___. (p.25 of opinion filed at D. Or. No. 3:10-cr-475, D.E. 517).
254. Id. at ___. (pp.42–45 of opinion filed at D. Or. No. 3:10-cr-475, D.E. 517).
255. Id. at ___. (p.47 of opinion filed at D. Or. No. 3:10-cr-475, D.E. 517).
256. Mohamud Docket Sheet, supra note 247.
Agron Hasbajrami

On January 16, 2013, Agron Hasbajrami received a sentence of 15 years in prison from Judge John Gleeson, Eastern District of New York, on a plea of guilty to charges of providing material support to terrorism.257 Five days after the September 8, 2011, indictment, the government filed a notice that the government had collected FISA evidence against Hasbajrami.258

On February 24, 2014, the government informed Hasbajrami that the FISA evidence against him was obtained pursuant to orders based on section 702 FISA evidence.259 "In the government’s view, this supplemental notification does not afford you a basis to withdraw your plea or to otherwise attack your conviction or sentence because you expressly waived those rights, as well as the right to any additional disclosures from the government, in your plea agreement."260

A June 30, 2014, motion by Hasbajrami to compel discovery will be heard on September 12.261

Reaz Qadir Khan

A fourth case arose in April.

A grand jury in the District of Oregon returned a sealed indictment against Reaz Qadir Khan on December 27, 2012, for providing advice and financial assistance to Ali Jaleel and his family; Jaleel perished in a suicide attack against Pakistan’s Inter-Services Intelligence headquarters in Lahore on May 27, 2009.262 Khan, who worked at Portland's wastewater treatment plant, was arrested on March 5, 2013.263 The court assigned Khan’s case to Judge Michael W. Mosman.264

On the day that Khan was arrested, the government filed a notice that it would use against the defendant evidence collected pursuant to FISA.265 On April 3, 2014, just over one year later, the government filed a notice that evidence against Khan was acquired pursuant to FISA’s section 702.266 FISA motions will be heard.

on January 6, 2015. On June 17, 2014, Judge Mosman denied Khan’s suggestion that the judge’s 2013 appointment to the FISA court required recusal.

**Adel Daoud**

Litigation over section 702 arose in a fifth case because it was championed by Senator Dianne Feinstein on December 27, 2012, as a success story for the FISA Amendments Act.

Adel Daoud was arrested in Chicago on September 14, 2012, for attempting to bomb a bar with a fake bomb provided by the FBI. The court assigned the case to Judge Sharon J. Coleman. The government filed a notice on September 18 that it would use against Daoud evidence derived pursuant to FISA. On May 22, 2013, Daoud filed a motion for clarification from the government whether the FISA evidence against Daoud derived from traditional pre-FAA FISA surveillance or FAA FISA surveillance, often referred to as section 702 FISA surveillance. The government responded on June 12 that “the information the government intends to use was acquired pursuant to a traditional FISA order . . . as opposed to a Section 702 Order.” In sur-reply on August 8, the government said that it would “provide notice to the defense and this Court if the government intended to use in this case any information obtained or derived from surveillance authorized under Title VII of FISA . . . as to which the defendant is an aggrieved person.” On the following day, Daoud’s attorneys moved to examine and suppress all FISA evidence because “there is no indication that the prerequisites for a FISA warrant were present in this case.”

On January 29, 2014, Judge Coleman ruled that Daoud’s secured counsel should be able to review FISA application materials pertaining to Daoud’s case.

---

273. Notice, id. (Sept. 18, 2012), D.E. 9; Daoud, ___ F.3d at ___, 2014 WL 2696734 (p.3 of opinion filed at 7th Cir. 14-1284, D.E. 56).
274. FISA Clarification Motion, id. (May 22, 2013), D.E. 43.
277. FISA Suppression Motion at 2, id. (Aug. 9, 2013), D.E. 52.
Here, counsel for defendant Daoud has stated on the record that he has top secret SCI (sensitive compartmented information) clearance. Assuming that counsel’s clearances are still valid and have not expired, top secret SCI clearance would allow him to examine the classified FISA application material, if he were in the position of the Court or the prosecution. Furthermore, the government had no meaningful response to the argument by defense counsel that the supposed national security interest at stake is not implicated where defense counsel has the necessary security clearances. The government’s only response at oral argument was that it has never been done. That response is unpersuasive where it is the government’s claim of privilege to preserve national security that triggered this proceeding. Without a more adequate response to the question of how disclosure of materials to cleared defense counsel pursuant to protective order jeopardizes national security, this Court believes that the probable value of disclosure and the risk of nondisclosure outweigh the potential danger of disclosure to cleared counsel. Upon a showing by counsel, that his clearance is still valid, this Court will allow disclosure of the FISA application materials subject to a protective order consistent with procedures already in place to review classified materials by the court and cleared government counsel.

While this Court is mindful of the fact that no court has ever allowed disclosure of FISA materials to the defense, in this case, the Court finds that the disclosure may be necessary. This finding is not made lightly, and follows a thorough and careful review of the FISA application and related materials. The Court finds however that an accurate determination of the legality of the surveillance is best made in this case as part of an adversarial proceeding. The adversarial process is the bedrock of effective assistance of counsel protected by the Sixth Amendment. *Anders v. California*, 386 U.S. 738, 743 (1967). Indeed, though this Court is capable of making such a determination, the adversarial process is integral to safeguarding the rights of all citizens, including those charged with a crime. “The right to the effective assistance of counsel is thus the right of the accused to require the prosecution’s case to survive the crucible of meaningful adversarial testing.” *United States v. Cronic*, 466 U.S. 648, 656 (1984).

On June 4, 2014, the court of appeals—Circuit Judges Richard A. Posner, Michael S. Kanne, and Ilana Diamond Rovner—heard the government's appeal from Judge Coleman's order granting Daoud’s attorneys access to FISA application materials. Following a public argument, the court held a closed ex parte session with the government. Daoud’s attorneys were not notified in advance that the court would hold part of the proceeding ex parte.

Because of an error by court staff, the public argument was not recorded as it should have been. Court staff members misinterpreted security precautions for...
the ex parte session as a signal that the public session should not be recorded. The ex parte session was recorded by a cleared court reporter, however. The court agreed to ask the government to approve a redacted transcript for defense counsel’s use. Attached to a motion to remove some redactions, the defense filed the redacted transcript on the public docket.

To remedy the recording error the court ordered a second argument session at the beginning of the following week. Daoud was represented by a different attorney at the second argument.

At the second argument, Judges Posner and Rovner explained to the defense attorney that the purpose of the ex parte proceeding was to provide the court with an opportunity to cross-examine the government about the government’s representations to the court. At the closed proceeding, the government assured the court that Senator Feinstein’s comment about Daoud “was not meant to be understood as a statement that the FISA was used in this case.” Following the ex parte proceeding, the court issued a “Classified Ex Parte Order Requiring Additional Submission from the Government.”

On June 16, the court of appeals reversed Judge Coleman’s discovery order, because she had not adequately established Daoud’s attorneys “need to know” the classified FISA application materials.

The court of appeals also ruled that the investigation of Daoud did not violate FISA. The court also determined that Senator Feinstein had not identified Daoud’s case as an FAA success story; the court concluded that Senator Feinstein meant to list thwarted attacks as evidence of needed vigilance, only some of which were FAA success stories.

284. See Meisner, supra note 283.
285. Daoud, F.3d at n.*, 2014 WL 2696734 (p.1 n.* of opinion filed at 7th Cir. 14-1284, D.E 56); see Meisner, supra note 283.
289. Daoud 7th Cir. Docket Sheet, supra note 280.
291. Transcript at 7, attached to Transcript Motion, supra note 287.
294. Daoud, F.3d at , 2014 WL 2696734 (p12 of opinion filed at 7th Cir. 14-1284, D.E 56).
The Qazi Brothers

Raees Alam Qazi and Sheheryar Alam Qazi, brothers who were born in Pakistan and who became naturalized U.S. citizens, were indicted on November 30, 2012, in the Southern District of Florida for a plot to use a weapon of mass destruction somewhere in the United States. On December 6, the government filed notices that it would use FISA evidence against the defendants. On April 22, 2013, the defendants moved for notice whether any of the FISA evidence was obtained pursuant to the FAA. The defendants observed that their capture also was championed by Senator Feinstein as an FAA success. On May 6, Magistrate Judge John J. O’Sullivan granted the defendants’ motion so that they could challenge the lawfulness of any FAA surveillance, as promised by Clapper. A motion to declare the FAA unconstitutional is now pending before Judge O’Sullivan.


Moalin, Mohamud, Doreh, and Taalil

Judge Jeffrey T. Miller, Southern District of California, denied a new trial motion on November 14, 2013, a motion based in part on post-conviction Snowden revelations. “Here, when Defendant Moalin used his telephone to communicate with third parties, whether in Somalia or the United States, he had no legitimate expectation of privacy in the telephone numbers dialed.”

297. Notice, Qazi, No. 0:12-cr-60298 (S.D. Fla. Dec. 6, 2012), D.E. 10 (Sheheryar); Notice, id. (Dec. 6, 2012), D.E. 9 (Raees).
299. Amended FAA Motion, supra note 298, at 3–4.

I would like to have someone here maybe, you know, from the Solicitor General’s Office who took the position in front of the Supreme Court that, “Hey, Supreme Court, dcn’t rule on this now because, you know, these people don’t have standing,” but some day there is going to be somebody who is going to have standing, and they are going to be able to come before the Supreme Court, and now we have got some folks here who may have standing, but you don’t want to tell them they have standing.

304. Id. at 12; see Smith v. Maryland, 442 U.S. 735 (1979).
The defendants were indicted in San Diego late in 2010 for sending money to support Al-Shabaab in Somalia. A jury found them guilty on February 22, 2013. Appeals are pending.

*Directoral Clapper’s Letter*

James Clapper, the Director of National Intelligence provided Senator Wyden with a letter on March 28, 2014, explaining that “NSA sought and obtained the authority to query information collected under Section 702 of the Foreign Intelligence and Surveillance Act (FISA), using U.S. person identifiers,” and “[t]hese queries were performed pursuant to minimization procedures approved by the FISA Court as consistent with the statute and the Fourth Amendment.”

*Reform*

On December 12, 2013, the President’s Review Group on Intelligence and Communications Technologies issued a 303-page report presenting 46 recommendations for surveillance reform. One month later, Judge Bates, who had been appointed Director of the Administrative Office of the U.S. Courts as of July 1, 2013, submitted to Congress a report on behalf of the judiciary urging moderation in any reforms that would substantially change the work of the FISA court.


At a televised address to the Justice Department on January 17, 2014, President Obama announced that he was “ordering a transition that will end the Section 215 Bulk metadata program as it currently exists, and establish a mechanism that preserves the capabilities we need without the government holding this bulk metadata.”

Among the ordered changes, the President decided that the NSA’s extensive database of who has called whom now “can be queried only after a judicial finding or in the case of a true emergency.” On February 6, the Director of National Intelligence reported that the FISA court had approved such a change in procedures.

President Obama ordered the Attorney General and the intelligence community to present by March 28 alternatives to the NSA’s maintaining the metadata database. On March 25, newspapers reported that a proposal in development would cease the government’s bulk harvesting of metadata and rely on individual orders for metadata customarily held by telecommunication companies.

The House of Representatives’ Permanent Select Committee on Intelligence proposed to the House on May 8 a Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet Collection, and Online Monitoring Act (USA FREEDOM Act), which would modify the NSA’s surveillance authority. Judge Bates, on May 13, asked that the committee’s report include another letter by him on behalf of the judiciary recommending that Congress not impose on the FISA court “a permanent institution of a public advocate or impose[e] an adversarial process in the general run of cases” or create a requirement for public summaries of secret FISA court opinions, because summaries in the absence of access to the originals could be misleading. Judge Bates expressed


similar sentiments in an August 5 letter to Senate Judiciary Committee Chair Patrick Leahy, explaining that while occasional amicus curiae participation in FISA court proceedings could be helpful, a special advocate would interfere with the court’s special ex parte relationship with the government.  

---


Sealing Court Records and Proceedings:
A Pocket Guide

Robert Timothy Reagan

Federal Judicial Center
2010

This Federal Judicial Center publication was undertaken in furtherance of the Center’s statutory mission to develop and conduct research and education programs for the judicial branch. The views expressed are those of the author and not necessarily those of the Federal Judicial Center.
Table of Contents

Introduction ................................................................. 1
The Public Right of Access ........................................... 2
   The Common Law and the First Amendment .................. 2
   The Sixth Amendment ............................................. 4
Specific Record and Proceeding Issues ......................... 5
   National Security .................................................. 6
   Grand Jury Proceedings .......................................... 6
   Juveniles ............................................................. 7
   False Claims Act ................................................... 7
   Criminal Justice Act .............................................. 8
   Personal Identifiers ................................................ 9
Search Warrants ...................................................... 10
Discovery ............................................................... 11
Pleas ...................................................................... 12
Voir Dire ................................................................. 13
Trial Evidence ......................................................... 14
Sentencing ................................................................. 15
Settlement Agreements ............................................. 16
General Considerations ............................................... 17
   Discretion .......................................................... 17
   Appeals .............................................................. 18
   Storage .............................................................. 19
Procedural Checklist ................................................ 19
Introduction

Essential to the rule of law is the public performance of the judicial function. The public resolution of court cases and controversies affords accountability, fosters public confidence, and provides notice of the legal consequences of behaviors and choices.

On occasion, however, there are good reasons for courts to keep parts of some proceedings confidential. Courts will keep confidential classified information, ongoing investigations, trade secrets, and the identities of minors, for example.

The public in general and news media in particular have a qualified right of access to court proceedings and records. This right is rooted in the common law. The First Amendment also confers on the public a qualified right of access. In 1980, the Supreme Court held that the First Amendment right of access to court proceedings includes the public’s right to attend criminal trials. The Court suggested that a similar right extends to civil trials, but they were not at issue in the case. Some courts of appeals have held that the public’s First Amendment right of access to court proceedings includes both criminal and civil cases.

The process used by courts to keep some of their proceedings and records confidential is generally referred to as seal-

---

3. Id. at n.17.
Sealing Court Records and Proceedings: A Pocket Guide

If a proceeding is sealed, often referred to as closed, it is not open to the public. Usually that means that any transcript made of the proceeding will be regarded as a sealed record. Clerks of court traditionally protected sealed filings and records by storing them separately from the public case file in a secure room or vault. As court records have become more electronic in form, electronic methods of security have been developed.

The Public Right of Access

The common law and the Constitution afford the public a qualified right of access to judicial records and proceedings. The Constitution affords a criminal defendant both a right to public proceedings and limited protection from public proceedings.

The Common Law and the First Amendment

If the public has a First Amendment right of access to a court proceeding or record, then sealing the proceeding or record to preserve confidentiality must be narrowly tailored to a compelling confidentiality interest. Some courts have said that the

5. This pocket guide discusses the sealing of court proceedings and records. It does not discuss the related issue of protective orders, which are orders that courts issue requiring parties to keep their own records confidential.

Sealing Court Records and Proceedings: A Pocket Guide

First Amendment right of access requires a higher showing of the need for confidentiality than the common-law right of access. The common-law right of access requires a balancing of the need for confidentiality against the public's strong right of access to court proceedings and records. Some courts have said that even under the common law, sealing requires narrow tailoring or a compelling showing.

Courts have articulated a two-prong test to determine whether a public right of access is rooted in the First Amendment. The history, or experience, prong is an analysis of whether the proceeding has historically been open. The logic, or function, prong is an analysis of whether the right of access fosters good operation of the courts and the government. Some

---

7. Lugosch, 435 F.3d at 124; In re Cendant Corp., 260 F.3d 183, 198 n.13 (3d Cir. 2001); In re Baltimore Sun Co., 886 F.2d 60, 64 (4th Cir. 1989); Valley Broadcasting Co. v. U.S. Dist. Court, 798 F.2d 1289, 1293 (9th Cir. 1986).


10. In re Providence Journal Co., 293 F.3d 1, 10 (1st Cir. 2002); Pintos v. Pacific Creditors Assoc., 565 F.3d 1106, 1115 (9th Cir. 2009).

11. In re Reporters Comm. for Freedom of the Press, 773 F.2d 1325, 1331–32 (D.C. Cir. 1985); Lugosch, 435 F.3d at 120; United States v. Simone, 14 F.3d 833, 837 (3d Cir. 1994); In re Baltimore Sun Co., 886 F.2d at 64; United States v. Corbitt, 879 F.2d 224, 237 (7th Cir. 1989); Phoenix Newspapers, Inc. v. U.S. Dist. Court, 156 F.3d 940 (9th Cir. 1998).
courts of appeals have determined that the constitutional right of access requires both a historical and a logical foundation.\textsuperscript{12}

In practical terms, it may be of little consequence whether a right of access is rooted in the First Amendment or "only" in the common law. It may be a rare situation in which the need for confidentiality is strong enough to outweigh the common-law right of access, but the need for confidentiality is not compelling enough to overcome the First Amendment right of access and the court has determined that the First Amendment does not apply to the proceeding or record. On the other hand, some courts of appeals have said that appellate review of sealing decisions under the First Amendment is more searching than appellate review of sealing decisions under the common law.\textsuperscript{13}

\textbf{The Sixth Amendment}

The Sixth Amendment guarantees "[i]n all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury . . . ."\textsuperscript{14}

Courts have recognized limited exceptions to the defendant's right to a completely public trial. For example, it can be permissible to close the courtroom to the public while taking testimony from a witness whose safety would be endangered if the testimony were public.\textsuperscript{15} Courts sometimes permit light

\textsuperscript{12} In re Reporters Committee, 773 F.2d at 1332; Phoenix Newspapers, Inc., 156 F.3d at 946.

\textsuperscript{13} In re Providence Journal Co., 293 F.3d at 10; United States v. Smith, 123 F.3d 140, 146 (3d Cir. 1997); EEOC v. Westinghouse Elec. Corp., 917 F.2d 124, 127 (4th Cir. 1990).

\textsuperscript{14} Emphasis added.

\textsuperscript{15} Brown v. Kuhlmann, 142 F.3d 529, 531, 533, 537–38, 544 (2d Cir. 1998) (noting that the transcript, in which the witness, an undercover police officer, was identified only by his badge number, was neither sealed nor
Sealing Court Records and Proceedings: A Pocket Guide

disguise or visual screening of the witness instead of full closure of the courtroom. 16
Although the Sixth Amendment guarantees a public trial, it also guarantees a fair trial. 17 Sometimes the right to a fair trial is served by withholding from the public, from which the jury will be drawn, preliminary information about the case. 18 One court of appeals approved a district court’s delaying until the end of the trial the public release of evidentiary sidebar conferences, noting that one juror had already been excused because he had seen inadmissible evidence in the press. 19

Specific Record and Proceeding Issues

Some sealing issues have arisen frequently enough for case law about them to be developed. Some types of information are understood to be properly protected by sealing, such as national security secrets. Some proceedings are understood to be properly held in secret, such as grand jury proceedings. The identities of some parties, such as juveniles, are properly protected by sealing or redaction. The following are summaries of the case law pertaining to several such issues.

redacted, and the witness’s testimony occupied less than six pages of the transcript, which was over 900 pages long.


Sealing Court Records and Proceedings: A Pocket Guide

National Security

On rare occasions, adjudication of a case requires presenting to the court classified information, which is information an intelligence agency has determined could result in damage to national security if it were disclosed to the wrong person.\textsuperscript{20} The Executive Branch decides access and storage limits for classified information.\textsuperscript{21} The public is given access to cases involving classified information by redacting the classified information from the public record.\textsuperscript{22}

Grand Jury Proceedings

Grand jury proceedings are held in secret.\textsuperscript{23} Sometimes, however, justice may require the availability of portions of grand jury records for other proceedings.\textsuperscript{24} In addition, one court of appeals found a qualified right of "access to ministerial records in the files of the district court having jurisdiction of the grand jury."\textsuperscript{25}

Judicial proceedings ancillary to grand jury proceedings often arise. For example, a witness may move to quash a grand jury subpoena, or the government may initiate contempt pro-

\textsuperscript{20} See Robert Timothy Reagan, Keeping Government Secrets: A Pocket Guide for Judges on the State-Secrets Privilege, the Classified Information Procedures Act, and Court Security Officers 1–2 (Federal Judicial Center 2007) [hereinafter Keeping Government Secrets]; see also Reagan, supra note 16 (providing case examples of how courts have protected national security).

\textsuperscript{21} See Reagan, Keeping Government Secrets, supra note 20, at 3, 19.

\textsuperscript{22} E.g., United States v. Ressam, 221 F. Supp. 2d 1252 (W.D. Wash. 2002).


\textsuperscript{24} Douglas Oil Co., 441 U.S. at 219–20.

\textsuperscript{25} In re Special Grand Jury, 674 F.2d 778, 781 (9th Cir. 1982).
ceedings against an uncooperative witness. Such judicial proceedings are often conducted under seal, but it has been held that there should be a public record of such proceedings and that only parts of the record should be sealed as necessary to protect grand jury secrecy.

**Juveniles**

Courts must protect the identities of juvenile defendants in criminal cases, unless they are tried as adults. Some courts seal the entire case, but protection of the juvenile's identity can also be accomplished by using initials for the juvenile's name and sealing or redacting filings as necessary.

The identities of minors who are parties in civil cases can also be protected by using their initials and sealing documents that must include their complete names.

**False Claims Act**

The False Claims Act permits persons to file qui tam actions on behalf of the government against entities that the filers claim have defrauded the government. Such an action is filed initially under seal, without notice to the defendant, to give the government time to investigate the complaint and decide

28. 18 U.S.C. §§ 5038(a), (e).
whether or not to take the lead in the action. The statute provides for a 60-day seal, but the government frequently requests long extensions of time to decide whether or not to intervene.

After the government decides whether or not to intervene, the complaint is unsealed and served on the defendant. Sometimes courts grant the government’s request to keep sealed court filings pertaining to the government’s investigation, such as materials supporting motions for extensions of time.

If the government decides not to intervene, the qui tam filer, known as the relator, may determine that the action is unlikely to lead to a monetary recovery and may decide to dismiss the action voluntarily, or the parties may settle the case. Sometimes a party will ask the court to keep the whole action permanently sealed. Courts typically deny this request. Closed False Claims Act cases ordinarily should not be sealed.

Criminal Justice Act

When a court appoints and supervises counsel for an indigent criminal defendant, the court is not exercising the judicial function at the core of the common-law and constitutional rights of public access. The Criminal Justice Act, however, affords the

32. Id. § 3730(b)(2).
34. E.g., United States ex rel. Herrera v. Bon Secours Cottage Health Servs., 665 F. Supp. 2d 782, 785 (E.D. Mich. 2008) (“there is nothing in the FCA suggesting that the initial seal was imposed to protect the identity of the relator or that qui tam complaints in which the Government decides not to intervene should be permanently sealed”); United States ex rel. Permison v. Superlative Techs., Inc., 492 F. Supp. 2d 561, 564 (E.D. Va. 2007) (“the presumption in favor of public access to court filings is especially strong where, as here, the filings involve matters of particular concern to the public, such as allegations of fraud against the government”).
35. E.g., In re Boston Herald, Inc., 321 F.3d 174, 191 (1st Cir. 2003) (“neither the First Amendment nor the common law provides a right of ac-
Sealing Court Records and Proceedings: A Pocket Guide

public a qualified right of access to information about funds spent pursuant to the Act.\textsuperscript{36}

Court approval of defense expenses in appointed-counsel cases, especially expenses for services other than counsel, is usually an ex parte process so that the confidentiality of the defendant’s litigation strategy is protected.\textsuperscript{37} However, the Antiterrorism and Effective Death Penalty Act of 1996 requires, in capital cases, a “proper showing” of a need for confidentiality to conduct ex parte proceedings concerning the approval of expenses for investigators, experts, and other service providers.\textsuperscript{38}

Public disclosure of appointed-counsel expenses is often delayed until after judicial proceedings pertaining to the case are completed.\textsuperscript{39}

\textbf{Personal Identifiers}

In light of court files’ now being available for inspection on the Internet, federal rules of practice and procedure provide that certain identifiers be redacted in court filings: minors should be represented by their initials; Social Security, taxpayer-

\begin{itemize}
  \item \textsuperscript{36} 18 U.S.C. § 3006A(d)(4), (e)(4).
  \item \textsuperscript{37} \textit{Id.} § 3006A(e)(1); 7A Guide to Judiciary Policy §§ 310.30, 640.20.
  \item \textsuperscript{39} 7A Guide to Judiciary Policy § 510.40.
\end{itemize}

9
identification, and financial-account numbers should be represented by the last four digits only; and only years should be given in birth dates. The Federal Rules of Criminal Procedure extend this protection to a home address, which should be represented by the city and state only. The rules provide for optional filing of more complete unredacted information under seal, in the form of either unredacted versions of the redacted filings or separate reference lists.

Search Warrants

Law enforcement entities typically obtain search warrants from magistrate judges in ex parte proceedings that often are sealed to protect the confidentiality of ongoing investigations. This is a temporary justification for sealing, although for some information in supporting affidavits permanent redaction from the public record may be justified.

Some courts have held that the public has a qualified right of access to judicial records of search warrants and their supporting documentation, once temporary reasons for keeping them sealed have expired.

42. Fed. R. Bankr. P. 9037(e)–(f); Fed. R. Civ. P. 5.2(f)–(g); Fed. R. Crim. P. 49.1(f)–(g).
Sealing Court Records and Proceedings: A Pocket Guide

Some local rules provide that search warrant files are public records unless otherwise ordered. Other local rules provide for keeping search warrant files under seal.

Discovery

Information exchanged by the parties during discovery is not subject to a First Amendment or common-law public right of access. If the fruits of discovery are filed in conjunction with a dispositive motion, a qualified right of access attaches. If


46. Seattle Times Co. v. Rhinehart, 467 U.S. 20, 33 (1984) ("pretrial depositions and interrogatories are not public components of a civil trial"); Cipollone v. Liggett Group, Inc., 785 F.2d 1108, 1118–20 (3d Cir. 1986) (the standard for issuing a discovery protective order is good cause; First Amendment concerns are not a factor); In re Gannett News Serv., Inc., 772 F.2d 113, 116 (5th Cir. 1985) ("The results of pretrial discovery may be restricted from the public."); Bond v. Utreras, 585 F.3d 1061, 1066 (7th Cir. 2009) ("[T]here is no constitutional or common-law right of public access to discovery materials exchanged by the parties but not filed with the court. Unfiled discovery is private, not public."); Pintos v. Pacific Creditors Ass., 565 F.3d 1106, 1115 (9th Cir. 2009) ("[d]iscovery documents are not part of the judicial record"); United States v. Anderson, 799 F.2d 1438, 1441 (11th Cir. 1986) ("Discovery, whether civil or criminal, is essentially a private process because the litigants and the courts assume that the sole purpose of discovery is to assist trial preparation.").

47. Joy v. North, 692 F.2d 880, 893 (2d Cir. 1982) ("documents used by parties moving for, or opposing, summary judgment should not remain under seal absent the most compelling reasons"); Rushford v. New Yorker Magazine, Inc., 846 F.2d 249, 252 (4th Cir. 1988) ("if the case had gone to trial and the documents were thereby submitted to the court as evidence, such documents would have been revealed to the public and not protected"); Baxter Int'l, Inc. v. Abbott Labs., 297 F.3d 544, 546 (7th Cir.
they are attached to a filing in conjunction with a discovery motion, however, the public right of access is substantially diminished.48

**Pleas**

Courts have found a qualified right of access to plea agreements49 and plea hearings.50


48. Anderson v. Cryovac, Inc., 805 F.2d 1, 11–13 (1st Cir. 1986); Leucadia, Inc. v. Applied Extrusion Techs., Inc., 998 F.2d 157, 165 (3d Cir. 1993) ("we hold there is a presumptive right to public access to all material filed in connection with nondiscovery pretrial motions, whether these motions are case dispositive or not, but no such right as to discovery motions and their supporting documents"); Phillips v. Gen. Motors Corp., 307 F.3d 1206, 1213 (9th Cir. 2002); see D. Alaska Civ. R. 5.4(a)(4); W.D. Wash. Civ. R. 5(g)(2).

49. Washington Post v. Robinson, 935 F.2d 282, 292 (D.C. Cir. 1991) (vacating orders sealing the plea agreement of a criminal defendant cooperating in the prosecution of Mayor Barry for cocaine possession) ("Under the first amendment, plea agreements are presumptively open to the public and the press."); United States v. Haller, 837 F.2d 84, 85–89 (2d Cir. 1988) (holding that it was improper to seal the whole plea agreement but proper to redact one paragraph specifying the defendant’s obligation to testify before a grand jury); In re Copley Press, Inc., 518 F.3d 1022, 1026 (9th Cir. 2008) (finding a First Amendment right of access to a cooperation addendum to a plea agreement).

50. In re Washington Post Co., 807 F.2d 383, 389–90 (4th Cir. 1986); but see United States v. El-Sayegh, 131 F.3d 158, 159, 162 (D.C. Cir. 1997) (holding that the right of access does not attach until the plea agreement is
It is common for courts to temporarily seal records of criminal defendants' cooperation in order to protect the confidentiality of ongoing investigations, and to either temporarily or permanently seal records of cooperation to protect the safety of the cooperating defendants and the defendants' families.  

Some courts have local rules that call for the filing under seal of a plea supplement in all cases in which there is a plea agreement. If the defendant is a cooperator, then the document contains details of cooperation; if the defendant is not a cooperator, then the document is empty and there is no public clue concerning the defendant's cooperation. The rules for one district specify that the sealing of the supplement is temporary, unless the court orders otherwise.

**Voir Dire**

The Supreme Court has determined that the public has a qualified First Amendment right to attend jury voir dire in criminal trials. Balancing the public's right of access to jury selection against legitimate privacy interests of prospective jurors presents the court with the sometimes challenging obligation to keep confidential only what needs to be kept confidential.

---

filed as such; the public did not have a right of access to an agreement filed with a motion to seal it but withdrawn before the court ruled on the sealing motion.


52. D. Alaska Crim. R. 11.2(e), 32.1(e); D. Me. Crim. R. 111(b), 157.6(a)(10); N.D. & S.D. Miss. Crim. R. 49.1(B)(2); D.P.R. R. 111(b); D.S.D. Crim. R. 111.1.A.


To preserve fairness and at the same time protect legitimate privacy, a trial judge must at all times maintain control of the process of jury selection and should inform the array of prospective jurors, once the general nature of sensitive questions is made known to them, that those individuals believing public questioning will prove damaging because of embarrassment, may properly request an opportunity to present the problem to the judge in camera but with counsel present and on the record.

By requiring the prospective juror to make an affirmative request, the trial judge can ensure that there is in fact a valid basis for a belief that disclosure infringes a significant interest in privacy. This process will minimize the risk of unnecessary closure. The exercise of sound discretion by the court may lead to excusing such a person from jury service. When limited closure is ordered, the constitutional values sought to be protected by holding open proceedings may be satisfied later by making a transcript of the closed proceedings available within a reasonable time, if the judge determines that disclosure can be accomplished while safeguarding the juror’s valid privacy interests. Even then a valid privacy right may rise to a level that part of the transcript should be sealed, or the name of a juror withheld, to protect the person from embarrassment.\textsuperscript{55}

Trial Evidence

Courts have determined that a qualified right of public access attaches to evidence admitted at trial.\textsuperscript{56} In high-profile cases,

\textsuperscript{55} Press-Enterprise Co., 464 U.S. at 511–12.

\textsuperscript{56} Poliquin v. Garden Way, Inc., 989 F.2d 527, 532–34 (1st Cir. 1993); In re NBC, 635 F.2d 945, 952 (2d Cir. 1980); United States v. Criden, 648 F.2d 814, 823 (3d Cir. 1981); United States v. Guzzino, 766 F.2d 302, 303–04 (7th Cir. 1985); United States v. Massino, 356 F. Supp. 2d 227 (E.D.N.Y. 2005); United States v. Sampson, 297 F. Supp. 2d 342 (D. Mass. 2003); but see In re Providence Journal Co., 293 F.3d 1, 17 (1st Cir. 2002) (the news media did not have a right of access to original tapes, portions of which were played at trial); Littlejohn v. BIC Corp., 851 F.2d 673, 682–83 (3d Cir. 1988) (a newspaper did not have a right to copy trial exhibits that it
courts work with the parties to make copies of exhibits that are entered into evidence available to news media, to the extent practical, and courts often post these exhibits on their websites. Some courts have held that it is proper to deny news media the right to copy and broadcast audiovisual evidence so that the court can protect the fairness of a possible retrial or another defendant’s subsequent trial. A district court held that audiovisual recordings played at a motion hearing in a criminal case should not be released for broadcast until after the trial, but transcripts of the evidence were released publicly in advance of trial.

Sentencing

Courts have found qualified rights of access to sentencing. In one illustrative case, a district judge concluded that a psychiatric evaluation of the defendant submitted as part of the sentencing process should be publicly filed with limited redactions to protect the privacy of information on the defendant’s personal history that was not germane to sentencing.

---

57. United States v. Webbe, 791 F.2d 103, 107 (8th Cir. 1986).
58. Belo Broadcasting Corp. v. Clark, 654 F.2d 423, 425–26, 429, 431 (5th Cir. 1981); United States v. Edwards, 672 F.2d 1289, 1296 (7th Cir. 1982).
Sealing Court Records and Proceedings: A Pocket Guide

Presentence reports, however, are not considered judicial records to which the public has a right of access. 62

Settlement Agreements

Parties may wish to settle their cases according to confidential terms, and often there is no need to file settlement agreements. 63 Often, however, the agreement requires court approval or the parties wish to retain the court’s jurisdiction over enforcement. In those situations, the agreement may be filed, and then a qualified right of public access attaches. 64 As one court observed, “The public has an interest in knowing what terms of settlement a federal judge would approve and perhaps therefore nudge the parties to agree to.” 65

62. In re Siler, 571 F.3d 604, 610 (6th Cir. 2009) (presentence reports are not court documents: they are documents prepared by and maintained by the U.S. Probation Office, and they are released to courts for the limited purpose of sentencing); United States v. Corbitt, 879 F.2d 224, 239 (7th Cir. 1989) (“Only where a compelling, particularized need for disclosure is shown should the district court disclose [a presentence] report; even then, however, the court should limit disclosure to those portions of the report which are directly relevant to the demonstrated need.”); United States v. McKnight, 771 F.2d 388, 391 (8th Cir. 1985) (“Generally, pre-sentence reports are considered as confidential reports to the court and are not considered public records, except to the extent that they or portions of them are placed on the court record or authorized for disclosure to serve the interests of justice.”).

63. See generally Robert Timothy Reagan, Sealed Settlement Agreements in Federal District Court (Federal Judicial Center 2004).


65. Jessup v. Luther, 277 F.3d 926, 929 (7th Cir. 2002).
Sealing Court Records and Proceedings: A Pocket Guide

General Considerations

In the end, whether a judicial record should be sealed depends on the judgment and discretion of the presiding judge. Appellate review of sealing decisions is by interlocutory appeal in some circuits and by mandamus in others. Local rules concerning sealing often were crafted to help clerks clean out their vaults; for paper records, storage of sealed files was often a substantial burden.

Discretion

The court has discretion to weigh the need for secrecy against the public’s right of access.66 Court records should be sealed to keep confidential only what must be kept secret, temporarily or permanently as the situation requires. Sealing of judicial records is not considered appropriate if it is done merely to protect parties from embarrassment.67 Public versions of court documents are sometimes redacted, however, to protect the privacy interests of persons who are not parties, such as clients, employees, or witnesses.

66. In re Nat’l Broadcasting Co., 653 F.2d 609, 613 (D.C. Cir. 1981) (“Because of the difficulties inherent in formulating a broad yet clear rule to govern the variety of situations in which the right of access must be reconciled with legitimate countervailing public or private interests, the decision as to access is one which rests in the sound discretion of the trial court.”); Siedle v. Putnam Invs., Inc., 147 F.3d 7, 10 (1st Cir. 1998) (“The trial court enjoys considerable leeway in making decisions of this sort.”); San Jose Mercury News v. U.S. Dist. Court, 187 F.3d 1096, 1102 (9th Cir. 1999); United States v. McVeigh, 119 F.3d 806, 811 (10th Cir. 1997).

67. Siedle, 147 F.3d at 10; Kamakana v. City and County of Honolulu, 447 F.3d 1172, 1178–79 (9th Cir. 2006).
Appeals

Some courts of appeals have determined that they have jurisdiction to hear interlocutory appeals of trial court decisions to seal, to not seal, or to unseal judicial records. Other courts of appeals review district court sealing orders by mandamus. Appellate review is for abuse of discretion, but some courts of appeals have determined that review must be more searching than ordinary abuse-of-discretion review. Some courts have determined that appellate review of the constitutional right of access is more searching than appellate review of the common-law right of access.

68. United States v. Raffoul, 826 F.2d 218, 222 (3d Cir. 1987); In re Tribune Co., 784 F.2d 1518, 1521 (11th Cir. 1986).
69. McVeigh, 119 F.3d at 810 (noting that the Courts of Appeals for the First, Fourth, Eighth, and Ninth Circuits review district court sealing orders by mandamus and that the Courts of Appeals for the Second, Third, Fifth, Sixth, Seventh, and Eleventh Circuits review district court sealing orders by appeal).
70. In re Providence Journal Co., 293 F.3d 1, 10 (1st Cir. 2002).
71. Id. ("constitutional access claims engender de novo review"); United States v. Smith, 123 F.3d 140, 146 (3d Cir. 1997) ("[W]hen we deal with a First Amendment right of access claim, our scope of review of factual findings is substantially broader than that for abuse of discretion. With respect to the newspapers' common law right of access to judicial proceedings and papers, we review the district court's order for abuse of discretion.") (citations and quotation marks omitted); EEOC v. Westinghouse Elec. Corp., 917 F.2d 124, 127 (4th Cir. 1990) ("Under the common law the trial court's denial of access to documents is reviewed for abuse of discretion, but under the First Amendment, such denial is reviewed de novo and must be necessitated by a compelling government interest that is narrowly tailored to serve that interest.").
Sealing Court Records and Proceedings: A Pocket Guide

Storage

Some local rules provide presumptive time limits for sealing records, and these rules were motivated in substantial part by storage considerations. When case files were in paper form, before the advent of electronic filing, clerks of court kept sealed records in their vaults.72 When it was time to send case files to National Archives records centers, the clerks usually kept the sealed records, because the records centers were ill-equipped to keep records sealed.73

Many courts enacted local rules specifying a time limit after which sealed documents would be unsealed, returned, or destroyed. It is important to observe that the return or destruction of sealed documents makes them even less available to the public than they were when they were sealed but in the court’s care. Some local rules, therefore, provide for unsealing documents after the expiration of a time limit, unless the court orders otherwise, and do not list return or destruction as options.

Procedural Checklist

Courts generally require the following when a record is sealed or a proceeding is closed:

1. Absent authorization by statute or rule, permission to seal must be given by a judicial officer.

Clerks’ offices should not agree to seal a record unless directed to by a statute, rule, or court order.74 Also, sealing requires more than an agreement among the parties.75

72. See, e.g., In re Orion Pictures Corp., 21 F.3d 24, 26 (2d Cir. 1994).
74. See, e.g., United States v. Amodeo, 44 F.3d 141, 147 (2d Cir. 1995) (reviewing sealed reports by a special master, the court observed, “While
2. **Motions to seal should be publicly docketed.**

Public notice of motions to seal gives the public, the news media, and interested parties an opportunity to be heard on the matter.  

3. **Members of the news media and the public must be afforded an opportunity to be heard on motions to seal.**

Courts routinely permit non-parties to intervene for the purposes of challenging motions to seal.

we think that it is proper for a district court, after weighing competing interests, to edit and redact a judicial document in order to allow access to appropriate portions of the document, we consider it improper for the district court to delegate its authority to do so.”); Media Gen. Operations, Inc. v. Buchanan, 417 F.3d 424, 429 (4th Cir. 2005) (“The decision to seal documents must be made after independent review by a judicial officer, and supported by findings and conclusions specific enough for appellate review.”) (quotation marks omitted).

75. R&G Mortgage Corp. v. Fed. Home Loan Mortgage Corp., 584 F.3d 1, 12 (1st Cir. 2009) (“Sealing orders are not like party favors, available upon request or as a mere accommodation.”); see N.D. & S.D. Miss. Civ. R. 79(d).

76. See Washington Post v. Robinson, 935 F.2d 282, 289 (D.C. Cir. 1991); In re Herald Co., 734 F.2d 93, 102 (2d Cir. 1984); United States v. Criden, 675 F.2d 550, 554 (3d Cir. 1982); In re Washington Post Co., 807 F.2d 383, 390 (4th Cir. 1986); In re Knoxville News-Sentinel Co., 723 F.2d 470, 475 (6th Cir. 1983).

77. Washington Post, 935 F.2d at 289, 292; In re Globe Newspaper Co., 729 F.2d 47, 56 (1st Cir. 1984); United States v. Aref, 533 F.3d 72, 81 (2d Cir. 2008); United States v. Raffoul, 826 F.2d 218, 221–22 (3d Cir. 1987); In re Knight Publ’g Co., 743 F.2d 231, 234 (4th Cir. 1984); Ford v. City of Huntsville, 242 F.3d 235, 241 (5th Cir. 2001); In re Knoxville News-Sentinel Co., 723 F.2d 470, 475–76 (6th Cir. 1983); In re Associated Press, 162 F.3d 503, 507 (7th Cir. 1998); Phoenix Newspapers, Inc. v. U.S. Dist. Court, 156 F.3d 940, 949 (9th Cir. 1998); In re Tribune Co., 784 F.2c 1518, 1521 (11th Cir. 1986).
Sealing Court Records and Proceedings: A Pocket Guide

4. There should be a public record of permissions to seal.
There should be a public record of what is sealed and why, consistent with the reason for sealing.78

5. Sealing should be no more extensive than necessary.
Although it is often easier to seal more than is necessary, courts should be careful to seal only the portions of the record that require sealing.79 An entire case file should not be sealed to protect the secrecy of some documents. An entire filing should not be sealed to protect the secrecy of an exhibit. When possible, redacted versions of sealed documents should be filed.

78. Washington Post, 935 F.2d at 289; United States v. Haller, 837 F.2d 84, 87 (2d Cir. 1988) ("the fact that a sealing order [has] been entered must be docketed"); In re Associated Press, 162 F.3d at 510 ("Sealing of the entire explanation would indeed be an extraordinary step for a district court to take, given the heavy burden it would place on the Press . . . ."); In re Search Warrant, 855 F.2d 569, 575 (8th Cir. 1988) ("The fact that a closure or sealing order has been entered must itself be noted on the court’s docket, absent extraordinary circumstances."); cf. In re Washington Post Co., 807 F.2d 383, 391 (4th Cir. 1986) ("if the court concludes that a denial of public access is warranted, the court may file its statement of the reasons for its decision under seal"); In re Copley Press, Inc., 518 F.3d 1022, 1028 (9th Cir. 2008) (the public does not have a First Amendment right to documents explaining why something should be sealed if those documents contain secrets that the sealing is designed to protect).

publicly. Courts should be skeptical of arguments that following proper procedures is too burdensome.\footnote{80}

6. The record of what is sealed and why should be complete for appellate review.

The record of the case should include specific reasons for sealing and specific reasons for not employing more limited forms of secrecy, such as redacting a document instead of sealing the whole document.\footnote{81} If part of the record of what is sealed and why must itself be sealed to protect necessary secrecy, it should still be included in the case record for possible appellate review.

7. Records should be unsealed when the need for sealing expires.

Records are often sealed for a temporary purpose, and courts should follow procedures that ensure records become unsealed when they can be.\footnote{82}

\footnote{80}{See Banks v. Office of the Senate Sergeant-at-Arms, 233 F.R.D. 1, 10–11 (D.D.C. 2005).}

\footnote{81}{EEOC v. Nat’l Children’s Ctr., Inc., 98 F.3d 1406, 1410 (D.C. Cir. 1996); In re Globe Newspaper Co., 729 F.2d 47, 56 (1st Cir. 1984); In re Herald Co., 734 F.2d at 100; In re Knight Publ’g Co., 743 F.2d 231, 234–35 (4th Cir. 1984); In re Washington Post Co., 807 F.2d at 391; In re Associated Press, 162 F.3d at 510, 513 (“district courts should articulate on the record the reason for any order that inhibits the flow of information between the courts and the public.”); In re Search Warrant, 855 F.2d at 574.}

\footnote{82}{See United States v. Antar, 38 F.3d 1348, 1362 (3d Cir. 1994) (“Under the First Amendment, once an overriding interest initially necessitating closure has passed, the restrictions must be lifted.”); Phoenix Newspapers, Inc. v. U.S. Dist. Court, 156 F.3d 940, 948 (9th Cir. 1998) (“consistent with history, case law requires release of transcripts when the competing interests precipitating hearing closure are no longer viable”); United States v. Valenti, 987 F.2d 708, 714 (11th Cir. 1993).}
The Federal Judicial Center

Board
The Chief Justice of the United States, Chair
Judge Susan H. Black, U.S. Court of Appeals for the Eleventh Circuit
Judge David O. Carter, U.S. District Court for the Central District of California
Magistrate Judge John Michael Facciola, U.S. District Court for the District of Columbia
Judge James B. Haines, U.S. Bankruptcy Court for the District Maine
Judge Edward C. Prado, U.S. Court of Appeals for the Fifth Circuit
Judge Loretta A. Preska, U.S. District Court for the Southern District of New York
Judge Philip M. Pro, U.S. District Court for the District of Nevada
James C. Duff, Director of the Administrative Office of the U.S. Courts

Director
Judge Barbara J. Rothstein

Deputy Director
John S. Cooke

About the Federal Judicial Center

The Federal Judicial Center is the research and education agency of the federal judicial system. It was established by Congress in 1967 (28 U.S.C. §§ 620–629), on the recommendation of the Judicial Conference of the United States.

By statute, the Chief Justice of the United States chairs the Center’s Board, which also includes the director of the Administrative Office of the U.S. Courts and seven judges elected by the Judicial Conference.

The organization of the Center reflects its primary statutory mandates. The Education Division plans and produces education and training programs for judges and court staff, including satellite broadcasts, video programs, publications, curriculum packages for in-court training, and Web-based programs and resources. The Research Division examines and evaluates current and alternative federal court practices and policies. This research assists Judicial Conference committees, who request most Center research, in developing policy recommendations. The Center’s research also contributes substantially to its educational programs. The two divisions work closely with two units of the Director’s Office—the Systems Innovation & Development Office and Communications Policy & Design Office—using print, broadcast, and on-line media to deliver education and training and to disseminate the results of Center research. The Federal Judicial History Office helps courts and others study and preserve federal judicial history. The International Judicial Relations Office provides information to judicial and legal officials from foreign countries and assesses how to inform federal judicial personnel of developments in international law and other court systems that may affect their work.
National Security Case Management:
An Annotated Guide

Robert Timothy Reagan

Federal Judicial Center
2011

This Federal Judicial Center publication was undertaken in furtherance of the Center’s statutory mission to develop and conduct research and education programs for the judicial branch. The views expressed are those of the author and not necessarily those of the Federal Judicial Center.
## Contents

Table of Cases ........................................................................................................... v

Introduction .............................................................................................................. 1

### Part I

Classified Information .............................................................................................. 3

- The Classified Information Procedures Act .......................................................... 3
- Classified Information Security Officers ............................................................... 6
- Security Clearances for Court Staff ....................................................................... 7
- Security Clearances for Attorneys ......................................................................... 9
- Handling and Storing Classified Information ....................................................... 12
- Sharing Classified Information with Criminal Defendants .............................. 17
- Discovery .............................................................................................................. 18
- FISA Evidence ..................................................................................................... 19
- Civil Cases .......................................................................................................... 21
- Other Government Secrets .................................................................................. 22
- Filings and Proceedings ....................................................................................... 23
- State-Secrets Privilege ......................................................................................... 27
- Silent Witness Rule ............................................................................................. 28
- Special Judicial Resources ................................................................................. 28
- Courts of Appeals ............................................................................................... 29
- Putting the Cat Back in the Bag ........................................................................... 32

### Part II

Other Issues .............................................................................................................. 33

- Attorney–Client Issues ....................................................................................... 33
  - Criminal Justice Act Appointments .................................................................. 33
  - Conflicts of Interest ......................................................................................... 34
  - Communication .................................................................................................. 35
  - Rapport ............................................................................................................. 36
- Conditions of Detention ....................................................................................... 37
  - Security ............................................................................................................ 37
  - Access to Counsel ............................................................................................ 38
  - Mental Health .................................................................................................. 38
- Cultural Accommodation ...................................................................................... 39
- High Profile ........................................................................................................ 40
  - Gag Orders ....................................................................................................... 40
  - Media Attention ............................................................................................... 41
  - Reserved Seating ............................................................................................. 42
  - Remote Viewing ............................................................................................... 42
  - Courtroom Displays of Support or Opposition ................................................ 43
  - Making Filings and Evidence Available to News Media ................................. 43
- Courthouse Security ............................................................................................ 44
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jury Issues</td>
<td>45</td>
</tr>
<tr>
<td>Size of Venire</td>
<td>45</td>
</tr>
<tr>
<td>Anonymous Jury</td>
<td>46</td>
</tr>
<tr>
<td>Jury Questionnaire</td>
<td>47</td>
</tr>
<tr>
<td>Sequestration</td>
<td>49</td>
</tr>
<tr>
<td>News of National Security Events</td>
<td>50</td>
</tr>
<tr>
<td>Special Evidence Issues</td>
<td>51</td>
</tr>
<tr>
<td>Witness Security</td>
<td>51</td>
</tr>
<tr>
<td>Foreign Evidence</td>
<td>53</td>
</tr>
<tr>
<td>Examination of High-Security Detainees</td>
<td>55</td>
</tr>
<tr>
<td>Senior Government Officers</td>
<td>55</td>
</tr>
<tr>
<td>Pro Se Issues</td>
<td>56</td>
</tr>
</tbody>
</table>
Table of Cases

First World Trade Center Bombing
First World Trade Center Bombing

Plot to Bomb New York City Tunnels and Landmarks

Plot to Bomb U.S. Airplanes in Southeast Asia

Burma

Kenya and Tanzania
First Prosecution for 1998 Embassy Bombings
*United States v. El-Hage* (S.D.N.Y. 1:98-cr-1023) .............................. 8, 10, 17, 18, 24, 34, 35, 36, 37, 38, 40, 43, 44, 46, 47, 48, 50, 51, 56

Prosecution of a Guantánamo Bay Detainee for 1998 Embassy Bombings

Millennium Bomber
*United States v. Ressam* (W.D. Wash. 2:99-cr-666) and
*United States v. Haouari* (S.D.N.Y. 1:00-cr-15) ...................... 8, 14, 19, 35, 45, 46, 47, 50, 52, 54

Would-Be Spy
*United States v. Regan* (E.D. Va. 1:01-cr-405) ...................................... 10, 14

Detroit
*United States v. Koubrit* (E.D. Mich. 2:01-cr-80778) ...................... 8, 10, 14, 41, 46, 47, 49, 49, 56

Twentieth Hijacker
*United States v. Moussaoui* (E.D. Va. 1:01-cr-455) ............................ 10, 17, 24, 30, 32, 36, 40, 43, 45, 46, 47, 49, 57

American Taliban
*United States v. Lindh* (E.D. Va. 1:02-cr-37) .................................... 14, 19, 22, 52, 55

September 11 Damages
*In re Terrorist Attacks on September 11, 2001* (S.D.N.Y. 1:03-md-1570),
*In re September 11 Litigation* (S.D.N.Y. 1:21-mc-97), and
Related Actions .................................................................................. 14, 22, 28, 52

Guantánamo Bay
*In re Guantánamo Bay Detainee Litigation* (D.D.C. 1:08-mc-442) and
Related Actions .................................................................................. 11, 14, 17, 21, 22, 25, 29, 35, 39, 54, 56

Dirty Bomber
*Padilla v. Rumsfeld* (S.D.N.Y. 1:02-cv-4445),
*Padilla v. Hanft* (D.S.C. 2:04-cv-2221),
*Padilla v. Rumsfeld* (D.S.C. 2:07-cv-410),
*United States v. Hassoun* (S.D. Fla. 0:04-cr-60001), and
Related Actions .................................................................................. 8, 11, 14, 17, 19, 25, 30, 35, 38, 39, 45, 46, 47, 49, 49, 52

Lackawanna
*United States v. Goba* (W.D.N.Y. 1:02-cr-214) .................................... 33, 40, 42, 45

A Plot to Kill President Bush
*United States v. Abu Ali* (E.D. Va. 1:05-cr-53) .................................... 11, 14, 17, 30, 52, 54
Paintball

United States v. Royer (E.D. Va. 1:03-cr-296),
United States v. Al-Timimi (E.D. Va. 1:04-cr-385),
United States v. Chandia (E.D. Va. 1:05-cr-401), and
United States v. Benkahla (E.D. Va. 1:06-cr-9) ........................................ 5, 11, 19, 25, 36, 40

Minneapolis

United States v. Warsame (D. Minn. 0:04-cr-29) ........................................ 5, 9, 11, 15, 20, 37, 38, 39

Mistaken Rendition

El-Masri v. Tenet (E.D. Va. 1:05-cv-1417) ................................................... 15, 21, 27, 31

Detainee Documents

ACLU v. Department of Defense (S.D.N.Y. 1:04-cv-4151) ............................... 9, 21, 25

Prosecution of a Charity

United States v. Holy Land Foundation (N.D. Tex. 3:04-cr-240) ................. 9, 11, 15, 17, 20, 34, 49, 50, 52, 55

Chicago

United States v. Abu Marzook (N.D. Ill. 1:03-cr-978) ............................. 5, 9, 11, 15, 25, 37, 47, 53, 55

Giving State Secrets to Lobbyists

United States v. Franklin (E.D. Va. 1:05-cr-225) ...................................... 5, 9, 11, 15, 23, 26, 28, 31, 56

Lodi

United States v. Hayat (E.D. Cal. 2:05-cr-240) ........................................ 6, 9, 11, 19, 26

Warrantless Wiretaps

Hepting v. AT&T (N.D. Cal. 3:06-cv-672),
In re NSA Telecommunication Records Litigation (N.D. Cal. 3:06-md-1791),
Al-Haramain Islamic Foundation v. Bush (D. Or. 3:06-cv-274),
ACLU v. NSA (E.D. Mich. 2:06-cv-10204),
Terkel v. AT&T (N.D. Ill. 1:06-cv-2837),
Center for Constitutional Rights v. Bush (S.D.N.Y. 1:06-cv-313),
Electronic Privacy Information Center v. Department of Justice (D.D.C. 1:06-cv-96),
Electronic Frontier Foundation v. Department of Justice (D.D.C. 1:07-cv-403), and
Related Actions .......................................................................................... 9, 12, 15, 21, 26, 27, 29, 31, 32

Toledo

United States v. Amawi (N.D. Ohio 3:06-cr-719) and
Related Actions ......................................................................................... 20, 36, 37, 38, 45, 47, 48, 50, 53

Atlanta


Sears Tower

United States v. Batiste (S.D. Fla. 1:06-cr-20373) ....................................... 16, 47, 48, 50

Fort Dix

United States v. Shnewer (D.N.J. 1:07-cv-459) .......................................... 9, 12, 16, 17, 20, 27, 33, 42, 43, 44, 45, 47, 48, 50

Torture Flights

Mohamed v. Jeppesen DataPlan, Inc. (N.D. Cal. 5:07-cv-2798) ....................... 16, 22, 28, 31

National Security Case Management (2011)
Introduction

National security cases come in many types, including terrorism prosecutions, espionage prosecutions, and actions against the government concerning programs cloaked in secrecy.

A significant challenge faced by courts presiding over national security cases is the handling of classified information. Court proceedings and records are presumptively public, but courts are familiar with sealing selected proceedings and records to protect important secrets. Classified information, however, is a special type of secret, and its protection is controlled by the executive branch. Generally speaking, access to classified information requires a security clearance granted by the executive branch and a determination by the executive branch that the person granted access has a “need to know.” Article III judges have automatic security clearances.

Other challenges that arise in national security cases, especially criminal prosecutions, are often very similar to issues that arise in other cases, but they can occur more frequently and be more serious. For example, special security measures used for detainees awaiting trial can be similar to measures used in other cases, but they are often on the extreme end of the scale for such measures. Attorney-client rapport issues in terrorism prosecutions are often among the most challenging. National security cases are also often among the highest in profile.

This annotated guide describes special case-management issues that typically arise in national security cases. Guide text is followed by instructive examples drawn from a selection of cases that are more fully described in a companion publication, National Security Case Studies: Special Case-Management Challenges (Federal Judicial Center 2011).

National Security Case Studies includes an illustrative and instructive selection of cases concerning national security issues that have appeared in Article III courts. Many of the lessons derived from these cases came from close examinations of the case files and from interviews with presiding judges—especially with respect to case-management issues that are not always written up in published opinions.

The case note headings here correspond to chapter titles in the Case Studies, with a few exceptions: The Case Studies chapter on the “First World Trade Center Bombing” includes the prosecution for the bombing itself as well as related prosecutions for a “Plot to Bomb New York City Tunnels and Landmarks” and a “Plot to Bomb U.S. Airplanes in Southeast Asia.” The Case Studies chapter titled “Kenya and Tanzania” includes the “First Prosecution for 1998 Embassy Bombings” and a much later “Prosecution of a Guantánamo Bay Detainee for 1998 Embassy Bombings.”

The electronic version of this publication appearing at FJC Online (http://cwn.fjc.dcn, on the federal judiciary’s intranet) includes hyperlinks to relevant sections of the Case Studies and to other references. The electronic version of the publication appearing on the Internet (at http://www.fjc.gov) does not include hyperlinks.
Part I
Classified Information


There are three levels of classification. “Confidential” information is “information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.” Exec. Order No. 13,526, supra, § 1.2(a)(3). “Secret” information is “information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security . . . .” Id. § 1.2(a)(2) (emphasis added). “Top secret” information is “information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security . . . .” Id. § 1.2(a)(1) (emphasis added).

The designation “confidential” is used infrequently. Most classified information presented to courts is either secret or top secret.

The executive branch allows only persons with security clearances to see or handle classified information. A security clearance is a necessary condition, but it is not a sufficient condition. The executive branch also limits access to classified information to persons whom it has determined have a “need to know.”

In addition to being classified, information can be designated as “sensitive compartmented information” (SCI). Classified information that includes information about sources and methods is often “compartmented,” which means that there are additional restrictions placed on access to the information, including a more restrictive requirement of need to know. Sources and methods are valuable national security resources of general application, and so they are given extra protection.

A designation of “SCI” is in addition to a designation of confidential, secret, or top secret. With respect to access, handling, and storage, the designation of SCI is effectively a designation above top secret. Information designated “secret SCI,” for example, requires greater protection than top secret information that is not SCI.

The Classified Information Procedures Act

The Classified Information Procedures Act (CIPA), enacted in 1980, specifies procedures for the fair prosecution of criminal cases involving classified information. 18 U.S.C. app. 3 (2006). It does not, by its terms, apply to civil cases, but some of its provisions are often used as guidance for the handling of civil cases involving classified information.
In a terrorism prosecution, the government often has classified evidence against the defendant. The government may have additional discoverable classified information relevant to the case. In an espionage prosecution, the defendant may also have classified information relevant to the case, which the defendant may or may not contemplate introducing into evidence. These are but typical possibilities.

CIPA provides for how to incorporate classified information into a criminal case at both the discovery stage and at the trial or hearing stage. Each party has a duty to provide notice if classified information is at issue. Id. §§ 5(a), 6(b). Case-specific details are typically addressed at a pretrial conference:

At any time after the filing of the indictment or information any party may move for a pretrial conference to consider matters relating to classified information that may arise in connection with the prosecution. Following such motion or on its own motion the court shall promptly hold a pretrial conference . . . .

Id. § 2.

As in any criminal case, the court may be called on to rule on whether information in the government’s possession is discoverable. In a CIPA case, the court is also frequently called on to decide whether classified information in discovery can be fairly (1) omitted, (2) summarized, or (3) substituted with an admission.

The court, upon a sufficient showing, may authorize the United States to delete specified items of classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure, to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove. Id. § 4.

The court’s consideration of whether to limit discovery of classified information or authorize substitutions is typically ex parte, but a record must be preserved for appeal. Id.

The court customarily issues a protective order requiring the defense to preserve the secrecy of classified information, and the protective order may limit what information can be shared with the defendant by defense counsel. See id. § 3.

At a public hearing or trial, the court may authorize the substitution for classified evidence of either (1) a summary or (2) an admission, so long as the substitution “will provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information.” Id. § 6(c)(1). A hearing on this issue may be conducted in camera, id., and the court may receive information from the government “explaining the basis for the classification of such information” ex parte, id. § 6(c)(2).

Any ruling adverse to the government respecting access to classified information, including a sanction for denying access to classified information, may be resolved by expedited interlocutory appeal. Id. § 7.

If a fair trial necessitates the disclosure of classified information, and the government refuses to disclose the classified information, then the remedy is dismissal of the case or dismissal of one or more counts. Id. § 6(e).
It is also possible for the government to declassify information. This typically requires negotiation between two parts of the executive branch: the intelligence community and the prosecution. At one proceeding, the U.S. attorney observed that “the intelligence community always wants the Government to wait as long as it possibly can before it declassifies or gets substitutions because every step in that direction poses some risk of disclosure of sources, even if we do substitutions.” Transcript at 16, United States v. Ahmed, No. 1:06-cr-147 (N.D. Ga. Sept. 18, 2008, filed Sept. 23, 2008).

CASE NOTES

Paintball
In the prosecution of Ali al-Timimi, the spiritual leader of northern Virginia men who played paintball in preparation for violent jihad, the defendant filed a CIPA motion to use classified information at trial. The judge issued a sealed protective order after a sealed CIPA hearing.

Minneapolis
Because of a plea agreement, the case against Mohamed Abdullah Warsame, who was indicted for attending Al-Qaeda training camps, never went to trial, but part of the government’s case relied on classified evidence. The government was willing to declassify some of the evidence. Pursuant to CIPA, the government asked the judge to approve unclassified substitutions for other evidence. The judge compared all proposed substitutions with their corresponding originals and frequently asked for modifications.

Chicago
The prosecution of Muhammad Abdul Hamid Khalil Salah for helping to provide funds to Hamas involved a substantial amount of classified evidence. Pursuant to CIPA, the judge approved five admissions by the government as substitutions for classified evidence concerning Salah’s interrogation by Israeli agents while he was in Israeli custody. For example, the government offered to admit that Israel authorized its agents to use hoods, handcuffs, and shackles during interrogations. The judge found that the substitutions were consistent with the agents' previous testimony, and Salah would be able to question the agents at trial about his specific treatment. As the trial unfolded, Salah cross-examined the agents extensively, and the vast majority of the topics covered did not involve classified information.

To explain to the jury why some topics were being skirted during examination of the witnesses, the judge prepared a jury instruction to accompany presentation of the admissions:

This case involves certain classified information. Classified information is information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure. In lieu of disclosing specific classified information, I anticipate that you will hear certain substitutions for the classified information during this trial. These substitutions are admissions of relevant facts by the United States for purposes of this trial. The witnesses in this case as well as attorneys are prohibited from disclosing classified information and, in the case of the attorneys, are prohibited from asking questions to any witness which if answered would disclose classified information. Defendants may not cross-examine a particular witness regarding the underlying classified matters set forth in these admissions. You must decide what weight, if any, to give to these admissions.


Giving State Secrets to Lobbyists
In a sting prosecution of lobbyists for sharing classified information, CIPA governed many proceedings. Pursuant to section 5(a), the defendants gave notice of their intent to introduce classified evidence at trial. Pursuant to section 6, the judge “determined that a substantial volume of the classified information was indeed relevant and admissible.” United States v. Rosen, 557 F.3d 192, 195 (4th Cir. 2009). As permitted by section 6(c)(1), the
government proposed redactions and summaries as substitutions for the classified evidence. The judge approved some of the substitutions. "In some instances, the court concluded that less extensive redactions, or the use of replacements for particular names, places, or terms, would adequately protect the defendants' rights while simultaneously offering adequate protection for classified information."  *Id.* at 196.

The court of appeals heard expedited interlocutory appeals of the district judge’s CIPA rules, as provided by section 7 of CIPA.

*Lodi*
In the prosecution of Hamid Hayat for attending a terrorist training camp, and of his father Umer for lying about it, the government filed a notice that CIPA may apply to the case because of potentially discoverable classified evidence. In the end, the only classified evidence at issue was foundational to unclassified trial evidence, and the defense attorneys were willing to stipulate to the trial evidence’s admissibility.

*Atlanta*
In a prosecution of two young men in Atlanta for preparing for violent jihad by, among other things, making casing videos of strategic landmarks, some classified evidence had to be either declassified or substituted with court-approved summaries or admissions before it was presented at trial, and in some instances before it could be shared with defense counsel.

**Classified Information Security Officers**

The Department of Justice provides the courts with security experts who help the courts store and handle classified information and who help court staff and attorneys obtain security clearances.

CIPA provides for the designation of "classified information security officers," formerly and ambiguously known as "court security officers," to assist the court in keeping classified information secure.

Section 9 of CIPA calls for the Chief Justice to write procedural rules:

> Within one hundred and twenty days of the date of the enactment of this Act, the Chief Justice of the United States, in consultation with the Attorney General, the Director of National Intelligence, and the Secretary of Defense, shall prescribe rules establishing procedures for the protection against unauthorized disclosure of any classified information in the custody of the United States district courts, courts of appeal, or Supreme Court. Such rules, and any changes in such rules, shall be submitted to the appropriate committees of Congress and shall become effective forty-five days after such submission.


CIPA "Security Procedures," issued in 1981 by Chief Justice Burger and revised in 2010 by Chief Justice Roberts, specify how classified information security officers are designated:

2. *Classified Information Security Officer.* In any proceeding in a criminal case or appeal therefrom in which classified information is within, or is reasonably expected to be within, the custody of the court, the court will designate a "classified information security officer." The Attorney General or the Department of Justice Security Officer will recommend to the court a person qualified to serve as a classified information security officer. This individual will be selected from the Litigation Security Group, Security and Emergency Planning Staff, Department of Justice, to be detailed to the court to serve in a neutral capacity. The court may designate, as required, one or more alternate classified information security officers who have been recommended in the manner specified above.

The Justice Department has established a unit in its Management Division called the Litigation Security Group that consists of information security experts who are detailed to the courts. This unit is by design organizationally quite separate from the parts of the Justice Department that represent the government's interests in court cases. This unit, although expert in protecting classified information, is also separate from the intelligence community. It is to the Litigation Security Group whom courts should turn for guidance on matters relating to classified information. Although courts may be more familiar with the attorneys representing the government, it is the Litigation Security Group whose primary purpose is to provide the courts with neutral assistance. Their specific guidance is also superior to the general guidance presented here.

In a criminal case, if it is likely that the court will have to handle classified information, the Department of Justice Security Officer, who is the head of the department's Security and Emergency Planning Staff (SEPS), a unit in the Justice Management Division that includes the Litigation Security Group, recommends a security officer in the Litigation Security Group as the classified information security officer for the case. The recommendation is presented by letter to the presiding judge. Typically, the letter also recommends other security officers as alternates.

The presiding judge should appoint the security officer and alternates to the case by order. The judge may include this appointment in a protective order specifying defense attorneys' responsibilities in handling classified information. In a civil case involving classified information, the court should also contact the Litigation Security Group and appoint a classified information security officer to the case.

It is common for the security officer to deliver classified materials to the judge for in camera review. The security officer will advise the judge on security precautions for the review, such as keeping windows covered or doors closed. It is not necessary for security officers to watch a judge review classified material. Security officers generally remain available while a judge reviews classified material in private and return to the judge when the judge is finished reviewing the material.

Another important role of the security officer is to attend public proceedings in order to assist the court in preventing public disclosure of classified information.

**Security Clearances for Court Staff**

Article III judges are automatically cleared to see classified information necessary to the performance of their judicial function. 18 U.S.C. app. 3 § 9 note (2006); see Robert Timothy Reagan, *Keeping Government Secrets: A Pocket Guide for Judges on the State-Secrets Privilege, the Classified Information Procedures Act, and Court Security Officers* 3 (Federal Judicial Center 2007). Magistrate judges do not have automatic clearance, so they require a background check before they can have access to classified information. Because of the background check necessary to become a magistrate judge, this process typically takes a matter of
days. Background checks for other court personnel typically take a matter of months. In some cases, interim clearances can be granted while the background investigation is under way. Only United States citizens are eligible for security clearances.

The Litigation Security Group will facilitate security clearances for court personnel. Judges in courts that frequently have cases involving classified information commonly require their law clerks to obtain security clearances. It is useful to begin the clearance process when the law clerk is hired and not wait until the law clerk begins work.

Most courts have to deal with classified information only occasionally, so it is common for court personnel to seek security clearances only when a case requiring clearances presents itself. Court personnel who already have security clearances sometimes assist with cases to which they otherwise would not be assigned. Judges sometimes decide to work on classified information without staff assistance.

Levels of security clearance relevant to the court's work usually include (1) secret, (2) top secret, or (3) TS/SCI (top secret/sensitive compartmented information). A higher security clearance requires a more extensive background check. Because it is not always possible to know with precision in advance what level of classification will be involved in a case, the Litigation Security Group customarily initiates FBI background checks on court personnel sufficiently extensive for them to be cleared at the highest level if necessary.

Access to specific classified information is limited to persons with the appropriate security clearance and a "need to know." Occasionally, classified information is designated for judges' eyes only, and even law clerks with high security clearances cannot see the information.

CASE NOTES

First Prosecution for 1998 Embassy Bombings

In the original prosecution for the 1998 bombings of American embassies in Kenya and Tanzania, the district judges' law clerks had security clearances. Among the judges who heard the original defendants' appeals, one judge regularly asks his law clerks to obtain security clearances, but another judge has never had a law clerk obtain one.

Millennium Bomber

In the prosecution of Ahmed Ressam, who planned to bomb the Los Angeles International Airport at the turn of the millennium, the district judge reviewed classified material to determine whether it was discoverable. The judge did this without the assistance of a law clerk, because there was not enough time for a clerk to obtain a top-secret security clearance.

Detroit

To assess the extent of prosecutorial misconduct in the first post-September 11, 2001, prosecution for terrorism, the judge had to review the prosecution's entire case file, which included extensive classified information. All of the judge's staff obtained security clearances.

Dirty Bomber

The District of South Carolina district judge assigned to consider a habeas corpus petition by Jose Padilla—originally detained as an alleged dirty bomber but later tried for terrorism conspiracy—prepared for the possibility of classified evidence in the case by having his two law clerks, his judicial assistant, a courtroom deputy, and a court reporter obtain security clearances. Because Padilla's attorneys wanted his habeas petition decided on legal grounds rather than factual grounds, classified
evidence was never an important issue in the case, and it was not an issue at all during oral arguments. The judge examined some classified evidence at the court’s sensitive compartmented information facility (SCIF) in Charleston, but there was no need for his staff to do so.

The Southern District of Florida district judge who heard the criminal trial of Padilla and his two codefendants also had all of her staff obtain security clearances: her law clerks, her judicial assistant, her courtroom deputy, and her court reporter. During this case, the judge did not use interns, because they would not have security clearances.

**Minneapolis**

In the prosecution of Mohamed Abdullah Warsame for attending Al-Qaeda training camps, the district judge’s staff obtained security clearances. The district judge presided over pretrial matters that would ordinarily go to a magistrate judge so that another chambers’ staff would not have to obtain security clearances.

**Detainee Documents**

The Southern District of New York judge who heard a Freedom of Information Act case concerning extraterritorial detentions of terrorism suspects has all of his law clerks obtain security clearances. The clerks begin the process of obtaining clearances before they start work.

**Prosecution of a Charity**

The prosecution of the Holy Land Foundation and its principals for providing funds to Hamas required two trials because of a hung jury after the first one. Law clerks and other staff members for the judges presiding over both trials received security clearances.

**Chicago**

For a prosecution of Muhammad Abdul Hamid Khalil Salah for helping to provide funds to Hamas—a trial that involved a substantial amount of classified evidence relating to Salah’s imprisonment in Israel—the judge’s law clerks sought security clearances. Because the clearance process took a substantial fraction of the law clerks’ tenure, the judge handled classified issues without law clerk assistance. It was necessary, however, for a court reporter working on the case to have a security clearance.

**Giving State Secrets to Lobbyists**

The judge who presided over a sting prosecution of lobbyists for sharing classified information has a career law clerk with a security clearance. One of the judge’s temporary law clerks during the time of this case, however, was a Canadian citizen, so he was not eligible for a security clearance.

**Lodi**

For the prosecution of Hamid Hayat for attending a terrorist training camp, and of his father Umer for lying about it, the presiding judge’s court reporter obtained a security clearance, and as a backup precaution another court reporter at the courthouse did as well.

**Warrantless Wiretaps**

In actions challenging a secret and allegedly illegal surveillance program by the National Security Agency, all classified information presented to the court was designated by the government as for judges’ eyes only, and not even law clerks with security clearances were permitted to see it.

**Atlanta**

In a prosecution of two young men in Atlanta for preparing for violent jihad by, among other things, making casing videos of strategic landmarks, court staff had to obtain security clearances. This included magistrate judges, who do not have the same automatic security clearances as Article III judges.

**Fort Dix**

In a prosecution of six men for conspiracy to attack Fort Dix, all of the judge’s staff—law clerks, court reporters, courtroom deputies, and the judicial assistant—received security clearances. The judge observed that the clearance process went smoothly.

**Security Clearances for Attorneys**

If classified information is at least discoverable in a criminal case, it is customary for the defendant’s attorneys to have security clearances. In districts in which
such cases are common, there may be local criminal defense attorneys who already have security clearances. Often, the case at hand is an attorney’s first need for a clearance.

The Litigation Security Group can facilitate security clearances as needed for defense attorneys and for persons working with defense attorneys, such as paralegals and investigators. It is customary for obligations to preserve the secrecy of classified information to be specified in a protective order signed by the judge and in a memorandum of understanding signed by the persons granted clearance.

The Federal Judicial Center has assembled a selection of protective orders used in national security cases: National Security Prosecutions: Protective Orders. Judges should consult the classified information security officer when drafting national security protective orders.

In some cases, an attorney may be denied a security clearance or the attorney may decline to seek one. The court might replace the attorney unless there is another cleared attorney on the defense team, or the court might make a special appointment of a cleared attorney to work on issues in the case pertaining to classified information.

The Litigation Security Group can also facilitate security clearances for attorneys in civil cases, including habeas corpus cases. The government’s willingness to actually grant plaintiffs’ attorneys access to classified information in civil cases challenging the government depends on the circumstances of the case.

In any case involving classified information, it is often useful for the judge to meet jointly with attorneys and the classified information security officer early in the case.

CASE NOTES

First Prosecution for 1998 Embassy Bombings

In the original prosecution for the 1998 bombings of American embassies in Kenya and Tanzania, defense counsel had to have security clearances in order to have access to classified evidence. The court of appeals affirmed a district judge’s ruling that requiring security clearances for defense attorneys did not violate their clients’ Sixth Amendment rights. In re Terrorist Bombings of U.S. Embassies in East Africa, 552 F.3d 93, 119–28 (2d Cir. 2008); see United States v. Bin Laden, 58 F. Supp. 2d 113 (S.D.N.Y. 1999).

Would-Be Spy

In the prosecution of Brian Patrick Regan for attempted espionage, defense attorneys had security clearances, and the defendant himself was cleared to see some classified information related to the information he was accused of trying to sell. United States v. Regan, 281 F. Supp. 2d 795, 801 (E.D. Va. 2002).

Detroit

An assessment of prosecutorial misconduct in the first post-September 11, 2001, prosecution for terrorism required review of the prosecution’s entire case file, which included extensive classified information. Defense attorneys were required to obtain security clearances.

The district judge in this case recommends that a judge in a case that might include classified information meet early with attorneys to discuss how much classified information is at issue and who will need security clearances. It is important to establish contact with the Litigation Security Group as soon as it is known that the case might involve classified information.

Twentieth Hijacker

In the prosecution of Zacarias Moussaoui for terrorism conspiracy, the defendant’s attorneys obtained security clearances and signed a memorandum of understanding requiring that classified secrets be kept secret forever. Unit-
ed States v. Moussaoui, 591 F.3d 263, 267 (4th Cir. 2010).

Guantánamo Bay

Habeas attorneys representing Guantánamo Bay detainees needed security clearances to visit their clients.

Among the Guantánamo Bay detainees who filed habeas corpus petitions was Abu Zubaydah, a senior Al-Qaeda figure who was treated for frequent seizures. The district court ordered the government to grant Abu Zubaydah’s attorneys, who had security clearances, access to his medical records so that they could investigate whether side effects from medical treatment at Guantánamo Bay were interfering with his ability to communicate effectively with his attorneys, despite the government’s initial determination that portions would be redacted for lack of a need to know.

Dirty Bomber

In the trial of Jose Padilla, originally detained as a dirty bomber but ultimately tried with two other men for terrorism conspiracy, all defense attorneys received security clearances.

A Plot to Kill President Bush

In the prosecution of Ahmed Omar Abu Ali for terrorism conspiracy and conspiracy to kill the President, some of the evidence against the defendant was classified. One of the defendant’s attorneys was denied a security clearance and the other did not apply for one, so the court appointed an attorney who already had a clearance. United States v. Abu Ali, 528 F.3d 210, 248–49 (4th Cir. 2008). Only the cleared attorney, and not the defendant or either uncleared attorney, was allowed to see classified evidence or participate in hearings in which classified evidence was discussed.

Paintball

On appeal from the conviction of Ali al-Timimi, the spiritual leader of northern Virginia men who played paintball in preparation for violent jihad, the court of appeals remanded the case for an investigation of possibly discoverable surveillance. On remand, the government presented to the judge classified submissions that neither the prosecuting nor the defense attorneys were cleared to see. The judge issued an order that her law clerk and the attorneys be granted clearance to examine at least some of the secret submissions.

Minneapolis

In the prosecution of Mohamed Abdullah Warsame for attending Al-Qaeda training camps, the defendant’s attorneys obtained security clearances. The court initially appointed the federal defender’s office to represent Warsame. The defendant’s supporters, however, thought that retained counsel would provide better representation, so they hired a law professor in Chicago to represent Warsame. Because the professor could not identify local counsel likely to obtain a security clearance, the court kept the federal defender’s office as second counsel.

Prosecution of a Charity

In the prosecution of the Holy Land Foundation and its principals for providing funds to Hamas, defense attorneys received security clearances.

Chicago

In the prosecution of Muhammad Abdul Hamid Khalil Salah for helping to provide funds to Hamas—a prosecution that involved a substantial amount of classified evidence relating to Salah’s imprisonment in Israel—defense counsel elected not to seek security clearances, so the judge resolved evidentiary issues by holding ex parte conferences with defense counsel to determine their defense needs and ex parte conferences with government counsel to determine what classified information the government held.

Giving State Secrets to Lobbyists

In a sting prosecution of lobbyists for sharing classified information, defense attorneys had security clearances, and some witnesses for the defense also had security clearances.

Lodi

In the Sacramento prosecution of Hamid Hayat for attending a terrorist training camp, and of his father Umer for lying about it, the government filed a notice that it had potentially discoverable classified evidence. Defense attorneys did not want to obtain security clearances, so the judge looked for other local attorneys who already had clearances. The classified information security officer could not find a local defense attorney with a securi-
ty clearance, but he was able to identify two in a neighboring district who were cleared. Because the defendants were willing to stipulate to the admissibility of trial evidence that had classified information as part of its foundation, having cleared counsel ultimately was not necessary.

**Warrantless Wiretaps**

In an action challenging a secret and allegedly illegal surveillance program—an action arising from evidence of surveillance in a top-secret document mistakenly disclosed to an Islamic charity during proceedings to freeze the charity’s assets for allegedly funding terrorism—the plaintiffs were required to surrender all copies of the document, and they were forbidden by the government from having access to the copy they delivered to the court. *Al-Haramain Islamic Found. v. Bush*, 451 F. Supp. 2d 1215, 1217, 1229 (D. Or. 2006).

Attorneys representing the government told the court that they were not at liberty to disclose whether or not they had clearance to see the document.

The action was consolidated with other actions, for pretrial purposes, by the Judicial Panel on Multidistrict Litigation, and the transferee judge ordered the government to give the plaintiffs’ attorneys security clearances and access to the document. *In re NSA Telecomm. Records Litig.*, 595 F. Supp. 2d 1077, 1089–90 (N.D. Cal. 2009). Two attorneys for the plaintiffs received security clearances, but the government decided that pursuing the action against the government was not a sufficient “need to know” required for access to the document.

**Atlanta**

In a prosecution of two young men in Atlanta for preparing for violent jihad by, among other things, making casing videos of strategic landmarks, defense attorneys had to obtain security clearances.

**Fort Dix**

In a prosecution of six men for conspiracy to attack Fort Dix, the defense attorneys needed security clearances.

**Handling and Storing Classified Information**

Courts and attorneys for parties other than the federal government must rely on the Litigation Security Group for guidance on handling and storing classified information. Following are summary guidelines, but the classified information security officers provided by the Litigation Security Group are the experts.

Security requirements for classified information depend on the level of classification. A person handling classified information must have a security clearance at least as high as the information’s level of classification. Handling classified information includes not only reviewing it but also carrying it from a place of storage to a judge for review. A person handling top secret information, for example, must have at least a top secret security clearance, but only a secret security clearance is required to handle secret information. A TS/SCI security clearance is required to review SCI (sensitive compartmented information). In addition, access to classified information will be restricted to persons who “need to know.”

Classified information must not be reviewed in the presence of persons without an appropriate security clearance and must never be reviewed in public.

Classified documents are marked with the applicable level of classification. Each paragraph of a classified document should be marked with the level of classification for the paragraph: (U) for unclassified, (C) for confidential, (S) for secret, (TS) for top secret, and (TS/SCI) for top secret/sensitive compartmented information. The level of classification for a document is the highest level of classification among its parts.
Confidential, secret, and top secret material must be stored in an approved safe in a secure room. The classified information security officer will provide a suitable safe and will work with the court to identify or help establish a suitable room. Judges presiding over cases involving classified information typically keep a safe suitable for storing classified materials in their chambers. If defense attorneys need to review classified materials, the court and the classified information security officer typically identify a secure room for this purpose and establish a safe to store the materials.

SCI must be stored in a sensitive compartmented information facility (SCIF). A SCIF (customarily pronounced “skiff”) is a room, sometimes a building, that meets certain security specifications, such as slab-to-slab construction, special locks, and an alarm system connected to armed security guards. If a courthouse does not already have a SCIF, and it is determined that one is needed at the courthouse, then the classified information security officer will establish one, at the executive branch’s expense. 18 U.S.C. app. 3 § 9 note ¶12 (2006). Alternatively, the classified information security officer can often locate a SCIF nearby for the court’s use.

U.S. attorney offices and FBI offices often have SCIFs. Although judges sometimes express reluctance to use these for the court’s work, the classified information security officer can establish protective measures suitably limiting access to stored materials. If classified materials are stored in a SCIF for use by the court or a party opposing the government, and the SCIF is not under the court’s control, then the materials will be stored within the SCIF in a way that permits only the classified information security officer and the judge or attorney, as the case may be, to have access to the materials. Designated safes or locked bags are often used for this purpose.

Any document based on classified information, such as notes, briefs, and opinions, may be classified at the highest level of classification of the material on which the document is based. Storage requirements for the derivative document, therefore, may be the same as the storage requirements for the classified material on which it is based. Typically, the classified information security officer coordinates a security review to determine the level of classification, if any, for a derivative document.

Classified information cannot be discussed or transmitted by email or over a non-secure telephone line.

Court personnel with security clearances may transport classified material from the place of storage to the place of review for a judge or other persons.

CASE NOTES

*Plot to Bomb New York City Tunnels and Landmarks*

In the prosecution for a conspiracy to bomb New York tunnels and landmarks, the government presented six classified exhibits ex parte to the district judge, pursuant to CIPA. *United States v. Rahman*, 870 F. Supp. 47, 49 (S.D.N.Y. 1994). The judge kept the exhibits in a safe while he considered whether they had to be produced to the defense. He ruled which exhibit had to be disclosed to the defense, ordered that it not be disclosed to anyone else, and ordered that all of the exhibits be kept under seal with the classified information security officer.
Millennium Bomber
In the prosecution of Ahmed Ressam, who planned to bomb the Los Angeles International Airport at the turn of the millennium, the district judge reviewed classified materials to determine whether the materials were discoverable. The judge kept the materials in a safe to which the classified information security officer, but not the judge, had access. The judge preferred not to have to deal with the lock and combination himself.

Would-Be Spy
In the prosecution of Brian Patrick Regan for attempted espionage, the government discovered in the defendant’s jail cell what appeared to be coded messages to his wife and children concerning the locations of hidden information. United States v. Regan, 281 F. Supp. 2d 795, 800, 804–05, 807 (E.D. Va. 2002). The government wanted to search the defense SCIF to look for evidence that the documents were improperly created on a computer there. The district judge did not allow the U.S. Attorney’s Office or the FBI to conduct the search; instead, he authorized the classified information security officers to conduct the search.

Detroit
An assessment of prosecutorial misconduct in the first post-September 11, 2001, prosecution for terrorism required review of the prosecution’s entire case file, which included extensive classified information. Classified information security officers created a SCIF in the courthouse. Only chambers staff with security clearances could enter this SCIF.

The judge also had to review extensive highly sensitive records maintained at CIA headquarters. He negotiated with the CIA’s general counsel to establish a protocol for use of the CIA’s evidence. Because many of the CIA records were too sensitive to transport to Michigan, the judge traveled to Virginia to review them.

American Taliban
In the prosecution of John Walker Lindh, who became known as the American Taliban, the government’s classified evidence that the district judge reviewed for discoverability was stored in the court’s SCIF. The judge’s law clerks typically obtain security clearances, and classified materials are kept within eyesight at all times.

September 11 Damages
In the consolidated civil actions against alleged supporters of the September 11, 2001, attacks, plaintiffs supported a discovery motion with anonymously leaked documents that the plaintiffs knew were sensitive and suspected might be classified. The attorneys delivered the documents to the court, sent copies to the U.S. attorney, and provided defendants with only a copy of the transmittal letter. The government determined that at least some of the documents were classified, so the court’s copies were securely stored. The plaintiffs were required to surrender their copies of the documents.

Guantánamo Bay
After news media reported that classified information about Guantánamo Bay detainees became available on the Internet as a result of unauthorized disclosures to WikiLeaks, cleared habeas attorneys for the detainees were admonished not to allow their knowledge of properly disclosed classified information to provide clues, by words or by actions, as to the authenticity of any leaked purportedly classified information.

Dirty Bomber
In the trial of Jose Padilla—who was originally detained as a dirty bomber but ultimately tried with two other men for terrorism conspiracy—classified information was reviewed by defense attorneys in the court’s basement SCIF. Both the judge and the defense attorneys viewed classified vicissitudes of interrogations of Padilla conducted while he was in military detention.

The judge reviewed, as provided by CIPA, an evidentiary substitute for classified evidence. An agent of the intelligence agency with authority over the evidence brought the original evidence to the classified information security officer, who delivered it to the judge in chambers for her private review in her office while the agent and the security officer waited outside her door.

A Plot to Kill President Bush
In the prosecution of Ahmed Omar Abu Ali for terrorism conspiracy and conspiracy to kill
the President, classified evidence was stored in the court’s SCIF.

**Minneapolis**

The case against Mohamed Abdullah Warsame, who was prosecuted for attending Al-Qaeda training camps, relied on classified evidence. Early in the case, the government produced to defense counsel discoverable classified evidence, and the attorneys reviewed the classified material in a secure room at the courthouse, which included a safe suitable for storing classified materials. The attorneys had to prepare any documents based on or referring to classified material in the secure room. The court reporter, who had a security clearance, also had to work on transcripts containing classified information in this room and store computer equipment she used for such transcripts in the safe. The judge could keep classified materials in a safe in his chambers office.

**Mistaken Rendition**

Relying on a classified declaration presented for the judge’s eyes only, the district court dismissed a complaint on state-secrets grounds, alleging that the CIA abducted and imprisoned Khaled el-Masri until it realized that it had picked up the wrong person. *El-Masri v. Tenet*, 437 F. Supp. 2d 530 (E.D. Va. 2006), aff’d, 479 F.3d 296 (4th Cir. 2007). The classified declaration was delivered to the judge by a classified information security officer, who took responsibility for storing the declaration when the judge was not privately reviewing it.

**Prosecution of a Charity**

The prosecution of the Holy Land Foundation and its principals for providing funds to Hamas was based in part on classified evidence, including information obtained under the Foreign Intelligence Surveillance Act and information provided by the government of Israel. A second trial was required because of a hung jury after the first one. The judges presiding over the two trials each kept classified documents in a chambers safe. The court found space that could be fitted as a secure room for defense counsel to store and review classified documents; a separate safe was established for each defendant.

**Chicago**

For the prosecution of Muhammad Abdul Hamid Khalil Salah for helping to provide funds to Hamas, the judge kept classified materials in a chambers safe to which only the judge and a cleared court reporter had the combination. For hearings concerning classified documents, the court reporter used a laptop provided by classified information security officers; the laptop was also stored in the safe.

To ensure against surveillance of proceedings by enemies, deputy marshals electronically monitored conferences and hearings in which classified information was discussed.

**Giving State Secrets to Lobbyists**

For a sting prosecution of lobbyists for sharing classified information, defense attorneys with security clearances reviewed classified evidence in a courthouse SCIF designed for use by criminal defense counsel. Defense witnesses with security clearances could also review classified information in the SCIF, but they were required to do so after usual operating hours.

**Warrantless Wiretaps**

Lawyers for an Islamic charity that the government shut down for allegedly funding terrorism filed an action in Portland, Oregon, against a secret and allegedly illegal surveillance program. The lawyers submitted as evidence of the surveillance a top-secret document mistakenly disclosed to the charity during proceedings to freeze the charity’s assets. After the classified document had remained in a sealed envelope in the judge’s chambers for two weeks, a government security officer reviewed it in chambers and determined that it contained sensitive compartmented information, which meant it had to be stored in a SCIF. The courthouse did not have a SCIF. The FBI had a SCIF in Portland, but the FBI was a party to the case, so the plaintiffs did not want the document stored there. It was agreed that the document would be sent to the Seattle U.S. attorney’s SCIF. Shortly thereafter, the plaintiffs agreed to a method of storage at the FBI’s Portland SCIF: the document was stored in a locked bag to which only the judge and a classified information security officer would have a key. *Al-Haramain Islamic*

The government required the plaintiffs and their attorneys to surrender all copies of the document. The attorneys said that they complied with the government's instructions, but the attorneys said that they could not comment on whether their clients had done so without violating the attorney-client privilege. The government made no effort to retrieve any copies of the document that may have been sent abroad, and it was reported that a reporter for the Washington Post had reviewed the document.

The district judge ruled that the plaintiffs could rely on their memories of the classified document to support their case, but the court of appeals determined that if they could not rely on the document itself then neither could they rely on their memories of it. Al-Haramain Islamic Found. v. Bush, 507 F.3d 1190, 1203 (9th Cir. 2007).

In a related action under the Freedom of Information Act (FOIA), the judge spent many hours over several days reviewing claimed exemptions in camera and ex parte. The government would not allow even law clerks with security clearances to assist the judge in this review. Doors were closed, windows were covered, and the documents were under the judge's immediate control at all times. The documents were not stored in chambers; classified information security officers, whose offices and storage facilities, at the time, were a few blocks away from the federal courthouse in the District of Columbia, delivered and retrieved the documents on request.

Another judge presiding over another related FOIA action adopted a procedure for ensuring an accurate appellate record: he initialed and dated any classified document he reviewed that was not kept in the court's file.

A judge hearing another related action prepared a sealed ex parte opinion responding to classified ex parte government submissions. See Terkel v. AT&T, 441 F. Supp. 2d 899, 902 (N.D. Ill. 2006). To write the classified opinion, the judge used a laptop computer provided by the classified information security officer. The computer, and all drafts of the opinion, were stored in the U.S. attorney's SCI in the same building.

Atlanta

In a prosecution of two young men in Atlanta for preparing for violent jihad by, among other things, making casing videos of strategic landmarks, some classified information in the case was designated SCI. Judges and court staff could view this information at the U.S. attorney's SCI in the same building as the courthouse.

Some classified information in the case was not SCI, and judges could store this in chambers safes. A secure room was set aside for defense counsel to store and review classified information.

Sears Tower

Not all national security cases involve classified information. The prosecution of the "Liberty City Seven" for conspiracy to topple the Sears Tower and attack other buildings in various cities, based on information provided by paid informants, involved no classified information.

Fort Dix

In a prosecution of six men for conspiracy to attack Fort Dix, defense attorneys, who had security clearances, reviewed classified materials in a secure room in the courthouse; a separate safe was designated for each defendant. The attorneys did not have to see SCI, but the judge did. A classified information security officer brought the SCI to the judge's chambers and took it away when the judge was finished examining it.

Torture Flights

In a tort action pertaining to extraordinary rendition, the government supported a successful motion to dismiss on state-secrets grounds with a classified ex parte declaration by the head of the CIA. A classified information security officer brought the declaration to the district judge's chambers. The judge reviewed the declaration privately in his office, with the blinds drawn, while the security officer waited outside. When the judge was finished reviewing the declaration, the security officer took it back and informed the judge that it could be brought back to him for another review at any time.
Sharing Classified Information with Criminal Defendants

Courts have found it proper for the government to share classified information with defense attorneys who have security clearances even if the attorneys cannot share the information with their clients. Protective orders prohibit counsel from sharing the information with unauthorized persons. It has been held improper, however, to deny the defendant access to classified information entered into evidence at the defendant’s criminal trial. United States v. Abu Ali, 528 F.3d 210, 248–55 (4th Cir. 2008).

CASE NOTES

First Prosecution for 1998 Embassy Bombings

In the original prosecution for the 1998 bombings of American embassies in Kenya and Tanzania, defense counsel could not discuss classified evidence with their clients. The court of appeals affirmed the district judge’s determination that this did not violate the Constitution. In re Terrorist Bombings of U.S. Embassies in East Africa, 552 F.3d 93, 116–23 (2d Cir. 2008).

Twentieth Hijacker

Attorneys representing Zacarias Moussaoui, in his trial for terrorism conspiracy, had security clearances, but they could not share classified information with the defendant. United States v. Moussaoui, 591 F.3d 263, 607 (4th Cir. 2010). Moussaoui pleaded guilty against his attorneys’ advice and sought to rescind his guilty plea after the jury spared his life. Id. at 272, 278; United States v. Moussaoui, 483 F.3d 220, 223–24 n.1 (4th Cir. 2007). On appeal, his attorneys argued that their client would not have pleaded guilty if he had access to some of the classified information concerning the case that the attorneys had access to. Moussaoui, 591 F.3d at 272. The court of appeals affirmed the district court’s denial of this request: “Moussaoui was well aware that there was classified, exculpatory evidence yet to be produced to him personally and he knew why the material was exculpatory. Rather than wait for the process to be completed, Moussaoui made the strategic decision to plead guilty immediately.” Id. at 287.

Guantánamo Bay

Habeas attorneys could not share classified information with Guantánamo Bay detainees, except for the detainees’ own statements made to government agents.

Dirty Bomber

More than two years after Jose Padilla—who originally was detained as a dirty bomber but was ultimately tried with two other men for terrorism conspiracy—was added to the indictment, the district judge granted him access to classified evidence created during his military detention. Although it is common to grant defense attorneys access to classified evidence relevant to a prosecution, it is very unusual for courts to grant such access to terrorism defendants.

A Plot to Kill President Bush

In the prosecution of Ahmed Omar Abu Ali for terrorism conspiracy and conspiracy to kill the President, some of the evidence against the defendant was classified, and the defendant was not allowed to see it. A small amount of classified information was presented to the jury at trial but not shown to the defendant; the court of appeals determined that this was error. United States v. Abu Ali, 528 F.3d 210, 248–55 (4th Cir. 2008). The court determined, however, that the error was harmless in this case.

Prosecution of a Charity

For the prosecution of the Holy Land Foundation and its principals for providing funds to Hamas, defense attorneys had security clearances, but they were not allowed to reveal classified information to their clients.

Fort Dix

In a prosecution for conspiracy to attack Fort Dix, defense attorneys had security clearances, and they had to examine classified materials, but they were not permitted to share classified information with their clients.
Discovery

In criminal cases involving classified information, the court must often not only decide what information in the government’s possession is discoverable, but, pursuant to CIPA, 18 U.S.C. app. 3 § 4 (2006), must decide whether the government can substitute summaries or admissions for the original classified information. These cases frequently present “a conflict raising vitally important interests to both parties—the government’s interest in protecting national security through the non-disclosure of classified information, on the one hand, and the defendant’s need to acquire this information to present an adequate defense, on the other.” Reggie B. Walton, Prosecuting International Terrorism Cases in Article III Courts, 39 Geo. L.J. Ann. Rev. Crim. Proc. iii, iii (2010).

Security precautions are required for the court’s review of classified information for discovery obligations. Classified information must not be reviewed in the presence of anyone without the appropriate security clearance. A law clerk may assist the judge only if the law clerk is granted a security clearance to do so. If the matter is delegated to a magistrate judge, the magistrate judge will have to be cleared first. Classified material must be properly stored when it is not being reviewed.

Sometimes, the government can declassify information to facilitate a prosecution. This typically requires negotiation between the prosecutors and the intelligence community. Because of the secrecy associated with classified information, the prosecutors may not be immediately aware of all discoverable information in the government’s possession.

Determining what information in the government’s possession might be helpful to the defense is often even more difficult in a case involving classified information than it is in other criminal cases. Some judges have ex parte conversations with the defense to learn defense strategies and ex parte conversations with the prosecution to learn what information the government has in order to better understand what classified information in the government’s possession might be helpful to the defense.

CASE NOTES

First Prosecution for 1998 Embassy Bombings

In the original prosecution for the 1998 bombings of American embassies in Kenya and Tanzania, the district judge resolved issues concerning discovery of classified information by conducting ex parte discussions with defense counsel concerning defense strategy and ex parte discussions with prosecutors concerning potentially relevant classified information. Sometimes, the judge was able to mediate a substitution for classified information. In re Terrorist Bombings of U.S. Embassies in East Africa, 552 F.3d 93, 118–19 (2d Cir. 2008).

Sometimes, the judge was able to determine that classified information was not as relevant as defense counsel thought it might be.

Prosecution of a Guantánamo Bay Detainee for 1998 Embassy Bombings

In preparation for the 2010 trial of Ahmed Khalfan Ghailani, a onetime fugitive, the district judge reviewed classified CIA reports containing statements made by the defendant during custodial interrogations. The judge determined that defense counsel were entitled to additional information about the time and circumstances of the defendants’ statements.
Millennium Bomber
In the prosecution of Ahmed Ressam, who planned to bomb the Los Angeles International Airport at the turn of the millennium, the district judge reviewed classified material to determine whether it was discoverable, and he decided that it was not.

American Taliban
In the prosecution of John Walker Lindh, who became known as the American Taliban, the district judge had to review a substantial amount of classified material to determine what evidence the government had to produce to the defense.

Paintball
In the prosecution of Ali al-Timimi, the spiritual leader of northern Virginia men who played paintball in preparation for violent jihad, it was difficult for the court to determine whether the defendant had been provided with all discoverable information, because prosecutors did not necessarily have access to classified information held by other parts of the government.

Lodi
In the Sacramento prosecution of Hamid Hayat for attending a terrorist training camp, and of his father Umer for lying about it, the government filed a notice that it had potentially discoverable classified evidence. After several sealed ex parte in camera reviews and hearings, the judge determined that classified information foundational to trial evidence was discoverable. Defense counsel elected to stipulate to the admissibility of the trial evidence rather than undergo the burden and delay of security clearance procedures.

FISA Evidence

FISA warrants are issued by a special FISA court, whose proceedings are conducted ex parte and in secret. 50 U.S.C. § 1803 (2006). The FISA court can also issue warrants for physical searches within the United States for the purpose of obtaining foreign intelligence. Id. § 1822.

If the prosecution believes that it will rely on evidence obtained because of a FISA warrant, then the court may be called upon to review the warrant application to determine whether the evidence was properly obtained pursuant to a properly issued warrant. The defense is not typically granted access to materials in the warrant application. On the one hand, the court must review the collection of FISA evidence without the benefit of adverse counsel; on the other hand, the review has the benefit of previous scrutiny by another judge.

CASE NOTES
Dirty Bomber
In the trial of Jose Padilla—who was originally detained as a dirty bomber but ultimately tried with two other men for terrorism conspiracy—some of the evidence against each of the defendants resulted from warrants issued by the FISA court. Challenges to this evidence necessitated the court’s review of the FISA warrant applications. The district judge referred the matter to a magistrate judge, who reviewed in camera all relevant FISA applications. After her own careful review, the district judge affirmed the magistrate judge’s findings of proper probable cause for all applications.
Minneapolis

In the prosecution of Mohamed Abdullah Warsame, who was indicted for attending Al-Qaeda training camps, some of the evidence against the defendant was obtained as a result of FISA warrants. *United States v. Warsame*, 547 F. Supp. 2d 982, 984–86 (D. Minn. 2008). The FISA court had issued warrants for surveillance of persons with whom Warsame communicated, and later the court approved a tap of Warsame’s telephone and a physical search of his apartment. The district judge presiding over the prosecution reviewed all warrant applications and supporting materials in camera, making de novo judgments as to probable cause, and determined that FISA procedures were properly followed.

Prosecution of a Charity

The prosecution of the Holy Land Foundation and its principals for providing funds to Hamas was based in part on wiretaps authorized by the FISA court. In discovery, the government produced FISA evidence to defense counsel, who had security clearances but who could not disclose classified information to their clients. Much of this evidence was in the form of declassified “tech-cuts,” which are English-language summaries of recorded conversations. Defense counsel discovered some errors in the summaries, and the judge declared the errors to be “disturbing,” but the defendants did not present evidence of sufficient inaccuracies to require a remedy.

In error, the government also disclosed to defense counsel the contents of some FISA warrant applications. This is not the usual procedure for affording a defendant an opportunity to challenge evidence based on FISA warrants. The usual procedure is for the government to present the FISA warrant records to the district judge ex parte. In fact, the judge spent several days conducting an in camera review of FISA warrants resulting in evidence the government sought to use in the case.

The judge was at a conference in another city when he received, in the lobby of his hotel, an emergency motion from the FBI stating that FISA applications had been inadvertently disclosed to defense attorneys. The FBI asked the judge for relief because the attorneys refused to return them. The judge issued an order preserving the status quo and then ultimately granted the FBI substantially the relief requested.

The government declassified some of the defendants’ recorded conversations, and that evidence could be shared with the defendants. The court approved an offer by the government to seek declassification of additional conversations specifically identified by the defendants. Defense counsel argued that the offer was unconstitutional because it required them to reveal too much about their own conversations with their clients and their trial strategy. The judge overruled this objection.

It was understood that any FISA evidence the government presented at trial would have to be declassified and provided to the individual defendants in advance of trial.

Toledo

In a prosecution of Americans for conspiracy to fight against U.S. forces in Iraq, the district judge determined that it was not necessary to disclose to defense counsel FISA application materials; the court would determine the validity of the FISA evidence ex parte and in camera. *United States v. Amawi*, 531 F. Supp. 2d 852 (N.D. Ohio 2008).

Atlanta

In a prosecution of two young men in Atlanta for preparing for violent jihad by, among other things, making casing videos of strategic landmarks, some evidence against the defendants was obtained pursuant to FISA warrants. The magistrate judge reviewed all relevant FISA applications, finding no errors in FISA procedures and finding that none of the FISA materials were discoverable. The judge observed that defense counsel is in a difficult position when arguing for suppression of FISA evidence, because they do not have access to the FISA records, but a FISA suppression motion is easier for the judge than many other suppression motions because collection of the FISA evidence has been subjected to prior judicial review.

Fort Dix

In a prosecution for conspiracy to attack Fort Dix, much of the evidence against the defendants had been obtained with FISA warrants. The judge reviewed FISA files to determine what was discoverable and to determine that the FISA surveillance was properly supported.
Much of the FISA evidence was declassified, but the affidavits supporting the FISA warrants generally were not. The judge observed that FISA discoverability decisions are some-
what hampered by the judge’s not knowing, particularly early in the case, what the defenses might be.

Civil Cases

Civil actions involving classified information include actions arising from contracts, torts, habeas corpus, and the Freedom of Information Act (FOIA). Typically, the government either is a defendant or it has interests aligned with a defendant. That means that the incentive structure for sharing classified information with the government’s opposing party is quite different. In a criminal case, the government has an incentive to share classified information, such as by declassifying it or granting defense attorneys security clearances to see it. In a civil case, the government’s goal is often to have the case dismissed. An interesting exception arose in habeas actions pertaining to detention at Guantánamo Bay, in which the district court imposed on the government the burden of proof.

CASE NOTES

Burma
In an action by the Drug Enforcement Administration’s attaché in Burma claiming illegal surveillance, the district court determined that CIPA, which technically applies only to criminal cases, would apply to classified evidence in this civil case.

The district judge also overruled a government determination that attorneys in the case did not have a need to know classified information. The Litigation Security Group determined that the attorneys were eligible for security clearances, but the government declined to acknowledge their need to know classified information that was actually already known to them.

Guantánamo Bay
Habeas actions by Guantánamo Bay detainees are technically civil actions, but the district court for the District of Columbia determined that the security principles of CIPA apply to these cases.

Mistaken Rendition
A court of appeals affirmed a district court’s dismissal on state-secrets grounds of a tort action arising from extraordinary rendition involving mistaken identity. El-Masri v. United States, 479 F.3d 296 (4th Cir. 2007).

Detainee Documents
A district court reviewed government information about terrorism suspects detained at extraterritorial military facilities since September 11, 2001, to determine what must be produced pursuant to FOIA requests. E.g., ACLU v. Dep’t of Defense, 723 F. Supp. 2d 621 (S.D.N.Y. 2010).

Warrantless Wiretaps
In an action challenging a secret and allegedly illegal surveillance program—an action arising from evidence of surveillance in a top-secret document mistakenly disclosed to an Islamic charity during proceedings to freeze the charity’s assets for allegedly funding terrorism—the district judge was able to resolve the case in the plaintiffs’ favor without use of the classified document. The government had publicly acknowledged surveillance of the charity and presented to the court no warrant for doing so. In re NSA Telecom. Records Litig., 700 F. Supp. 2d 1182 (N.D. Cal. 2010).

In a related FOIA action, the classified status of opinions concerning the surveillance program prepared by the Justice Department’s Office of Legal Counsel (OLC) changed during the course of litigation, so the government agreed to the plaintiffs’ demand that the government review again its position on whether the opinions or parts of them could be produced.
Torture Flights
A court of appeals affirmed a district court’s dismissal on state-secrets grounds of a tort action pertaining to extraordinary rendition. *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070 (9th Cir. 2010).

Other Government Secrets

CASE NOTES

American Taliban
In the prosecution of John Walker Lindh, who became known as the American Taliban, the government determined that it had to disclose to the defense information that was not classified but that nevertheless required sensitive handling for the benefit of national security: “reports of interviews of detainees captured in Afghanistan and elsewhere who may have knowledge of al Qaeda or who may have been members of that organization and who are housed primarily at Guantánamo Bay, Cuba.” *United States v. Lindh*, 198 F. Supp. 2d 739, 741 (E.D. Va. 2002).

The district judge approved redactions to the discovery, such as agent and case identifiers. The judge also issued a protective order requiring that defense personnel given access to the discovery preserve its secrecy. The defense agreed to a limited background check, coordinated by the classified information security officer, for personnel with access to the protected discovery.

September 11 Damages
The consolidated civil actions against airlines and security companies for damages resulting from the September 11, 2001, terrorist attacks required discovery concerning security procedures. The government decided that the Transportation Security Administration (TSA) should screen discovery for “sensitive security information” (SSI), which is secret information related to transportation security. *In re Sept. 11 Litig.*, 600 F. Supp. 2d 549, 552 (S.D.N.Y. 2009); 49 C.F.R. § 1520.5(a). This slowed substantially the progress of the litigation. *In re Sept. 11 Litig.*, 567 F. Supp. 2d 611, 616 (S.D.N.Y. 2008); *In re Sept. 11 Litig.*, 621 F. Supp. 2d 131, 142 (S.D.N.Y. 2009).

It took the TSA two years to screen an early set of discovery. *In re Sept. 11 Litig.*, 236 F.R.D. 164, 167 (S.D.N.Y. 2006). Then the TSA instructed the defendants to refuse to answer any deposition questions that called for SSI, and the TSA refused to attend the depositions. The district court concluded that the TSA’s reasons for intervening in the case required the agency’s attendance at the depositions.

The district judge suggested that representative plaintiff attorneys attend the depositions, but many plaintiffs’ attorneys were unwilling to be represented by other parties’ attorneys. The government, however, wanted to limit the number of people given access to sensitive discovery. Depositions could proceed once the government relaxed its insistence that deposition participation be limited.

Guantánamo Bay
In habeas actions on behalf of Guantánamo Bay detainees, the government sought to keep under seal substantial portions of the case files to protect information that was not classified but was nonetheless considered sensitive. In addition, the detainees’ attorneys sometimes sought to protect personal information about their clients that the clients considered sensitive. The court balanced requests to keep parts of the court records sealed against the public’s First Amendment and common-law rights.
Giving State Secrets to Lobbyists

In a sting prosecution of lobbyists for sharing classified information, the judge ruled that the indictment required proof that the information passed by the defendants qualified as national defense information (NDI). United States v. Rosen, 599 F. Supp. 2d 690, 694–95 (E.D. Va. 2009); United States v. Rosen, 471 F. Supp. 2d 651, 652 (E.D. Va. 2007); see 18 U.S.C. § 793 (2006). “To qualify as NDI, information must be closely held by the government and potentially damaging to national security if disclosed.” United States v. Rosen, 487 F. Supp. 2d 703, 705 n.1 (E.D. Va. 2007). “It is important to recognize that NDI and classified material may not be coextensive sets.” Id. “In short, the government designates what information is labeled and treated as classified, while a court or jury determines what information qualifies as NDI . . . .” Rosen, 599 F. Supp. 2d 690.

Filings and Proceedings

If a case involves classified information, then part of the case record may be classified. Security precautions greater than those ordinarily used for sealing part of a record typically are required. Classified information security officers provided by the Justice Department’s Litigation Security Group must control classified portions of a case record. They will provide case-specific guidance; the following is only a cursory introduction.

If a party or the court enters into the record a document containing classified information, or a document that might contain classified information, then the document is filed with the classified information security officer instead of with the clerk’s office, and the document is deemed filed with the clerk. It is good practice to simultaneously file a public document that gives public notice of the classified filing. The filing of a “half sheet” works well: the part of the first page containing the caption of the case and an unclassified title of the document is placed in the public file. The public record must not include classified information.

Often, unclassified parts of a document containing classified information can be in the public file: after a classification review, the document is redacted to remove the classified information. After a classified document is filed with the classified information security officer, the security officer can refer the document to the appropriate part of the intelligence community for a classification review. If the classification review is conducted on an opinion or an order before the document is served on the parties, then the review is performed by persons walled off from persons working with the government’s attorneys in the case. After the classification review, the security officer can place into the public file a redacted version of the document.

The parties, or at least their attorneys, may be cleared to receive unredacted copies of the classified document.

Sometimes, judges simultaneously file a public version of an opinion or order and a more complete version containing classified information with the classified information security officer. It is important to remember how difficult it can be to anticipate what must be redacted from a document in a case concerning classified information. The public docket sheet should reflect both filings. It is important for the court to ensure that this method does not keep from the public record informa-
tion that is neither classified nor properly sealed on specific findings of a need for sealing.

If a public proceeding might concern classified information, the classified information security officer can attend the proceeding to monitor it and interrupt if anyone appears to be about to say something classified. Often the security officer will be accompanied by someone from the intelligence community. It is important for all participants to know what they can and cannot say in public, so in practice the security officer seldom has to interrupt.

If classified information must be discussed at a proceeding, then all or part of the proceeding may be closed. Proceedings involving classified information are often bifurcated into a closed proceeding, at which classified information can be discussed, and an open proceeding. At the closed portion of the proceeding, only persons cleared to hear the classified information to be discussed can be present. The classified information security officer will advise the court on necessary security precautions and coordinate with the U.S. Marshals Service for physical security. For transcripts of proceedings in which classified information is discussed, the court reporter must have a suitable security clearance. A possibly redacted transcript of closed proceedings can often be released publicly after a classification review.

Documents and transcripts containing classified information must be prepared on approved computer equipment. The classified information security officer will provide an approved laptop computer, which cannot have any network or Internet connection and which must be stored in an approved safe or SCIF.

CASE NOTES

Burma

In an action by the Drug Enforcement Administration’s attaché in Burma claiming illegal surveillance, the district court initially sealed the whole record. Later, after a different judge assumed responsibility for the case, the court unsealed the case and ordered a classification review of all previous filings. Documents without classified information were put on the public record, as were redacted versions of documents that contained classified information.

First Prosecution for 1998 Embassy Bombings

The court of appeals approved a district court procedure to resolve a suppression motion in the original prosecution for the 1998 bombings of American embassies in Kenya and Tanzania: the district judge determined the reasonableness of searches in Africa by ex parte examination of classified evidence instead of hearing evidence in an adversary proceeding. In re Terrorist Bombings of U.S.


Prosecution of a Guantánamo Bay Detainee for 1998 Embassy Bombings

Concerning the 2010 trial of onetime fugitive Ahmed Khalifan Ghailani for the 1998 bombings of American embassies in Kenya and Tanzania, the judge filed seven opinions containing classified information. Each time, the opinion was filed with the classified information security officer and a cover half-sheet was filed on the public record containing only the case caption and the document title. For most opinions, from one day to two weeks later, a redacted copy of the opinion was filed on the public record. For one opinion concerning discovery, the redacted opinion was filed on the public record approximately two months after the original classified opinion was filed.

Twentieth Hijacker

In the prosecution of Zacarias Moussaouy for terrorism conspiracy, filings that might include classified information were not filed di-
rectly with the clerk’s office. Defense attorneys, who had security clearances, filed their papers with the classified information security officer, who, by order of the court, arranged for screening by the intelligence community within 48 hours. The government was responsible for classification review of its filings. After classification screening, redacted papers were filed with the clerk’s office for inclusion in the public record.

**Guantánamo Bay**

If there was a chance that a filing by a habeas attorney representing a Guantánamo Bay detainee would contain classified information, which included most filings involving matters more substantive than the dates of proceedings, then the filing would be presented to classified information security officers, at which time it was deemed filed with the court.

Classified materials used by habeas attorneys in court had to be transported to the courtroom by cleared couriers, and the proceedings had to be closed.

Opinions in the Guantánamo Bay habeas cases almost always required a classification review before they could be released publicly. Either the review was performed by persons walled off from representatives of the government in the actions before the opinion was issued simultaneously to the parties in complete form and to the public in redacted form, or the classification review was performed after the opinion was released to the parties and a redacted version was placed on the public record later.

**Dirty Bomber**

Jose Padilla, who was originally detained on a material witness warrant as part of the grand jury investigation of the September 11, 2001, attacks, was transferred to military detention and designated an enemy combatant for an alleged plan to detonate a dirty bomb. *Padilla ex rel. Newman v. Bush*, 233 F. Supp. 2d 564, 571 (S.D.N.Y. 2002). In response to Padilla’s habeas corpus petition, the government submitted both a public redacted declaration describing evidence supporting the designation of Padilla as an enemy combatant and an ex parte, in camera classified unredacted declaration. The only information in the unredacted declaration not in the public declaration was the identity of sources and some circumstantial evidence corroborating facts in the redacted declaration. The judge ruled that it was proper to deny Padilla access to the classified declaration unless Padilla rebutted facts presented in the redacted declaration, in which case the judge would give the government a choice between sharing the unredacted declaration with Padilla or withdrawing it.

**Paintball**

Ali al-Timimi, the spiritual leader of northern Virginia men who played paintball in preparation for violent jihad, was convicted of soliciting others to wage war against the United States and providing services to the Taliban. The court of appeals remanded the case for an investigation of possibly discoverable surveillance. The trial judge held several post-trial proceedings, which were closed because matters discussed touched on classified information. After the proceedings, the transcripts were submitted to the classified information security officer for a classification review. After the classification review, the transcripts became public documents, either in whole or in redacted form.

During some of the proceedings, the defendant was present; he was not authorized to hear classified information, so sometimes participants had to speak cryptically.

**Detainee Documents**

In an FOIA case concerning extraterritorial detentions of terrorism suspects, the government would not permit the law clerks to see some of the classified information presented to the judge even though the law clerks had security clearances. The judge, nevertheless, was able to review government documents with the law clerks present to make rulings on what had to be produced to the plaintiffs. See, e.g., *ACLU v. Dep’t of Defense*, 723 F. Supp. 2d 621, 624 (S.D.N.Y. 2010). The judge examined the documents without showing them to anyone else present, and a court reporter without a security clearance transcribed the proceeding. The judge determined which documents had to be produced, either redacted or unredacted, and did not retain the documents.

**Chicago**

For the prosecution of Muhammad Abdul Hamid Khalil Salah for helping to provide funds to Hamas—a prosecution that involved
a substantial amount of classified evidence relating to Salah’s imprisonment in Israel—
the judge’s opinion denying Salah’s motion to suppress a confession in Israel was published
in the Federal Supplement with 19 redactions because of references to classified information. United States v. Marzook, 435 F. Supp. 2d 708 (N.D. Ill. 2006). The parties received
unredacted copies, and an unredacted original is stored in the judge’s chambers safe.

A motion by the government for secrecy procedures protecting testimony from Israeli
agents was supported by a classified affidavit from the FBI’s assistant director for counterintelligence—the affidavit was stored in the judge’s safe rather than in the clerk’s office.

The judge set time limits of seven business days for the government to decide what portions of other documents and transcripts related to classified information could be released to the public. United States v. Abu Marzook, 412 F. Supp. 2d 913, 928 (N.D. Ill. 2006).

Giving State Secrets to Lobbyists
The judge presiding over a sting prosecution of lobbyists for sharing classified information
held several closed pretrial hearings, each of which required a court reporter with a security clearance because the hearings concerned classified information. The judge denied, however, a government motion to try the defendants in closed proceedings. United States v. Rosen, 487 F. Supp. 2d 703 (E.D. Va. 2007).

Some of the orders the judge issued in the case are sealed because they contain classified information. On some occasions, the judge issued a public order stating as much as he could on the public record and a sealed order with additional classified details. United States v. Rosen, 520 F. Supp. 2d 802, 814 (E.D. Va. 2007); United States v. Rosen, 520 F. Supp. 2d 786, 789, 802 (E.D. Va. 2007). On one occasion, a classified order could subsequently be made public.

Lodi
In the Sacramento prosecution of Hamid Hayat for attending a terrorist training camp,
and of his father Umer for lying about it, the government filed a notice that it had potentially discoverable classified evidence. Six sealed ex parte in camera submissions and two sealed ex parte in camera hearings followed. The judge filed rulings and orders under seal if they discussed potentially classified information.

Warrantless Wiretaps
In an action challenging a secret and allegedly illegal surveillance program—the action arising from evidence of surveillance in a top-secret document mistakenly disclosed to an Islamic charity during proceedings to freeze the charity’s assets for allegedly funding terrorism—the plaintiffs unsuccessfully opposed a motion by the government to deny them further access to the document. The plaintiffs supported their opposition with a declaration of what they remembered about the document. The plaintiffs filed the declaration under seal, but this afforded insufficient protection for classified information. The clerk’s office followed its usual procedures for sealed documents: it opened the sealed envelope, made a copy for the judge, and then resealed it. The government determined that the declaration had the same level of classification as the original document, so it had to be stored with the original document in a locked bag in a SCIF. All classified submissions by the government in this case, until the case was transferred as part of a multidistrict consolidation, were stored in the locked bag when the judge was not examining them.

It was difficult for the plaintiffs in this case to determine whom on the government side they could serve with any papers describing the classified evidentiary document. The government said that the identities of persons with clearance to see such documents was a state secret. The solution to this problem was to have the plaintiffs send classified information to the government on a secure fax line, leaving it up to the government to ensure that only authorized persons received the classified information.

In this and related actions before various judges challenging the surveillance program, the government frequently presented to the court classified briefs and declarations designated for judges’ eyes only. Sometimes the judge reviewed the document when it was presented. Sometimes the judge delayed reviewing the document until after a public hearing on the matter so there would be no danger of the judge referring to classified in-
formation at the hearing. Another approach was to carefully prepare questions for an oral hearing in advance so as to make sure classified information would not be mentioned. Sometimes the judge deferred decision on whether to examine the classified arguments until there was a showing of need for an in camera, ex parte presentation.

A judge in Chicago decided not to rely on classified submissions in ruling on a motion, but he decided to respond to the submissions in a sealed opinion available only to the government and to judges subsequently reviewing the case. See Terkel v. AT&T, 441 F. Supp. 2d 899, 902 (N.D. Ill. 2006).

**Atlanta**

In a prosecution of two young men in Atlanta for preparing for violent jihad by, among other things, making casing videos of strategic landmarks, filings based on classified information received classification reviews for possible redaction. The court denied as overly broad and excessively burcensome a government request that all filings based on discovery, whether classified or not, be filed under seal.

**Fort Dix**

In a prosecution for conspiracy to attack Fort Dix, the judge had to rule on the validity of FISA warrants. The judge’s opinion on the matter is classified. A redacted opinion was filed publicly after review by intelligence agencies, over 16 months after the original was issued. Redactions appear to conceal which agents of Al-Qaeda were the targets of FISA surveillance resulting in evidence against the defendants.

**State-Secrets Privilege**

The state-secrets privilege is most likely to arise in a civil action against the government or against a party with whom the government shares interests.

The government cannot be required to divulge state secrets. See Robert Timo-thy Reagan, Keeping Government Secrets: A Pocket Guide for Judges on the State-Secrets Privilege, the Classified Information Procedures Act, and Court Security Officers 3–7 (Federal Judicial Center 2007). Designation of information as a state secret requires high-level certification. United States v. Reynolds, 345 U.S. 1, 7–8 (1952). Although the executive branch has authority over what constitutes a state secret, the judicial branch has authority over its implications in specific cases.

**CASE NOTES**

**Burma**

In an action by the Drug Enforcement Administration’s attaché in Burma claiming illegal surveillance, the district court reasoned that because the privilege is a judicial doctrine, the court retains the authority to order secret information disclosed in litigation. Horn v. Huddle, 647 F. Supp. 2d 55, 62–63 (D.D.C. 2009), vacated on other grounds, 699 F. Supp. 236 (D.D.C. 2010).

**Mistaken Rendition**

A court of appeals affirmed a district court’s dismissal on state-secrets grounds of a tort action alleging that because of mistaken identity the government abducted a German citizen on vacation in Macedonia and imprisoned him in secret for five months. El-Masri v. United States, 479 F.3d 296 (4th Cir. 2007).

**Warrantless Wiretaps**

In an action challenging a secret and allegedly illegal surveillance program—the action arising from evidence of surveillance in a top-secret document mistakenly disclosed to an Islamic charity during proceedings to freeze the charity’s assets for allegedly funding terrorism—the court of appeals determined that the document and its contents were state secrets. Al-Haramain Islamic Found. v. Bush, 507 F.3d 1190, 1204 (9th Cir. 2007). The three judges on the appellate panel reviewed in camera the document and classified argu-
ments supporting its protection under the state-secrets privilege:

We take very seriously our obligation to review the documents with a very careful, indeed a skeptical, eye, and not to accept at face value the government’s claim or justification of privilege. Simply saying “military secret,” “national security” or “terrorist threat” or invoking an ethereal fear that disclosure will threaten our nation is insufficient to support the privilege. Sufficient detail must be—and has been—provided for us to make a meaningful examination. Id. at 1203.

Torture Flights

A court of appeals affirmed a district court’s dismissal on state-secrets grounds of a tort action pertaining to extraordinary rendition, finding that the case could not be litigated without endangering state secrets. Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070 (9th Cir. 2010).

Silent Witness Rule

It is not yet well established, but some courts have employed what is often called a silent witness rule to permit public discussion of classified information. See United States v. Zettl, 835 F.2d 1059, 1063 (4th Cir. 1987); United States v. Rosen, 520 F. Supp. 2d 786 (E.D. Va. 2007). The classified information, such as the identity of a person or a country, is referred to in code (such as “person 1” or “country A”). The judge, the parties, and the jury know the code but the public does not.

CASE NOTES

September 11 Damages

One action against airlines and security companies for damages resulting from the September 11, 2001, terrorist attacks came close to going to trial, but it ultimately settled. The court prepared for evidence based on “sensitive security information” (SSI), which is protected, but not classified, information related to transportation security. The court issued a protective order calling for use of the silent witness rule at trial.

Giving State Secrets to Lobbyists

For a sting prosecution of lobbyists for sharing classified information, which the government dismissed because of other pretrial rulings, the judge determined that it might be appropriate to introduce classified evidence at trial using the “silent witness rule.” United States v. Rosen, 520 F. Supp. 2d 786 (E.D. Va. 2007). The silent witness rule permits some evidence to be presented to the judge, the jury, and the parties, but not to the public. It is a partial closing of the trial. The judge determined that the silent witness rule would be appropriate only when the government established (i) an overriding reason for closing the trial, (ii) that the closure is no broader than necessary to protect that interest, (iii) that no reasonable alternatives exist to closure, and (iv) that the use of the [silent witness rule] provides defendants with substantially the same ability to make their defense as full public disclosure of the evidence, presented without the use of codes. Id. at 799.

Special Judicial Resources

As with other cases, in national security cases the court may want to consider both usual and creative ways to manage a case in the interests of justice. For Guantánamo Bay habeas cases, the court used senior judges and magistrate judges for matters common to cases before assigned judges. For a civil challenge to a government program, one judge considered using a special master to advise the court on national security issues.
CASE NOTES

Guantánamo Bay

The district court for the District of Columbia presided over several hundred habeas corpus petitions filed on behalf of Guantánamo Bay detainees. The court referred preliminary matters in the first few cases to a retired senior judge. Another senior judge handled preliminary matters later. A magistrate judge presided over matters concerning habeas attorneys’ contacts with their clients.

Warrantless Wiretaps

In an action challenging a secret and allegedly illegal surveillance program, the judge considered naming a court-appointed national security expert “to assist the court in determining whether disclosing particular evidence would create a ‘reasonable danger’ of harming national security.” Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 1010–11 (N.D. Cal. 2006). The government objected to the suggestion, and the judge never decided that such an appointment was necessary.

Courts of Appeals

Appeals are typically heard by three judges with chambers in three different locations, all of which may be different from the place of hearing, and this poses a logistical challenge for the handling of classified information in the appeal.

Classified information may be present in the lower court record, the briefing, and oral argument. If part of the briefing is classified, it is proper for redacted briefs to be filed publicly and unredacted briefs to be filed with the classified information security officer. Some clerk’s offices are equipped with storage facilities for classified information, depending on the level of classification. Frequently, classified information security officers or cleared court personnel transport classified briefing between the location of storage and the judge. Sometimes, judges review classified briefing or classified portions of the record while they are at the court to hear other appeals.

Some appellate law clerks obtain security clearances to assist judges with cases concerning classified information. Nevertheless, sometimes the case file includes classified information designated for judges’ eyes only.

The membership of an appellate panel and the identity of judges writing opinions are determined well in advance of that information’s becoming public, so courts work with the classified information security officers to protect the confidentiality of the judges the security officers are visiting. It is important for judges to be confident that case assignments will not be leaked to government attorneys, for example, in advance of the information’s becoming public.

If it is likely that classified information will be discussed at oral argument, part of the argument will be closed. A classified information security officer will attend the open portion to interrupt if it appears that classified information will be disclosed. If the argument is recorded for public broadcast, arrangements are typically made for a delay to ensure that classified information is not inadvertently released publicly.

The court may elect to have its opinion reviewed for redaction of classified information. This review is performed in confidence and shielded from the parts of the government acting as a party in the case. If redaction is necessary, then a re-
dacted opinion will be issued publicly and the unredacted opinion will be provided only to those cleared to see it. Classified information must not appear on the public record, and it is important for courts to keep in mind their limited expertise in what is classified and what is not.

CASE NOTES

Twentieth Hijacker

The court of appeals' clerk's office anticipated that the prosecution of Zacarias Moussaoui for terrorism conspiracy would result in an appeal that included classified information in the court record. So the clerk's office worked with the classified information security officer to (1) create a SCIF and (2) begin the process of obtaining security clearances for several staff members. In 2009, the court worked with the classified information security officer to establish a new SCIF suitable for working in and meeting in, in addition to storage.

Judges can review classified information stored in the court's SCIF in Richmond, Virginia, when they are in town for oral arguments. At judges' home chambers, they can review classified documents stored in SCIFs in one of two ways. Either the classified information security officer can bring classified documents to the judges, or the documents can be stored in nearby SCIFs for the judges to review there. For example, Judge Wilkins had chambers in Greenville, South Carolina, and the courthouse there has a SCIF. Judge Williams had chambers in Orangeburg, South Carolina, which is approximately 50 miles from an FBI SCIF in Columbia. Judge Shedd's Columbia chambers are much nearer to the FBI SCIF in Columbia.

Judge Gregory's home chambers are in Richmond, so he always has ready access to the court of appeals' SCIF. He does not have a career law clerk, and security clearances can take such a large fraction of a temporary law clerk's tenure to acquire that he relies on a court of appeals staff attorney, who has a security clearance, to help him with matters involving classified information.

Briefs containing classified information were filed with the classified information security officer, and redacted briefs were filed in the public record. While the defendant was pro se, he filed many papers with the court of appeals as well as with the district court. The court of appeals typically regarded the filings as appeals, which were reviewed and dismissed. The court worked out a procedure with the jail where the defendant was being detained: the jail would forward a filing directly to the classified information security officer, who would notify the court that a document had been received. After a security review, a redacted version of the document would be filed in the public record.

For an unsuccessful petition to rehear en banc a ruling on an interlocutory discovery appeal, full briefs were filed in the court's Richmond SCIF, and redacted copies were sent to each judge. Some judges opted to review the full briefs in Richmond, and some judges opted to rely on the redacted briefs.

Four appeals were heard in this case, and all oral arguments included both a public session and a closed session a: which classified information could be discussed. At the public session, a classified information security officer and a CIA officer attended to monitor the proceeding in case it needed to be interrupted to prevent disclosure of classified information. At these public sessions, no interruption was necessary.

Dirty Bomber

In the habeas corpus appeal of Jose Padilla—originally detained as an alleged dirty bomber but later tried for terrorism conspiracy—the court of appeals reviewed classified declarations presented to the district court but found that it could decide the case without relying on them. Padilla v. Rumsfeld, 352 F.3d 695, 701 n.4 (2d Cir. 2003).

A Plot to Kill President Bush

In the appeal of Ahmed Omar Abu Ali, who was convicted of terrorism conspiracy and conspiracy to kill the President, part of the record and part of the briefing were classified. United States v. Abu Ali, 528 F.3d 210, 244 n.13 (4th Cir. 2008). Some of the materials were designated for judges' eyes only, which meant that even law clerks with security clearances could not see them. Classified ma-
aterials were filed through the classified information security officer. Classified materials for this case had to be stored in a SCIF, so judges either viewed them while in Richmond, Virginia, for a session or by using a SCIF near home chambers. Communications among members of the panel about classified matters could happen only in person or by secure fax. Part of oral argument was conducted in closed session.

**Mistaken Rendition**

The Court of Appeals for the Fourth Circuit affirmed a district court’s dismissal, on state-secrets grounds, of a complaint alleging that the CIA abducted and imprisoned Khaled El-Masri until the agency realized that it had picked up the wrong person. *El-Masri v. Tenet*, 479 F.3d 296 (4th Cir. 2007). The three judges hearing the appeal reviewed a classified declaration designated for judges’ eyes only while they were in Richmond, Virginia, where the court sits. One judge made a special trip from Charleston, West Virginia, to review the declaration; the other judges reviewed the declaration when they were in town to hear other cases. Deputy clerks with security clearances transported the declaration from the court’s SCIF to each judge’s chambers, and back again, for the judges’ private reviews. While considering El-Masri’s unsuccessful petition for certiorari, two Supreme Court justices also reviewed the classified declaration.

**Giving State Secrets to Lobbyists**

The court of appeals heard expedited appeals of district court rulings on classified evidence in a sting prosecution of lobbyists for sharing classified information. *United States v. Rosen*, 557 F.3d 192, 197 (4th Cir. 2009). Briefing included classified information, so classified briefs were filed with the classified information security officer, and redacted briefs were filed in the public record. Judges reviewed classified briefs either while they were in Richmond to hear an earlier case or at a SCIF near their home chambers. Parts of oral arguments were held in closed sessions so that the parties could discuss classified information with the court. Eight portions of the court of appeals’ published opinion resolving the district judge’s rulings on classified evidence are redacted.

**Warrantless Wiretaps**

Judges hearing appeals in actions challenging a secret and allegedly illegal surveillance program by the National Security Agency were asked by the government to receive classified ex parte arguments. Typically, the government lodged complete classified briefs and declarations for in camera review by the judges and filed redacted versions of these documents for the public record. Plaintiffs were not granted access to any classified information in these cases. One proceeding before the Court of Appeals for the Sixth Circuit was conducted under seal with both sides present, but plaintiffs otherwise had access only to public filings and proceedings.

Classified information security officers do not disclose to persons outside the court, including attorneys representing the government, their visits to judges’ chambers before the judges assigned to the appeal or the judge assigned to write the opinion has been made public.

The Court of Appeals for the Ninth Circuit permitted C-SPAN to televise oral argument so long as the program was not aired until after the court had an opportunity to excise any inadvertently disclosed secrets, a contingency that did not occur. The classified information security officer offered to review the court’s opinion for inadvertently disclosed classified information before the opinion’s release, but the court declined the offer.

**Torture Flights**

For a Ninth Circuit en banc panel review of a district court’s dismissal on state-secrets grounds of a tort action pertaining to extraordinary rendition, circuit judges could review classified ex parte briefing and declarations (1) in their chambers, delivered by a classified information security officer, or (2) in San Francisco, while in town for oral arguments.

Classified information security officers received advance notice that the case would be reheard en banc, but they keep such information confidential with respect to units of the government responsible for representing the government as a party.
Putting the Cat Back in the Bag

Occasionally classified information is inadvertently put into the public record or disclosed to someone who should not have received it. This occurrence typically presents a choice between corrective action, which might draw additional attention to the classified information, and a hope that the matter will be minimally noticed.

It is difficult to describe specific instances of this unfortunate occurrence without drawing further attention to classified information.

The court security officer must be consulted in the crafting of a remedy to inadvertently disclosed classified information.

CASE NOTES

Twentieth Hijacker

In the prosecution of Zacarias Moussaoui for terrorism conspiracy, even while the defendant was appearing pro se he was not supposed to have access to classified information. But, the government inadvertently included classified materials among documents produced to him. The government told the district judge that two documents produced to Moussaoui had mistakenly not been marked classified and asked that a “walled-off FBI team” search the defendant’s cell to retrieve the documents. The judge determined that even a walled-off FBI team would not adequately protect the defendant’s work product. Instead, the judge permitted the U.S. Marshals Service, in consultation with the classified information security officer, to search the prison cell for the two documents plus an additional five that the government identified in the interim as improperly produced. Of the seven searched for, five were found. By the following week, the government presented to the judge a list of 43 improperly produced documents. Many of the documents were prepared by FBI agents who were brought into September 11 investigations without sufficient training in handling and labeling classified information. Eventually, the documents were retrieved and properly marked as classified.

Warrantless Wiretaps

It is important to ensure that information redacted from the public record is redacted effectively. In an action challenging a secret and allegedly illegal surveillance program, a defendant telecommunication company electronically filed a brief with several lines redacted, but the redacted text could be retrieved easily from the electronic document. When this was brought to the court’s attention, the electronic text file was replaced with an electronic image file. The redacted information in this case was not classified, but was at most trade secrets.
Part II
Other Issues

Attorney–Client Issues

Attorney–client issues in national security prosecutions are similar to the issues in other criminal cases, but they tend to occur more frequently and be more serious.

Criminal Justice Act Appointments

Acting as a defense attorney in a prosecution for terrorism or espionage often requires special skills and a security clearance. Courts appointing defense counsel in national security cases often have to consider whether to make appointments outside of the routine selection of attorneys pursuant to the Criminal Justice Act.

Sometimes defense attorneys cannot obtain security clearances, and sometimes they are unwilling to submit to the necessary background checks. Courts sometimes appoint a cleared attorney to assist in a defense if only part of the case involves classified information. If the defendant elected to proceed pro se, then courts often appoint cleared counsel as backup.

CASE NOTES

Plot to Bomb New York City Tunnels and Landmarks

El Sayyid Nosair was a coconspirator of the blind sheik Omar Abdel Rahman in a plot to bomb New York City tunnels and landmarks in the 1990s. When the indictment was filed, Nosair was in prison on a state conviction related to the killing of Rabbi Meir Kahane, a former member of the Israeli parliament. United States v. Rahman, 189 F.3d 88, 105 & n.3 (2d Cir. 1999). Michael Warren had represented Nosair at the state murder trial. Warren had also appeared on behalf of Ibrahim el-Gabrowny, the first-indicted member of the bombing conspiracy, at el-Gabrowny’s first appearance on a criminal complaint filed in advance of the indictment. The district court denied Nosair’s request that Warren be appointed under the Criminal Justice Act (CJA), as an exception to regular CJA procedures. Instead, the court appointed a CJA panel attorney.

Prosecution of a Guantánamo Bay Detainee for 1998 Embassy Bombings

Ahmed Khalifan Ghailani was indicted in 1998 for participation in the bombing of the American embassies in Kenya and Tanzania, but after his capture in 2004 he was transferred to Guantánamo Bay until 2009, when he was transferred to the district court. United States v. Ghailani, 751 F. Supp. 2d 515, 518 (S.D.N.Y. 2010). Military commission proceedings had been initiated at Guantánamo Bay, and Ghailani asked that his military lawyers continue to represent him. But the Department of Defense did not consent to Ghailani’s request, and the district judge ruled that an indigent defendant does not have a constitutional right to select counsel.

The judge did agree to dismiss one appointed attorney because of the defendant’s dissatisfaction with him.

Lackawanna

For the high-profile prosecution of six Lackawanna men for attending a violent jihadist training camp in Afghanistan, a magistrate judge made a deliberate effort to appoint well-known and well-respected attorneys, including the federal defender, to represent the defendants.

Fort Dix

After being successfully prosecuted for conspiracy to attack Fort Dix, four defendants sought new counsel for their appeals. The district court determined that circumstances did not justify departure from the usual practice of trial counsel continuing on appeal.
Conflicts of Interest

In criminal cases, conflicts of interest are avoided by codefendants having separate counsel. Because conflicts are waivable, courts must often grapple with attorney and client preferences that could create conflicts.

CASE NOTES

Plot to Bomb New York City Tunnels and Landmarks

The first defendant indicted in the 1990s prosecution for a plot to bomb New York City tunnels and landmarks was Ibrahim el-Gabrowny, who was initially indicted for assaulting federal agents executing a search warrant of his home. *United States v. El-Gabrowny*, 35 F.3d 63, 64 (2d Cir. 1994). After one of the 1993 World Trade Center bombers, Mohammad A. Salameh, failed four attempts to get a New Jersey driver’s license, he got a New York driver’s license using el-Gabrowny’s address, so agents obtained a warrant to search the home as part of the investigation of the World Trade Center bombing. *United States v. Rahman*, 189 F.3d 88, 108 (2d Cir. 1999).

El-Gabrowny was represented by William M. Kunstler, a famous defense lawyer, see Albert Ruben, *The People’s Lawyer: The Center for Constitutional Rights and the Fight for Social Justice, From Civil Rights to Guantánamo* 91 (2011), at a preindictment bail hearing on a criminal complaint filed the day after the search. *United States v. Rahman*, 837 F. Supp. 64, 65 (S.D.N.Y. 1993). When the indictment was superseded to include Siddig Ibrahim Siddig Ali and others as defendants, Kunstler appeared for both el-Gabrowny and Siddig Ali. Over Kunstler’s objection, the district judge appointed for each defendant a CJA panel attorney to advise the defendant of the hazards of joint representation.

Nearly one month after the indictment was expanded to include blind sheik Omar Abdel Rahman, Abdel Rahman’s retained attorney notified the court that he could no longer represent his client because they could not agree on a fee agreement. *United States v. Rahman*, 861 F. Supp. 266, 271 (S.D.N.Y. 1994). Kunstler appeared for Abdel Rahman, but the government objected to Kunstler’s representing multiple defendants, and the court ruled that Kunstler could represent either el-Gabrowny and Siddig Ali or Abdel Rahman, but not all three. Abdel Rahman opted to represent himself, and the judge appointed a CJA panel attorney to assist him. Abdel Rahman was fully represented by the time of trial.

Seven months before trial, Siddig Ali obtained substitute counsel to help him try to cooperate with the government, but the government decided not to strike a deal. The district court determined that Kunstler could not resume representation of Siddig Ali because of Siddig Ali’s actions adverse to the interests of Kunstler’s other past and present clients. The court also determined that Kunstler’s various current and previous associations with several defendants in the case meant that he could no longer represent el-Gabrowny.

First Prosecution for 1998 Embassy Bombings

A severe conflict of interest arose when a defendant in the prosecution for the 1998 bombings of American embassies in Kenya and Tanzania stabbed a prison guard, because the defendant’s attorneys were not only witnesses to the stabbing but potential targets of a more elaborate scheme of violence. *United States v. Bin Laden*, 160 F. Supp. 2d 670, 673 (S.D.N.Y. 2001). Because the trial was scheduled to begin only two months later, the defendant was severed from the trial. He pleaded guilty to attempted murder for the stabbing and has not been tried for the bombings.

Prosecution of a Charity

In the prosecution of the Holy Land Foundation and all of its principals for providing funds to Hamas, the foundation and its CEO were represented by the same attorney until the eve of trial on a waiver of conflict signed by the foundation’s chairman. At the pretrial oral conflict colloquy, the attorney for the chairman announced that he was not sure his client could speak for the foundation. The attorney for the CEO said that she was not sure anyone could speak for the foundation, so the
judge allowed her to withdraw as the foundation’s attorney, and the trial proceeded without the foundation’s having representation. A mistrial resulted from the jury’s deadlock on counts against all defendants, and a different judge presided over the retrial because of the first judge’s taking senior status and no longer taking criminal cases. Because the docket sheet did not reflect the foundation’s attorney’s withdrawal, the second judge did not know that the foundation was not represented until sentencing. The sentencing judge determined that the foundation had de facto representation because of its common interests with the other defendants, and the issue is now on appeal.

Atlanta
In a prosecution of two young men in Atlanta for preparing for violent jihad by, among other things, making casing videos of strategic landmarks, Ehsanul Islam Sadequee was represented by the federal defender’s office. Sadequee was assaulted in detention by another inmate who was also represented by that office. The office, therefore, could no longer represent Sadequee, and another attorney was appointed.

Communication
Communication between defense attorneys and their clients in national security cases can be made complicated by (1) the attorneys’ not being able to share classified information with their clients and (2) security measures that infringe on the privacy or even possibility of attorney–client communications.

CASE NOTES

First Prosecution for 1998 Embassy Bombings
When the original defendants in the prosecution for the 1998 bombings of American embassies in Kenya and Tanzania were detained, they were cut off from virtually all communications. United States v. Bin Laden, 92 F. Supp. 2d 225, 231–32 (S.D.N.Y. 2000). The defendants were permitted to meet with their attorneys, but the attorneys were prohibited from sharing anything said in the attorney–defendant meetings with investigators or experts, which seriously hampered the preparation of a defense.

Millennium Bomber
Because of an error by personnel at a Canadian courthouse, the attorneys representing Ahmed Ressam, who planned to drive from Canada to bomb the Los Angeles International Airport at the turn of the millennium, were permitted to copy certain documents in Canada, but they had to surrender the copies when the error was discovered. The U.S. prosecution moved for an order prohibiting the attorneys from discussing the documents with their client. The district judge told the attorneys that they could use the information that they obtained from the Canadian files as a last resort, but they could not disclose to their client the origin of the information.

Guantanamo Bay
Information provided to their habeas attorneys by Guantanamo Bay detainees was presumptively classified. A “privilege review team,” walled off from attorneys representing the government in litigation, performed a classification review on detainee communications and their lawyers’ notes.

Dirty Bomber
Jose Padilla, who was originally detained on a material witness warrant as part of the grand jury investigation of the September 11, 2001, attacks, was transferred to military detention and designated an enemy combatant for an alleged plan to detonate a dirty bomb. Padilla ex rel. Newman v. Bush, 233 F. Supp. 2d 564, 571 (S.D.N.Y. 2002). The government denied Padilla access to counsel upon his transfer to military custody, arguing that Padilla might use contacts with counsel to communicate with other terrorists. The district court determined that Padilla was entitled to counsel “for purposes of presenting facts to the court in connection with” a habeas corpus petition.
Paintball

In the prosecution of Ali al-Timimi, the spiritual leader of northern Virginia men who played paintball in preparation for violent jihad, defense attorneys claimed that the Bureau of Prisons opened the defendant’s clearly labeled attorney-client mail and transferred the defendant so frequently from prison to prison that it was difficult for the attorneys to know where he was and make arrangements to see him. The judge ordered the defendant returned to the district.

Rapport

Terrorism defendants’ attitudes toward the U.S. system of justice often range from distrust to hatred. This often makes rapport between defendants and their attorneys, especially appointed attorneys, difficult.

When appointing an attorney to represent a terrorism defendant, the court may want to consider the attorney’s experience with difficult clients or with clients from other cultures. There are many potential pitfalls. For example, attorneys often use humor to foster rapport with their clients, but that strategy is frequently risky in these cases.

Terrorism defendants may be more likely than other criminal defendants to act against the advice of counsel, such as by pleading guilty or electing to proceed pro se.

CASE NOTES

First Prosecution for 1998 Embassy Bombings

One of the attorneys appointed to represent a defendant in the original prosecution for the 1998 bombings of American embassies in Kenya and Tanzania had to be dismissed for mocking his client’s religious beliefs. When the client explained to the attorney his belief that a martyr would have 13 virgin brides in paradise, the attorney jokingly lamented having 13 fathers-in-law. On the next morning, the judge found on his desk a request by the defendant for a new attorney. The judge granted the request.


Twentieth Hijacker

The district court appointed the federal defendant and a private attorney to represent Zacarias Moussaoui in his prosecution for terrorism conspiracy. United States v. Moussaoui, 591 F.3d 263, 267 (4th Cir. 2010). The defendant had a strained relationship with his attorneys, especially with the private attorney. At a hearing on conditions of confinement, four months after his indictment, Zacarias Moussaoui announced that he would like to represent himself, possibly with the assistance of a Muslim attorney, because his assigned attorneys did not understand Muslims. Id. at 269–70; United States v. Moussaoui, 333 F.3d 509, 512–13 (4th Cir. 2003).
Moussaoui identified a Muslim attorney in Texas whom he wanted to consult with, but this attorney never made an appearance, never sought admission to the court’s bar, and never consented to the screening required for the security clearance that would be needed to represent Moussaoui in court.

While Moussaoui was proceeding pro se, the district judge appointed a second private attorney as standby counsel; by the end of the case, this was the attorney that the defendant was most willing to talk to because the defendant judged him to be the most respectful.

Toledo
In a prosecution of Americans for conspiracy to fight against U.S. forces in Iraq, the judge appointed the federal defender’s office as counsel for one of the defendants. The defendant was concerned that a government employee would not represent him adequately, and the judge reluctantly agreed to appoint substitute counsel. The defendant, however, was no more satisfied with substitute counsel, and he eventually asked the judge to reappoint the federal defender’s office, which the judge did.

Conditions of Detention
Conditions of detention for persons accused of doing harm to our national security are often very strict. Strict detention security measures are sometimes referred to as special administrative measures (SAMs).

Judges are often attentive to the possibility that security measures will impair an effective defense, especially with respect to the confidentiality and effectiveness of attorney–client communications and the defendant’s mental health.

Security
Security measures for national security defendants can include solitary confinement. Security is tight to prevent defendants from communicating with conspirators. Also, national security defendants are often at an elevated risk of harm from other inmates.

Courts have not found incarceration necessary to ensure all national security defendants’ presence for trial. Bail, perhaps with electronic monitoring or home detention, has been found sufficient for some.

CASE NOTES

First Prosecution for 1998 Embassy Bombings
When the original defendants in the prosecution for the 1998 bombings of American embassies in Kenya and Tanzania were detained, they were held in solitary confinement. United States v. Bin Laden, 92 F. Supp. 2d 225, 231–32 (S.D.N.Y. 2000). In response to complaints by defense attorneys, the district judge visited the jail and approved the conditions of detention, except that he ordered that the defendants be permitted to call their families three times a month instead of once. United States v. El-Hage, 213 F.3d 74, 77 (2d Cir. 2000).

Minneapolis
Mohamed Abdullah Warsame, who was indicted for attending Al-Qaeda training camps, was held in solitary pretrial detention for over five years. The district judge observed a resulting decline in the defendant’s mental health. The case was resolved by a plea bargain.

Chicago
In the prosecution of Muhammad Abdul Hamid Khalil Salah and Abdelhaleem Hasan Abdelrazig for helping to provide funds to Hamas, the judge permitted friends and relatives to post nearly $4 million worth of property to secure detention by home confinement.
Toledo
In a prosecution of Americans for conspiracy to fight against U.S. forces in Iraq, the judge decided that one of the defendants could be released on bond with electronic monitoring.

Access to Counsel
Because the government is worried about terrorism suspects’ communicating with terrorism conspirators, either directly or indirectly, there is often an effort to restrict or monitor counsel visits with and communication with their clients. Judges frequently attend to the possibility of excessive restrictions or monitoring. Sometimes judges intervene formally. Sometimes more informal inquiries and suggestions can achieve positive results.

CASE NOTES
Dirty Bomber
In the trial of Jose Padilla—who was originally detained as a dirty bomber but ultimately tried with two other men for terrorism conspiracy—the district court was called upon to issue orders directing the detention center to provide defendants with adequate access to counsel. One order granted defendants two 15-minute telephone calls with their attorneys each week: “During these legal telephone calls the [federal detention center] officials shall stay a reasonable distance away from the Defendant to allow for sufficient privacy.” Order, United States v. Hassoun, No. 0:04-cr-60001 (S.D. Fla. Sept. 21, 2005). As trial approached, the judge ordered the detention center to provide a larger conference table for meetings between the defendants and their attorneys.

Minneapolis
Mohamed Abdullah Warsame, who was indicted for attending Al-Qaeda training camps, was represented by the federal defender’s office. For a time, the government imposed restrictions on who in the defender’s office could communicate with Warsame, and the defender’s office could not agree to the restrictions. Eventually, the two sides were able to work out an agreement.

Mental Health
Strict conditions of detention, especially solitary confinement, can have a negative impact on a defendant’s mental health. Judges often attend to this possibility to ensure that the defendant’s ability to participate in his defense is not impaired.

Courts must nevertheless be wary of false or exaggerated claims of mental health impairment.

For a defendant held in solitary confinement as a preventive security measure, court appearances can be therapeutic. On the other hand, sometimes body searches performed on defendants as they are transported between court and the place of confinement can be unpleasant.

CASE NOTES
First Prosecution for 1998 Embassy Bombings
During a hearing, after several months of restrictive confinement, Wadih el-Hage, one of the defendants in the prosecution for the 1998 bombings of American embassies in Africa, angrily criticized the district judge for not reading a letter el-Hage had prepared proclaiming his innocence and contending that the United States could have prevented the bombings. In re Terrorist Bombings of U.S. Embassies in East Africa, 552 F.3d 93, 149 (2d Cir. 2008). Deputy marshals restrained the defendant when he leapt from his chair in the courtroom and appeared to charge the judge. Ap-
proximately six months later, a psychiatrist reported that el-Hage’s solitary confinement was seriously impairing his mental health. The prison agreed to give el-Hage a cell mate, but the court ruled that his conditions of confinement were largely proper, and el-Hage complained that the cell mate made his cell too crowded.

After a prison guard was stabbed by a co-defendant, an incident not involving el-Hage, the prison removed el-Hage’s possessions and privileges. According to his wife, his mental state deteriorated sharply and he stopped recognizing his attorney. However, two court-appointed psychiatrists and a court-appointed psychologist determined that el-Hage was faking mental illness. The judge decided that the expert opinions were well founded and that el-Hage was competent to stand trial.

Prosecution of a Guantanamo Bay Detainee for 1998 Embassy Bombings
During the 2010 prosecution of Ahmed Khalifan Ghailani, a onetime fugitive, for the 1998 bombings of American embassies in Kenya and Tanzania, the defendant complained that intrusive body cavity searches every time he appeared in court were causing him post-traumatic stress disorder. The district judge determined that the defendant was not suffering from post-traumatic stress disorder and denied relief. United States v. Ghailani, 751 F. Supp. 2d 508, 514 (S.D.N.Y. 2010). The defendant began to appear in court less frequently.

Guantanamo Bay

Guantanamo Bay detainees occasionally protested their confinement with hunger strikes and, more rarely, suicide attempts, some of which were successful. The district court determined that Congress had stripped the detainees of habeas rights concerning the conditions of their confinement, but that they could challenge conditions that affected their abilities to work with their attorneys on their cases, so the court sometimes was called on to issue orders concerning detainees’ medical issues.

Dirty Bomber

Jose Padilla, who was originally detained on a material witness warrant as part of the grand jury investigation of the September 11, 2001, attacks, was transferred to military detention and designated an enemy combatant for an alleged plan to detonate a dirty bomb. Padilla ex rel. Newman v. Bush, 233 F. Supp. 2d 564, 571 (S.D.N.Y. 2002). During his military detention, the government applied substantial psychological pressure as part of the detainee’s interrogation. Padilla ex rel. Newman v. Rumsfeld, 243 F. Supp. 2d 42, 43 (S.D.N.Y. 2003). Padilla was subsequently transferred to civilian custody for a trial with two other men for terrorism conspiracy, unrelated to a dirty bomb, and Padilla’s attorneys claimed that the psychological pressure during military detention had resulted in incapacitating post-traumatic stress disorder. Because the security measures imposed for Padilla’s pretrial detention made psychiatric evaluation difficult within the detention center, the district judge provided her courtroom, without the judge present, for the evaluation. The judge found Padilla competent to stand trial.

For security reasons, Padilla and his co-defendants were detained in solitary confinement. Three months after they were convicted, one defendant attempted suicide.

Minneapolis

Mohamed Abdullah Warsame, who was indicted for attending Al-Qaeda training camps, was held in solitary pretrial detention for over five years. For the sake of the defendant’s mental health, the judge encouraged the defendant’s attendance at proceedings, which afforded him time outside his cell and time in the presence of other people. Warsame was a Canadian citizen, and visits by the Canadian consulate were also helpful.

Cultural Accommodation

Prosecutions for assaults on national security may entail elements of cultural diversity. Judges strive to prevent cultural differences from creating distractions from the pursuit of justice.
For example, prosecutions of Muslim defendants as suspected terrorists have accommodated breaks for prayers and religious holidays. Some judges take testimony by affirmation rather than by oath so that jurors are not biased by unnecessary religious references.

CASE NOTES

First Prosecution for 1998 Embassy Bombings
The district judge carefully timed breaks in the trial to permit prayer at the appropriate times by the Muslim defendants, whose entry to and exit from the courtroom were made cumbersome by their hidden shackles.

Twentieth Hijacker
In his prosecution for terrorism conspiracy, Zacarias Moussaoui refused to honor the judge by standing when she entered or left the courtroom, so the judge arranged proceedings so that she and the defendant would enter and leave the courtroom at the same time.

Lackawanna
For the prosecution of six Lackawanna Muslim men for attending a violent jihadist training camp in Afghanistan, the district court timed hearings to accommodate both daily prayers and religious holidays. All testimony at the detention hearing before a magistrate judge was taken from government witnesses under oath, but the defendants’ pleas before the district judge were taken by affirmation.

Paintball
In the prosecution of northern Virginia men for playing paintball in preparation for violent jihad and for attending terrorist training camps in the Middle East, the district judge took all testimony by affirmation rather than by oath, a practice she developed so that no bias could result from whether a witness swore on a Bible or a Quran.

Atlanta
In a prosecution of two young men in Atlanta for preparing for violent jihad by, among other things, making casing videos of strategic landmarks, the court appointed a Muslim attorney from a nearby district to represent one of the defendants.

High Profile
National security cases are often high in profile. Sealing parts of the case record and closing some proceedings to protect national security often fosters curiosity in the news media about what they are missing. Otherwise, issues relating to some high-profile national security cases are largely similar to issues that arise in other high-profile cases.

Gag Orders
In high-profile cases, especially criminal cases, judges often consider issuing gag orders restricting the participants’ public comments on the cases so that prospective jurors will not be improperly influenced. The parties often stipulate to such orders. Appellate courts work to ensure that gag orders are no more restrictive than necessary.

CASE NOTES

First World Trade Center Bombing
In the prosecution for the 1993 bombing of the World Trade Center, the Court of Appeals for the Second Circuit vacated as overbroad a district court gag order prohibiting attorneys from making any public statements related to the case. United States v. Salameh, 992 F.2d 445, 447 (2d Cir. 1993). The district judge issued the gag order orally and sua sponte at arraignments one day after a superseding in-
dictment was filed, which was two weeks after the original indictment was filed. The judge said that his primary interest was retaining venue. But the court of appeals held that the gag order was not narrowly tailored.

An order that prohibits the utterance or publication of particular information or commentary imposes a “prior restraint” on speech. A prior restraint on constitutionally protected expression, even one that is intended to protect a defendant's Sixth Amendment right to trial before an impartial jury, normally carries a heavy presumption against its constitutional validity. *Id.* at 446–47.

**Detroit**

In the first post-September 11, 2001, prosecution for terrorism, the judge issued a stipulated gag order forbidding public comments about the case that would have a reasonable likelihood of interfering with a fair trial. Eight days later, the Attorney General incorrectly stated at a press conference that the defendants were “suspected of having knowledge of the September 11th attacks.” *United States v. Koubrite*, 305 F. Supp. 2d 723, 725, 728–30, 733 (E.D. Mich. 2003). Also, during the trial, the Attorney General commented favorably at a press conference on the credibility of a cooperating codefendant’s testimony. The judge issued “a public and formal judicial admonishment of the Attorney General.” *Id.* at 726.

**Media Attention**

Enhanced media attention in a case poses two types of challenge for the court: (1) an increase in the number of people visiting the courthouse, many of whom come with extensive collections of electronic equipment, and (2) an increased expectation of the amount of information provided.

Most news media pay attention only to major events in a case, although some news media may follow the case in greater detail. It is not always predictable what will draw heavy media attention.

Managing the logistics of media attention can be quite a challenge. An increase in the number of persons visiting the courthouse often requires additional security considerations, including attention to the efficiency of security in light of the increased number of visitors. Courts have to address the issue of what electronic equipment can be brought into the courthouse. Even if electronic equipment is forbidden in the courtroom, courts often accommodate it elsewhere in the courthouse, such as in an overflow courtroom.

Logistical issues pertaining to an increase in courthouse visitors often extend to the neighborhood. Courts often work with local authorities to anticipate and manage increased traffic near the courthouse. This increased traffic often includes large media vehicles parked to transmit information.

Media reports on the courthouse steps are a common practice. Because of weather, security, or logistical issues, courts may prefer that media reports be delivered from another location. Courts sometimes have space they can use as a media room for this purpose.

It is helpful to both the court and the media for the court to provide the media with a designated contact person for information and for what the media can expect in terms of schedules, filings, and proceedings. *E.g.*, Steve Leben, *Ten Tips for Judges Dealing with the Media*, 47 Ct. Rev. 38 (2011).
CASE NOTES

_Lackawanna_

The prosecution of six Lackawanna men for attending a violent jihadist training camp in Afghanistan drew media attention from all over the world. The pretrial detention hearing was held soon after the first anniversary of the September 11, 2001, attacks. The public square in front of the courthouse was filled with large media vans, and there were public picketers in the square and around the courthouse. A popular picket read, “Jail, No Bail.” The magistrate judge who conducted the hearing strove to provide the government and the defendants with a fair and peaceful hearing, mindful that the world was watching how the criminal defendants were treated.

_Atlanta_

A prosecution of two men for preparing for violent jihad by, among other things, making casing videos of strategic landmarks received extensive media coverage, especially by local news media. One local journalist sat through the entire trial.

Several news media attended a routine status conference held in the magistrate judge’s chambers, because there had been talk of closing the proceeding. The judge observed that sealing documents and closing proceedings often intensifies news media interest.

_Fort Dix_

A prosecution for conspiracy to attack Fort Dix received substantial media attention. In part because of the cold December weather in Camden, New Jersey, where the trial was held, the judge did not want press conferences on the steps of the courthouse following the verdict, so news media were asked to gather in the jury assembly room. The government addressed the media for the first half hour; then defense counsel and families of the defendants addressed the media. The media could bring in cameras and recording devices during these presentations. Because it worked well, a similar procedure was used after sentencing.

Reserved Seating

If spectator space in the courtroom will be at a premium, courts often work with the deputy marshals and security officers to ensure that some seating is reserved for the defendants’ families, persons affiliated with alleged victims, news media, and the public, respectively.

CASE NOTES

_Prosecution of a Guantánamo Bay Detainee for 1998 Embassy Bombings_

In the 2010 trial of Ahmed Khalafan Ghailani, a onetime fugitive, for the 1998 bombings of American embassies in Kenya and Tanzania, the judge reserved some seats in the courtroom for the news media.

_Atlanta_

At a trial of two young men for preparing for violent jihad by, among other things, making casing videos of strategic landmarks, the judge reserved a row of seats for the news media. Because it was a bench trial, the judge permitted sketch artists to sit in the jury box.

Remote Viewing

It is common for courts to set aside at least one additional courtroom during high-profile cases. Proceedings in the main courtroom are displayed in the overflow courtroom audiovisually. In some cases, courts have transmitted proceedings audiovisually to remote locations, such as other courthouses in the district or courthouses in other locations where interest is likely to be high.
Some judges provide the media with an overflow courtroom in which media members can use electronic equipment. On occasion, the news media have been permitted to use some electronic equipment in the main courtroom.

The extent to which overflow courtrooms are actually used, especially in remote locations, is often unpredictable.

CASE NOTES

Twentieth Hijacker
In the penalty trial for Zacarias Moussaoui, to determine whether he should be executed, proceedings were broadcast to viewing sites in Manhattan, Central Islip, Boston, Philadelphia, Newark, and a second courtroom in Alexandria, Virginia, for family members of September 11, 2001, victims. Fewer people watched the proceedings at off-site locations than was anticipated.

Fort Dix
For a high-profile prosecution charging conspiracy to attack Fort Dix, the court designated two overflow courtrooms: one for the news media and one for the rest of the public. Because the judge permitted the media to use laptop computers in the main courtroom and gave them wireless Internet access, they did not use their overflow courtroom. Journalists used the court’s wireless Internet access to blog about the case in real time. Recording devices were not permitted in the courtroom, published likenesses of the jurors were prohibited, and members of the public were forbidden from bringing in electronic equipment. The overflow courtroom was needed for the rest of the public on the first day of the trial and on the day of the verdict.

Courtroom Displays of Support or Opposition
Judges typically do not allow persons attending a trial in support of one of the parties to in any sense become a cheering section, especially if the case is tried before a jury.

CASE NOTES

First Prosecution for 1998 Embassy Bombings
In the original trial for the 1998 bombings of American embassies, many survivors of the bombings attended the trial wearing lapel pins, provided by a victims’ advocate, showing a map of Africa with Kenya and Tanzania highlighted. The pins helped the deputy marshals identify victims for appropriate seating; but after defense counsel argued that the pins would improperly influence the jurors, the judge ordered that they not be worn.

Making Filings and Evidence Available to News Media
Court filings are now available on the Internet through PACER (Public Access to Court Electronic Records). Use of PACER, however, requires a PACER account. Although filings by the judge typically are available in PACER without charge, other filings are only available for a per-page fee. In a high-profile case, a court will often set up a special webpage at the court’s Internet site and post all filings for the case there. That makes these filings available free of charge to anyone with access to the Internet, including news media, without their need to contact the court.

Some courts also work to promptly post on the Internet trial exhibits and even proceeding transcripts.
CASE NOTES

Atlanta
In a prosecution for preparing for violent jihad by, among other things, making casing videos of strategic landmarks, news media had access to all of the evidence on the day that it was admitted. The U.S. Attorney's Office was responsible for providing copies of evidence to the media.

Fort Dix
For a high-profile prosecution charging conspiracy to attack Fort Dix, the court set up a public website where documents in the case file were posted. This allowed access to the documents without going through PACER. Evidence was posted the moment it was admitted. Each side loaded digitized exhibits on a secure server in advance of moving for their admissibility. Neither side had access to the other side's exhibits on the server until they were admitted.

The court also posted proceeding transcripts on the server in a way that permitted free access to the proceedings while protecting the court reporters' proprietary rights in the transcripts. Transcript text rolled on the public website in continuous loops so that a website visitor would see whatever few lines of text were displayed at that moment, and lines of text scrolled by as the viewer looked at the transcript.

Courthouse Security
Concerns about physical security during trials and other proceedings are often heightened in high-profile cases involving persons possibly prone to dangerous behavior or in cases that might attract the interest of persons prone to dangerous behavior.

Sometimes, defendants are discreetly shackled. Sometimes, courts establish additional security at entrances to both the courthouse and the courtroom. The anticipated volume and type of traffic near the courthouse may be a reason for additional perimeter security.

One downside of tight security in a criminal jury trial is a possibly prejudicial message it might send to the jury that the defendants might be dangerous.

CASE NOTES

Plot to Bomb U.S. Airplanes in Southeast Asia
In the trial for conspiracy to bomb American airplanes in southeast Asia, the district judge had to dismiss the first 75 prospective jurors because they indicated that they would be influenced by heavy court security.

First Prosecution for 1998 Embassy Bombings
In the original prosecution for the 1998 bombings of American embassies in Kenya and Tanzania, defendants were always shackled when in the courtroom because of an incident during a hearing in which a defendant began to angrily charge toward the judge. When the jury trial began, a screen at the defense table covered the defendants' shackles and jurors were not present when the defendants were brought in and out. Persons in the courtroom were not asked to rise when the judge entered. Persons entering the courtroom had to pass through a metal detector and sign a log book stating their purpose in attending the trial. The jury room was guarded by deputy marshals and checked each morning by bomb-sniffing dogs.

The defendants were sentenced on October 18, 2001. In re Terrorist Bombings of U.S. Embassies in East Africa, 552 F.3d 93, 102 (2d Cir. 2008); United States v. Bin Laden, 397 F. Supp. 2d 465, 474 (S.D.N.Y. 2005). Because of the recent and nearby attacks on September 11, court security on the day of sentencing was substantially enhanced. According to the New York Times, "The building resembled a military base, with federal marshals carrying shotguns, public entrances

National Security Case Management (2011)

**Millennium Bomber**

At the first appearance in court in Seattle of Ahmed Ressam, who planned to bomb the Los Angeles International Airport at the turn of the millennium, “Security was so tight at the courthouse that anyone entering—even employees—had to produce a photo identification. A phalanx of U.S. marshals also blocked the door to [the magistrate judge’s] courtroom and armed officers patrolled the streets as Ressam was brought to the courthouse.” Scott Sunde & Elaine Porterfield, *Wider Bomb Plot Possible*, Seattle Post-Intelligencer, Dec. 18, 1999, at A1.

For the subsequent trial in Los Angeles also, security was enhanced, including added patrols, bomb-sniffing dogs, and inspections of cars entering the underground garage.

**Twentieth Hijacker**

The federal courthouse in Alexandria, Virginia, had never seen such a level of security as it saw for the prosecution of Zacarias Moussaoui for terrorism conspiracy. At his arraignment, Moussaoui arrived before 6:00 a.m., while it was still dark. Deputy marshals surrounded the courthouse, and extra metal detectors were stationed at the courtroom. Although the outside air was frigid, members of the news media and the public were not allowed into the building until shortly before the hearing. At subsequent appearances also, extra deputy marshals guarded the courthouse.

**Dirty Bomber**

In the Miami trial of three men—including Jose Padilla, who was originally detained as a dirty bomber but was ultimately tried for terrorism conspiracy—federal deputy marshals were brought in from around the country to provide the courthouse with extra security. An extra metal detector was installed outside the courtroom door.

**Lackawanna**

For the prosecution of six Lackawanna men for attending a violent jihadist training camp in Afghanistan, the marshal established extra security at the courthouse doors. The courthouse received security sweeps three times a day, and security included a bomb-sniffing dog. The defendants pleaded guilty; during the days of pleas and sentences, armed surveillance officers were posted at the windows in the judge’s chambers.

**Toledo**

In a prosecution of Americans for conspiracy to fight against U.S. forces in Iraq, the judge was concerned about the impact on potential jurors of highly visible extra security. For example, parked outside the courthouse was a conspicuously marked Department of Homeland Security SUV. It did not help that one news station reported on the case with a graphic titled, “Terror in Toledo.” The judge worked with security forces to convey less of a siege image.

**Fort Dix**

In a high-profile trial for conspiracy to attack Fort Dix, court security was enhanced. Additional precautions were taken during the two days of sentencing. No other judge scheduled proceedings for those days, and court staff were encouraged to work at home. Because a jury was not present, there was a greater visible presence of security.

**Jury Issues**

Jury trials in national security cases present issues common to jury trials in other high-profile trials in which security is a matter of concern.

**Size of Venire**

Sometimes national security trials are long and complex, which means the court will have to assemble a large venire to allow for hardship excuses. Often it is anticipated that the facts of the case will stimulate prejudicial emotions among potential jurors, so judges sometimes allow for extra challenges and a larger venire.
to accommodate them. On the other hand, sometimes a normal-sized venire can be used for a national security case.

CASE NOTES

First World Trade Center Bombing
According to news media, the district court issued 5,000 extra jury summonses to assemble a jury pool for the trial against those accused of bombing the World Trade Center in 1993.

First Prosecution for 1998 Embassy Bombings
In the original prosecution for the 1998 bombings of American embassies in Kenya and Tanzania, the district judge screened a jury pool of 1,302 people with the help of a questionnaire.

Millennium Bomber
In the prosecution of Ahmed Ressam, who planned to bomb the Los Angeles International Airport at the turn of the millennium, a jury was selected from 44 prospective jurors after a little more than seven hours of voir dire.

Detroit
In the first post-September 11, 2001, prosecution for terrorism, the district court selected 280 prospective jurors for the case.

Twentieth Hijacker
In the prosecution of Zacarias Moussaoui for terrorism conspiracy, the district court sent out more than 1,000 jury summonses and had more than 500 potential jurors fill out jury questionnaires.

Dirty Bomber
In the trial of Jose Padilla, originally detained as a dirty bomber but ultimately tried for terrorism conspiracy, the district judge decided to send out 3,000 jury duty letters for the trial. Jurors were selected from an initial pool of approximately 300, and then from a pool culled using a jury questionnaire of 88 potential jurors.

Anonymous Jury
If defendants are likely to be dangerous or associated with dangerous people, judges often consider using anonymous juries to protect the jurors’ safety. Sometimes judges use anonymous juries to protect jurors from media harassment in high-profile cases. Judges are often cautious about using an anonymous jury to protect the jurors’ safety, because a suggestion that the jurors are in danger may have a prejudicial impact. On the other hand, jurors’ safety is a crucial consideration.

Sometimes the identities of anonymous jurors are known to the judge and the parties, but not the news media or the public; sometimes the jurors’ identities are known only to a few members of the clerk of court’s staff.

Voir dire of prospective anonymous jurors has sometimes been conducted in closed session. Judges have sometimes accommodated a public right of access to voir dire by releasing redacted transcripts or allowing select news media representatives to attend.

CASE NOTES

First World Trade Center Bombing
The district judge used anonymous juries for the two trials. When an alternate juror’s anonymity became at risk in the second trial, the judge dismissed the juror.

Plot to Bomb New York City Tunnels and Landmarks
The district judge used an anonymous jury. Voir dire was conducted in a conference room with the news media represented by two re-
First Prosecution for 1998 Embassy Bombings

In the original trial for the 1998 bombings of American embassies in Kenya and Tanzania, the district judge used an anonymous jury and closed jury selection.

Prosecution of a Guantánamo Bay Detainee for 1998 Embassy Bombings

In the 2010 trial of onetime fugitive Ahmed Khalifan Ghailani, the district judge used an anonymous jury.

Millennium Bomber

In the prosecution of Ahmed Ressam, who planned to bomb the Los Angeles International Airport at the turn of the millennium, the judge was not asked to use an anonymous jury; he has never used one.

Detroit


Twentieth Hijacker

In the prosecution of Zacarias Moussaoui for terrorism conspiracy, the district judge used an anonymous jury. Jurors assembled in a secret location and were driven to the courthouse. The court set up a special lunch room for the jurors, away from the public. Jurors were never permitted to be in the building unsupervised.

Dirty Bomber

In the Miami trial of three men—including Jose Padilla, who was originally detained as a dirty bomber but was ultimately tried for terrorism conspiracy—jurors’ identities were known to the court and the parties, but identifying information was not presented in open court or otherwise made public.

Chicago

In the prosecution of Muhammad Abdul Hamid Khalil Salah and Abdelhaleem Hasan Abdelraqiq for helping to provide funds to Hamas, the judge denied a government request for an anonymous jury, observing that the defendants were not in custody and that they had strictly adhered to the terms of their release and otherwise posed no danger.

Toledo

In a prosecution of Americans for conspiracy to fight against U.S. forces in Iraq, the judge used an anonymous jury. To minimize prejudice, the judge told the jurors that this was customary in a criminal case.

Sears Tower

For the prosecution of the “Liberty City Seven” for conspiracy to topple the Sears Tower and attack other buildings in various cities, the judge initially did not use an anonymous jury. Because an attorney working for one of the defendants gave a list of the jurors’ names to members of a defendant’s family, the judge used anonymous juries for the next two trials, which were required because of hung juries.

Fort Dix

In a high-profile trial for conspiracy to attack Fort Dix, the judge used an anonymous jury. Each juror met at one of two secret locations; deputy marshals shuttled the jurors to the courthouse. After the trial, jurors were given contact information for members of the news media, and they could contact them if they wished, but the media were not permitted to initiate the contacts.

Jury Questionnaire

In high-profile or sensitive cases, judges often accommodate the need to ask lots of voir dire questions by using a jury questionnaire. Such a questionnaire should be reviewed carefully to ensure that the questions are clear. Usually, shorter questionnaires are more likely to elicit more complete and thoughtful answers.
Some judges are disinclined to use jury questionnaires, preferring to conduct all voir dire orally, often with carefully prepared questions.

A jury questionnaire is always followed by individual oral voir dire of prospective jurors who have not been excluded on the basis of their questionnaire answers.

The Federal Judicial Center has assembled a selection of jury questionnaires used in national security cases: *National Security Prosecutions: Jury Questionnaires and Preliminary Remarks to Prospective Jurors.*

**CASE NOTES**

**First World Trade Center Bombing**
The district judge did not use a jury questionnaire, because “[t]here has been . . . absolutely no showing that jury questionnaires are of any particular help in the selection of a jury in highly publicized cases where a searching voir dire is conducted.” *United States v. Salameh*, No. 93-cr-180, 1993 WL 364486, at *2 (S.D.N.Y. Sept. 15, 1993).

**Plot to Bomb New York City Tunnels and Landmarks**
The district judge used a jury questionnaire, which he had seldom done before, and he found it very helpful.

**First Prosecution for 1998 Embassy Bombings**
In the original trial for the 1998 bombings of American embassies in Kenya and Tanzania, the district judge used a jury questionnaire. The judge discovered that the questionnaire caused many jurors to assume that the court would tell them what penalty would go with each crime, and the questionnaire did not make clear that ultimate decisions on the death penalty would be made by the jury.

**Prosecution of a Guantánamo Bay Detainee for 1998 Embassy Bombings**
For the 2010 trial of Ahmed Khalfan Ghailani, a onetime fugitive, the district judge used a jury questionnaire. The judge made a special effort to ensure that using the questionnaire would not deprive the court of the benefits of oral voir dire.

**Toledo**
In a prosecution of Americans for conspiracy to fight against U.S. forces in Iraq, the judge used a jury questionnaire. Had he to do it over again, the judge would have given closer scrutiny to the questionnaire, which was prepared by the attorneys, because some of the questions proved to be confusing to the potential jurors.

**Atlanta**
For a trial on preparing for violent jihad by, among other things, making casing videos of strategic landmarks, the judge used a jury questionnaire. Prospective jurors filled out the questionnaire a week in advance of voir dire. This gave the lawyers and the court ample time to review the questionnaires to focus follow-up voir dire on the most important issues. The judge bifurcated the questionnaire so that prospective jurors filled out the first part, which focused on general background issues and matters that might affect a panel member’s service, before they filled out the second part, which focused on issues related to the nature of the trial, beliefs about Islam, and other case-specific matters.

**Sears Tower**
For the prosecution of the “Liberty City Seven” for conspiracy to topple the Sears Tower and attack other buildings in various cities, the judge did not use a jury questionnaire. The judge has never used one. She prefers face-to-face voir dire in three phases: first are questions directed to the whole panel, second are individual general qualification questions, and third are more sensitive case-specific individual questions.

**Fort Dix**
In a high-profile trial for conspiracy to attack Fort Dix, the judge used a jury questionnaire. For five days, approximately 150 prospective jurors reported to the courthouse each day to fill out the questionnaire in the jury room, where the judge greeted them. In the court-
room, the judge and the attorneys reviewed answered questionnaires. Approximately two-thirds of the prospective jurors were disqualified on the basis of the questionnaires alone.

**Other Cases**

Judges used jury questionnaires in the following cases as well:

- *Detroit*
- *Twentieth Hijacker*
- *Dirty Bomber*
- *Prosecution of a Charity*

**Sequestration**

If there is a substantial risk to jurors of danger or harassment arising from their service, then judges often arrange for the jurors to report to a secret remote location for transportation to the court by deputy marshals. This is sometimes referred to as partial sequestration, semi-sequestration, or soft sequestration. Full sequestration—secure overnight hotel accommodations for jurors—is sometimes used during the deliberation phase but seldom used before that.

Courts often provide semi-sequestered jurors with extra comforts, such as meals, refreshments, or even games and magazines to use during breaks. Sometimes courts require semi-sequestered jurors to eat lunch together and away from the public.

Judges are cautious about imposing any form of sequestration unnecessarily because of its additional expense, its possible prejudicial impact, and its inconvenience for the jurors.

**CASE NOTES**

*First World Trade Center Bombing*

Jurors reported to secret locations from which deputy marshals transported them to court, but jurors were not sequestered overnight. The judge sought to provide the jurors with extra comforts, such as meals and beverages.

*Plot to Bomb New York City Tunnels and Landmarks*

Jurors reported to secret locations from which deputy marshals transported them to court. Jurors were not sequestered overnight until it was time to deliberate, at which time the judge moved from a schedule of four days a week to seven days a week. The judge sought to provide the jurors with extra comforts, such as meals and beverages.

*Prosecution of a Guantánamo Bay Detainee for 1998 Embassy Bombings*

In preparation for the 2010 trial of Ahmed Khalfan Ghailani, a one-time fugitive, deputy marshals shuttled the jurors to and from the courthouse and provided them with breakfast, lunch, and refreshments.

*Detroit*

In the first post-September 11, 2001, prosecution for terrorism, the jurors assembled each morning at a secret location, and they were driven by van to the courthouse. Someone found out about the secret location and called the jury room with a death threat. The marshal changed the jurors' meeting location, used a different-color van to transport them, and beefed up security for the courtroom.

*Dirty Bomber*

In the Miami trial of three men—including Jose Padilla, who was originally detained as a dirty bomber but ultimately was tried for terrorism conspiracy—potential jurors were shielded from the public during jury selection by a screen in the courthouse lobby.

The jury was semi-sequestered. Jurors did not report directly to the courthouse; they reported to one of two specific secret locations—one on the north side of town and one on the south side—from which they were shuttled to the courthouse. Instead of going their own way for lunch, they always ate together. Once a week or so, the deputy mar-
shalls took them out for lunch. Restrooms on the courtroom’s floor were reserved for use by jurors and court staff only. Cubicle walls were used to screen off a rest area outside the jury room, a table and chairs were set up outside on a porch, and extra games and magazines were brought in.

**Prosecution of a Charity**

The prosecution of the Holy Land Foundation and its principals for providing funds to Hamas required two trials because of a hung jury after the first one. The judge presiding over the first trial had jurors meet in a secret location, and even the judge did not know where that was. They were shuttled to the courthouse, and they came to the courtroom floor in a secure elevator. They took lunch in the jury room. The judge presiding over the second trial chose not to use these special procedures so as not to communicate to the jurors that the case was unusual.

**Toledo**

In a prosecution of Americans for conspiracy to fight against U.S. forces in Iraq, jurors reported to an off-site location instead of to the courthouse. To minimize the prejudicial impact of this procedure, the judge told the jurors that meeting off-site was necessary because of insufficient courthouse parking, which to some extent was actually true.

**Sears Tower**

The prosecution of the “Liberty City Seven” for conspiracy to topple the Sears Tower and attack other buildings in various cities required three trials because of hung juries. In the first trial, an attorney working for one of the defendants gave a list of the jurors’ names to members of a defendant’s family, so the judge used an anonymous jury with partial sequestration in the second trial. Jurors met at undisclosed locations and were shuttled to the courthouse; the court provided them with lunch. For the third trial, however, the judge did not use sequestration, because it is a burden on the jurors and an additional operating expense. The judge monitored the situation, however, to see if sequestration would be warranted after all.

**Fort Dix**

In a high-profile trial for conspiracy to attack Fort Dix, the judge sequestered the jurors at a nearby hotel during deliberations.

**Other Cases**

Judges semi-sequestered jurors in the following cases as well:

- *First Prosecution for 1998 Embassy Bombings*
- *Millennium Bomber*

**News of National Security Events**

It will sometimes happen that during a trial related to a significant national security incident another significant national security incident will occur. It may be unreasonable to expect jurors to shield themselves from news of the second event, but judges are likely to caution them not to allow this news to prejudice the participation in the current trial.

**CASE NOTES**

**Plot to Bomb New York City Tunnels and Landmarks**

While defendants were being tried for a plot to bomb New York City tunnels and landmarks, related to the 1993 bombing of the World Trade Center, a bomb partially destroyed the federal building in Oklahoma City, including the courthouse there. The district judge permitted the New York jurors to consult news of the event, but admonished them not to let it influence them in the trial.
Special Evidence Issues

Witness Security

It is not uncommon in national security cases for the court to be asked to protect the identity of witnesses. Witnesses against the defendant may include informants who would be at risk if their identities were known; they may even be in the witness protection program. Witnesses may also include covert government agents, including foreign agents or security personnel. With respect to foreign government witnesses, protection of their identity may be a condition of the foreign government’s permitting them to testify.

Courts have permitted witnesses to testify under pseudonyms. Courts have also permitted witnesses to use special entrances to the courtroom, often those generally used for prisoners. “Light disguise” is sometimes permitted so long as the disguise does not obscure the witness’s demeanor or indicia of credibility. Judges sometimes forbid courtroom sketch artists from sketching the witness’s likeness.

Courts have sometimes shielded the witness’s face or voice altogether. Although the witness may not be shielded from litigants and court personnel, and from the jury if present at the proceeding, the witness may be shielded from the public either by screens or by use of an audiovisual feed to a second courtroom for the public. The witness’s image might be omitted from the video display, and the witness’s voice might be electronically altered.

Sometimes the testimony of foreign witnesses must be taken remotely by video deposition. This often includes defense representation both in court and at the foreign deposition location.

Judges are careful not to impose unwarranted or excessive protections.

CASE NOTES

First Prosecution for 1998 Embassy Bombings

An informant testified for the government in the trial for the 1998 bombings of American embassies in Kenya and Tanzania. In re Terrorist Bombings of U.S. Embassies in East Africa, 552 F.3d 93, 137–39, 141 (2d Cir. 2008); United States v. Bin Laden, 397 F. Supp. 2d 465, 474 (S.D.N.Y. 2005). Prior to his testimony, he was identified, even to defense counsel, only as CS-1, which stood for “confidential source one.” In 1996, he separated from Al-Qaeda after embezzling money from one of Osama bin Laden’s companies. At an American embassy in Africa, he offered to help fight Al-Qaeda. The U.S. government kept him protected at an undisclosed location after he pleaded guilty in 1997 to a conspiracy charge in a sealed proceeding. In re Terrorist Bombings, 552 F.3d at 142; Bin Laden, 397 F. Supp. 2d at 474. The informant’s identity was not revealed to defense counsel until four days before his scheduled testimony, and a protective order forbade counsel from revealing the informant’s identity to the defendants until the day before the informant appeared in court. The district judge forbade courtroom artists from sketching the informant’s face.

Prosecution of a Guantánamo Bay Detainee for 1998 Embassy Bombings

In the 2010 trial of onetime fugitive Ahmed Khalfan Ghailani, the judge prohibited a courtroom artist from sketching a witness’s face. The witness did not testify at trial, because the judge found that his identity was discovered as a result of extremely harsh interrogation of the defendant. The witness testified at a suppression hearing, however, at a time when the witness’s identity was a secret. Because the witness’s identity was revealed at the hearing,
the judge unredacted his name from court documents.

**Millennium Bomber**

In the prosecution of Ahmed Ressam, who planned to bomb the Los Angeles International Airport at the turn of the millennium, one of the witnesses against the defendant was Abdelgani Mesinki, an accomplice who had pleaded guilty in another jurisdiction. He entered the witness protection program because of his testimony. He used a side door to enter the courtroom.

The district judge overruled the government’s attempts to protect the identity of another potential witness, such as by taking testimony remotely or behind a screen and withholding background information, and the government decided not to use the witness.

**American Taliban**

In the prosecution of John Walker Lindh, who became known as the American Taliban, the defendant pleaded guilty on a day the court was prepared to take testimony from a covert agent on a motion to suppress the defendant’s confession. To protect the witness’s identity, the district judge worked with the classified information security officers and the U.S. Marshals Service to make adjustments to the courtroom. The courtroom was outfitted with special draperies and screens. The witness box was shielded from the public, as was the path to the door through which prisoners often are brought—a door that would be used in this case for the witness.

The plan was for the defendant and his counsel to sit in the jury box so that they could see the witness, but the draperies shielded the witness from the public’s view. *United States v. Rosen*, 520 F. Supp. 2d 786, 795 n.15 (E.D. Va. 2007). The courtroom was equipped with an electronic device that would distort the witness’s voice, but the words would be understandable to the parties and the public.

**September 11 Damages**

In a civil action against alleged supporters of the September 11, 2001, attacks, some plaintiffs introduced as evidence supporting a default judgment against Iran videotaped testimony from Iranian government defectors. To protect the safety of the witnesses and their families, the court allowed the plaintiffs to file both a public brief and a sealed supplemental brief, with the defectors’ testimony as sealed exhibits.

**Dirty Bomber**

In the trial of Jose Padilla, originally detained as a dirty bomber but ultimately tried with two other men for terrorism conspiracy, special security measures were used for a witness who found an incriminating document in Afghanistan. The witness used a special entrance to enter and exit the courtroom, and he reached the floor of the courtroom from the basement in the prisoner elevator. The witness testified under pseudonym and in light disguise: black-rimmed glasses and a closely cropped beard. Sketch artists were prohibited from sketching him, and questioning could not breach CIA personnel and location secrets.

**A Plot to Kill President Bush**

Ahmed Omar Abu Ali, an American citizen educated at the University of Medina in Saudi Arabia, was convicted of terrorism conspiracy and conspiracy to kill the President. *United States v. Abu Ali*, 528 F.3d 210, 221, 226 (4th Cir. 2008). He was originally arrested in Saudi Arabia by the counterterrorism Mabahith on another matter: an investigation of a 2003 bombing in Riyadh. *Id.* at 223–24, 238; *United States v. Abu Ali*, 395 F. Supp. 2d 338, 341, 344, 367, 384 (E.D. Va. 2005). Mabahith questioning resulted in a confession to facts supporting the American indictment. Because the identities of Mabahith officers are secret, the Saudi government would not permit them to come to the United States to testify. They testified pseudonymously by video deposition conducted in Saudi Arabia. When portions of the depositions were played in court, only the judge, the parties, and the jury could see the audio portion, but the public could hear the audio portion.

**Prosecution of a Charity**

The prosecution of the Holy Land Foundation and its principals for providing funds to Hamas required two trials because of a hung jury after the first one. At both trials, two witnesses testified under cover. Methods of protecting the witnesses’ security were established by the judge who presided over the first trial.

Both witnesses testified under pseudonyms, and their identities were not disclosed.
to defense counsel. One witness was a lawyer in the counterterrorism section of the Israel Security Agency (ISA), also known as Shin Bet, who was to testify as an expert on Hamas financing. Israeli law prohibits the disclosure of ISA agents’ identities. The other witness worked for the Israeli Defense Forces, which looks to ISA rules for the protection of its personnel.

The courtroom was closed to the public and the news media during these witnesses’ testimony, but the defendants and their immediate family members were permitted to attend. The witnesses entered and exited the courtroom through a non-public door. The public and the news media could listen to an audio feed in another courtroom. In response to any question under cross-examination that called on them to reveal classified information, the witnesses were permitted to consult counsel.

Chicago
In the prosecution of Muhammad Abdul Hamid Khalil Salah for helping to provide funds to Hamas, Salah sought testimony from two Israel Security Agency (ISA) agents to prove that his confession in Israel was obtained by torture and coercion. *United States v. Abu Marzook*, 412 F. Supp. 2d 913, 916 (N.D. Ill. 2006). It was unprecedented for such officers to provide testimony outside of Israel.

The identities of ISA agents are kept secret by Israel. The judge agreed to close the hearing on Salah’s motion to suppress his confession while the ISA agents testified. *United States v. Marzook*, 435 F. Supp. 2d 708, 714 (N.D. Ill. 2006); *Abu Marzook*, 412 F. Supp. 2d 913. The government of Israel waived its secret classification of the agents’ testimony as to defense attorneys and Salah. All other persons in court during the testimony had security clearances.

To protect the agents’ identities, they were permitted to use private entrances to the courthouse and the courtroom. The agents and their Israeli attorneys were identified in court documents by code names. But the judge denied a request that they testify in “light disguise,” because Salah had already seen them, the public would not see them, and the government had presented no evidence of security concerns respecting the attorneys and court staff who would see them.

The hearing, which was conducted intermittently over the course of several weeks, was open for the testimony of other witnesses, including Israeli police officers.

For the trial, the judge again permitted the ISA agents to testify using pseudonyms in a closed courtroom. Again the judge permitted the witnesses to use private entrances. She permitted the defendants’ immediate family members to remain in the courtroom during the agents’ testimony. Because of the presence of the family members and the jury, the judge agreed to let the agents testify in light disguise, so long as the disguises did not interfere with the jurors’ ability to judge the witnesses’ credibility. But the agents ultimately decided to testify without disguise, because of the limitations on who would be in the courtroom to see them. The judge decided that the rest of the trial would be public.

The closed portion of the trial was kept as open as possible. The court established a live video and audio feed to another courtroom where spectators could listen to the closed session and see those in the courtroom, except for the witnesses. To disguise from the jury that the courtroom was closed, the jurors were told that the camera was a precaution in case of an overflow crowd, and the witnesses used the private entrance before the jury was brought in.

Toledo
A prosecution of Americans for conspiracy to fight against U.S. forces in Iraq was based, in part, on evidence from a government informant, called “the Trainer” in the indictment, who was hired to see who in the Toledo-area Muslim community would respond positively to professed approval of overseas jihad. The identity of the witness was initially a secret, but newspapers revealed his name, so the judge issued an order forbidding public dissemination of his image or identity.

Foreign Evidence
Foreign witnesses are beyond the court’s subpoena power. The witnesses may consent to travel to the United States to offer testimony, which may require per-
mission from their government if they are government officers. A condition of this travel may be security measures to protect the witness’s identity.

Testimony might also be taken remotely by video deposition. Typically the witness is abroad and the defendant is local and an audiovisual link is established to provide for adequate confrontation. Lawyers for each side are typically at both locations, and a communication link is established so that the defendant can confer with defense counsel at both locations. The judge might be either at the home court or at the foreign location.

CASE NOTES

Millennium Bomber
In the prosecution of Ahmed Ressam, who planned to bomb the Los Angeles International Airport at the turn of the millennium, the government sought testimony of witnesses in Canada, beyond the court’s subpoena power, who were unwilling to travel to the United States to offer testimony. By stipulation of the parties, the judge traveled to Canada to preside over video depositions in both Montreal and Vancouver to obtain the testimony. A Canadian court official attended to rule on potential issues of Canadian law. Ressam participated by videoconference from his jail cell with the assistance of an Arabic interpreter.

On one occasion, after the American judge had traveled to Canada for the deposition, a Canadian judge ruled, at a proceeding from which the American judge was excluded, that the witness did not have to testify.

Some of the witnesses subsequently indicated that they might be willing to testify live at Ressam’s trial, but the parties agreed that either side could substitute deposition videotapes.

The federal defender’s office represented Ressam, and the office agreed to accept service on his behalf of three seizure notices from the Royal Canadian Mounted Police. Two attorneys and an investigator traveled to Montreal to investigate the seizures, and they obtained from the Canadian court copies of documents in the related files. Apparently, the documents were disclosed to the attorneys in error and were taken back at the Montreal airport. The U.S. prosecution moved for an order prohibiting the attorneys from discussing the documents with their client. The district judge told the attorneys that they could only use the information they obtained from the Canadian files as a last resort, and they could not dis-close to their client the origin of the information.

Guantánamo Bay
Guantánamo Bay detainees who wished to testify at their habeas hearings had to do so by secure video link, because the government was unwilling to transport them to court. A habeas attorney and an interpreter, if necessary, were in Guantánamo Bay. Another habeas attorney was in the courtroom with the judge and the government’s attorney, possibly with additional interpreters.

A Plot to Kill President Bush
Ahmed Omar Abu Ali, an American citizen convicted of terrorism conspiracy and conspiracy to kill the President, was originally arrested in Saudi Arabia by the counterterrorism Mabahith in an investigation of a 2003 bombing in Riyadh. United States v. Abu Ali, 528 F.3d 210, 221, 223–24, 226, 238 (4th Cir. 2008); United States v. Abu Ali, 395 F. Supp. 2d 338, 341, 344, 367, 384 (E.D. Va. 2005). Because the identities of Mabahith officers are secret, the Saudi government would not permit them to come to the United States to testify. Instead, they testified pseudonymously by video deposition conducted in Saudi Arabia. The district judge sent to Saudi Arabia two prosecutors, two defense attorneys, a camera operator, and an interpreter. (If the judge had it to do over again, he would have sent at least one relief interpreter.) A live video feed was established between Saudi Arabia and the U.S. courtroom, in which were the judge, additional counsel for both sides, and the court reporter. The video image was constructed as a split screen with the defendant on one side and the witness on the other, so that the defendant could see the witness and the witness could see the defendant. The defendant could com-
municate with his attorneys in Saudi Arabia via cell phone during breaks or on request.

Challenges posed by this remote video de
donishment included the time-zone difference, the unreliable availability of a secure connection, and Saudi Arabian heat that sometimes caused technical difficulties.

**Prosecution of a Charity**

In the prosecution of the Holy Land Foundation and its principals for providing funds to Hamas, two Israeli witnesses testified under cover: one witness was a lawyer in the counterterrorism section of Shin Bet, the Israel Security Agency; the other witness worked for the Israeli Defense Forces.

**Chicago**

In the prosecution of Muhammad Abdul Hamid Khalil Salah for helping to provide funds to Hamas, Salah sought testimony from two Israel Security Agency (ISA) agents to prove that his confession in Israel was obtained by torture and coercion. *United States v. Abu Marzook*, 412 F. Supp. 2d 913, 916 (N.D. Ill. 2006). It was unprecedented for such officers to provide testimony outside of Israel. Israel permitted the witnesses to travel to the United States to provide testimony, and the court applied security measures to protect the secrecy of their identities.

Salah also sought to discover Israeli police documents to support his claim that his confession while in custody in Israel was obtained by torture and coercion. The judge suggested that he follow rogatory-letter procedures, but Salah ultimately relied on testimony from Israeli police officers.

**Examination of High-Security Detainees**

Sometimes national security defendants seek testimony from persons who are in custody for national security reasons. The government is frequently reluctant to permit examination of such detainees, but some examination may be necessary to afford the defendant an adequate defense. Solutions to these competing interests have sometimes involved not direct examination but examination through interrogators.

**CASE NOTES**

**American Taliban**

In the prosecution of John Walker Lindh, who became known as the American Taliban, defense counsel wanted to interview persons detained at Guantánamo Bay. The district judge denied face-to-face access to the detainees, but the judge established a procedure allowing counsel to submit questions to “firewall” government attorneys who passed them on to the detainees.

Firewall attorneys included attorneys from the Department of Justice and the Department of Defense “who are separate and independent from the attorneys who represent the government” in the case, including two assistant U.S. attorneys from another district.

Defense counsel submitted questions for each detainee to the firewall attorneys. The firewall attorneys could object to any questions, and the court would resolve any objections on sealed noticed filings. Approved questions were submitted to interrogators who interwove the questions into the interrogations. Firewall attorneys prepared written summaries, and defense counsel could submit follow-up questions. Soon thereafter, the firewall attorneys submitted to defense counsel video recordings of the interviews.

The judge monitored the procedure to ensure that it protected Lindh’s rights to a defense.

**Senior Government Officers**

In national security cases, attorneys sometimes seek evidence from national security policy makers. Judges are cautious about allowing these cases to interfere
with the important work of senior government officers. Judges will allow such interference, however, if justice so requires.

CASE NOTES

First Prosecution for 1998 Embassy Bombings

In the prosecution for the 1998 bombing of American embassies in Kenya and Tanzania, Mohamed Rashid Daoud al-'Owhali’s attorneys decided that testimony from Secretary of State Madeleine Albright about the impact of U.S. sanctions on Iraqi citizens might be helpful during the penalty phase of the trial. The district judge initially agreed to sign the subpoena, but on the government’s motion he quashed it. Al-'Owhali presented at trial as a substitute for her live testimony a 60 Minutes interview with Secretary Albright. Al-'Owhali also presented similar evidence through a willing witness, former Attorney General Ramsey Clark.

Guantanamo Bay

To resolve a motion to enjoin a Guantánamo Bay detainee’s transfer to Algeria, where he feared he would be tortured or killed, the district court ordered testimony from the special envoy for the closure of the Guantánamo Bay detention facility, who had the rank of ambassador, because the court determined that the ambassador’s declaration opposing the motion lacked specificity. The government refused to provide the testimony, the district court enjoined the transfer, and the court of appeals dissolved the injunction.

Giving State Secrets to Lobbyists

In a sting prosecution of lobbyists for sharing classified information, the defendants requested subpoenas for 20 current and former high-ranking government officials, including Secretary of State Condoleezza Rice, because of her former position as National Security Advisor. United States v. Rosen, 520 F. Supp. 2d 802, 804, 806–07 (E.D. Va. 2007). The judge sustained the government’s objection as to five witnesses, but overruled its objection as to the following: Secretary Rice; current National Security Advisor Stephen Hadley, who was her deputy; Paul Wolfowitz and Richard Armitage, each formerly Deputy Secretary of State; and seven others. Recognizing that the requested testimony would be more credible and probative than alternatives, the judge observed that “nothing in the Sixth Amendment right to compulsory process requires, nor should it require, an accused to refrain from calling government officials as witnesses until he has exhausted possible nongovernmental witnesses to prove a fact.” Id. at 811.

Pro Se Issues

A defendant’s exercising his or her right to pro se representation is usually a substantial complication.

The first line of defense against this complication is prevention. Judges will sometimes remedy bad fits between appointed counsel and defendants.
A defendant in a national security case may wish to use court proceedings to make a public statement. Judges often set limits with defendants so that they do not have both all the benefits of appointed counsel and opportunities to use court proceedings for personal proclamations. Such limits are usually set delicately. For example, a defendant who wishes to personally make an opening statement may be required to proceed through the trial pro se as a consequence.

Courts frequently appoint standby counsel for pro se defendants, even against the defendants' wishes. Courts may withdraw the pro se privilege if it is abused or if the defendant's exercise of the privilege becomes too disruptive.

If classified information is at issue in the case, the court may have to appoint counsel to handle classified issues, because the government may choose not to give the defendant access to classified information.

CASE NOTES

First World Trade Center Bombing
The four defendants convicted in 1994 of bombing the World Trade Center in 1993 dismissed their attorneys after they were convicted by the jury. United States v. Salameh, 856 F. Supp. 781, 782 (S.D.N.Y. 1994). They appeared at sentencing pro se. United States v. Salameh, 152 F.3d 88, 161 (1998). In 1998, the court of appeals vacated their sentences because the record did not reflect a knowing, intelligent, and voluntary waiver of their rights to counsel. In 1999, the defendants were resentenced, and those sentences were affirmed in 2001. United States v. Salameh, 261 F.3d 271 (2d Cir. 2001).

Plot to Bomb U.S. Airplanes in Southeast Asia
Ramzi Ahmed Yousef was a defendant in the prosecution for the 1993 bombing of the World Trade Center, but at the time of the 1993–1994 trial, Yousef was a fugitive. Salameh, 152 F.3d at 108. In 1995, because of an accidental home fire, he was discovered mixing bomb chemicals in Manila, Philippines, and this discovery led to a prosecution for a plot to blow up American air carriers' planes in southeast Asian routes. United States v. Yousef, 327 F.3d 56, 79–81 (2d Cir. 2003). Yousef initially eluded arrest, but he was apprehended the following month in Islamabad, Pakistan. At his trial for the Asian bomb plot, he asked to address the jury during opening arguments. The district judge said that if he did that, he would have to represent himself throughout the trial, and Yousef agreed to do that. He was convicted. At his later trial for the World Trade Center bombing, he allowed a lawyer to represent him. He was convicted again.

Twentieth Hijacker
At a hearing on conditions of confinement, four months after his indictment, Zacarias Moussaoui announced that he would like to represent himself, possibly with the assistance of a Muslim attorney, because his assigned attorneys did not understand Muslims. United States v. Moussaoui, 591 F.3d 263, 269–70 (4th Cir. 2010); United States v. Moussaoui, 333 F.3d 509, 512–13 (4th Cir. 2003).

A court-appointed psychiatrist determined that Moussaoui was a fanatic, but not mentally incompetent to stand trial or waive his right to counsel. The judge granted Moussaoui's motion to represent himself, keeping appointed counsel as standbys.

Nineteen months later, the judge revoked Moussaoui's right to proceed pro se, because of frequent inappropriate filings.

Once he began to proceed pro se, Moussaoui began to file with the court handwritten documents that the court regarded as motions. The district judge observed, "The defendant's pleadings have been replete with irrelevant, inflammatory and insulting rhetoric, which would not be tolerated from an attorney practicing in this court." Pro Se Filings Sealing Order at 3, United States v. Moussaoui, No. 1:01-cr-455 (E.D. Va. Aug. 29, 2002), available at 2002 WL 1990908. The government also became concerned that the filings might include coded messages to confederates. One remedy was to seal Moussaoui's filings, but
the news media were vigilant in advocating for a minimum of sealing. In general, the filings were initially sealed and then unsealed or redacted after a review by the government and the court.

Atlanta
Two young men were prosecuted in Atlanta for preparing for violent jihad by, among other things, making casing videos of strategic landmarks. As trial approached, each of the defendants expressed an interest in representing himself. The government decided to try the two defendants separately. Syed Haris Ahmed opted for a bench trial, but accepted representation by counsel. Ehsanul Islam Sadequee announced on the first day of jury selection that he would represent himself. The judge appointed his attorneys as standby counsel. Sadequee cross-examined the government’s witnesses but did not call any witnesses himself. For his defense, he offered only his own testimony and closing argument. Both defendants were convicted.
KEYNOTE ADDRESS:

THE HONORABLE SUZANNE E. SPAULDING
UNDER SECRETARY
NATIONAL PROTECTION AND PROGRAMS DIRECTORATE
U.S. DEPARTMENT OF HOMELAND SECURITY
Statement for the Record

The Honorable Suzanne E. Spaulding
Under Secretary, National Protection and Programs Directorate

and

The Honorable Francis X. Taylor
Under Secretary, Office of Intelligence and Analysis
U.S. Department of Homeland Security

Before the
U.S Senate Committee on Homeland Security and Governmental Affairs

Regarding

Cybersecurity, Terrorism and Beyond:
Addressing Evolving Threats to the Homeland

September 10, 2014
Introduction

Chairman Carper, Ranking Member Coburn and distinguished members of the committee, thank you for the opportunity to appear before you today to discuss terrorist, cyber and other human-caused threats to the Homeland and the current threat environment on the eve of the anniversary of the September 11, 2001 attacks.

Thirteen years later, we continue to face a dynamic threat environment. Threats to the Homeland are not limited to any one individual, group or ideology and are not defined or contained by borders. They display the increasing determination of individuals to carry out acts of terrorism that have potential to negatively impact the Homeland through loss of life, destruction of critical infrastructure, disruption of technological capabilities or services, or compromise of information security.

In the testimony today, we will highlight some of the threats we face and the risk-informed actions we take that assist government at all levels and owners and operators of critical infrastructure to understand evolving threats, share information on these threats and hazards, and promote best practices, training, and tools in the four priority areas outlined by Secretary Johnson: (1) aviation security, (2) border security, (3) countering violent extremism, and (4) cybersecurity.

Challenges Ahead

It is important to mention a couple items to provide some strategic context before covering specifics. First, the cornerstone of our mission at DHS has always been, and should continue to be, counterterrorism – that is, protecting the nation against terrorist attacks. We must remain vigilant in detecting and preventing terrorist threats that may seek to penetrate the homeland from the land, sea or air. From a security perspective, many of the resources we expend and activities we conduct apply to both countering terrorism, as well as countering transnational criminal organizations, and other homeland security challenges.

Second, to address the range of challenges the nation faces most collaboratively and effectively within the Department, we have recently undertaken an initiative entitled “Strengthening Departmental Unity of Effort.” In his April 22, 2014 memorandum, Secretary Johnson directed a series of actions to enhance the cohesiveness of the Department, while preserving the professionalism, skill, and dedication of the people within, and the rich history of, the DHS components.

The actions in this initiative: new senior leader forums led by Secretary and the Deputy, and cross-departmental strategy, requirements, and budget development and acquisition processes that are tied to strategic guidance and informed by joint operational plans and joint operations are building and maturing DHS into one that is greater than the sum of its parts – one that operates
much more collaboratively, leverages shared strengths, realizes shared efficiencies, and allows us to further improve our important role as an effective domestic and international partner.

**Terrorism and Aviation Security**

Core Al Qa’ida, Al-Qa’ida in the Arabian Peninsula (AQAP), and their affiliates remain a major concern for DHS. Despite senior leadership deaths, the group maintains the intent and capability to conduct attacks against U.S. citizens and our facilities, and has demonstrated an ability to adjust its tactics, techniques and procedures for targeting the West in innovative ways. AQAP’s three attempted attacks against the U.S. homeland—the airliner plot of December 2009, an attempted attack against U.S.-bound cargo planes in October 2010, and an airliner plot in May 2012—demonstrate their efforts to adapt to security procedures. Over the past several weeks DHS has taken a number of steps to enhance aviation security at overseas airports with direct flights to the United States, and other nations have followed with similar enhancements.

The Islamic State of Iraq and the Levant (ISIL) is a terrorist group operating as if it were a military organization, attempting to govern territory, and their experience and successes on the battlefields of Iraq and Syria have armed them with capabilities most terrorist groups do not possess. The group aspires to overthrow governments in the region and eventually beyond. At present, DHS is unaware of any specific, credible threat to the U.S. Homeland from ISIL. However, violent extremists who support them have demonstrated the intent and capability to target American citizens overseas, and ISIL constitutes an active and serious threat within the region and could attempt attacks on U.S. targets overseas with little-to-no warning. Attacks could also be conducted by supporters acting independently of ISIL direction with little-to-no warning. In January, ISIL’s leader publically threatened “direct confrontation” with the United States, which is consistent with the group’s media releases during the past several years that have alluded to attacking the United States.

ISIL exhibits a very sophisticated propaganda capability, disseminating high-quality media content on multiple online platforms, including social media, to enhance its appeal. ISIL’s English-language messaging and its online supporters have employed—and will almost certainly continue—Twitter “hashtag” campaigns that have gained mainstream media attention and have been able to quickly reach a global audience and encourage acts of violence. Media accounts of the conflict, and propaganda in particular, play a role in inspiring U.S. citizens to travel to Syria. We are aware of a number of U.S. persons who have attempted travel to Syria this year, which underscores their continued interest in partaking in the conflict. More than 100 U.S. persons and over two thousand Westerners have traveled or attempted travel to Syria to participate in the conflict—with some of them seeking to fight with or otherwise support violent extremist groups.

We remain concerned about the threat of U.S. foreign fighters and supporters returning from Syria and whether they would to conduct attacks either on their own initiative or at the direction
of terrorist groups abroad. In addition, a small number of U.S. persons have died while fighting in Syria—including the first suicide bombing by an identified U.S. person in Syria in May and at least one other recently killed while fighting alongside ISIL. These foreign fighters, many in possession of Western passports, have likely become further radicalized while receiving additional training and experience, and pose a potential threat upon their return to their home countries.

The DHS Office of Intelligence and Analysis (I&A) is working closely with interagency partners to evaluate threat data and ensure relevant information reaches DHS personnel and state, local, tribal and territorial (SLTT) partners who can use this information to reduce risks to the Homeland. For example, I&A, the Federal Bureau of Investigation (FBI), and the National Counterterrorism Center, produced a poster, handout and muster language for DHS screeners to have background about the conflict in Syria. To ensure our SLTT and private sector partners are kept informed of the current ISIL threat, I&A has hosted multiple calls with our partners in recent months to examine the ongoing situation and, jointly with the FBI, released Joint Intelligence Bulletins (JIB) that provided context and background, examined the potential retaliatory threat and ISIL’s use of social media to publicize the group’s actions and goals. Following the 9/11 attacks, the importance of an informed community of first responders became clear. I&A places priority on ensuring that the Nation’s first responders have the information that they need to identify the trends, tactics and behaviors of a terrorist. It also takes a vigilant public; the Department is dedicated to reminding Americans that “If You See Something, Say Something.”

**Border Security**

Border security must include an intelligence-driven, risk-based approach that focuses resources on the places where our surveillance and intelligence tells us the threats to border security exist, and prepares us to move when the threat moves. The collaborative intelligence work of I&A, the U.S. Coast Guard, the U.S. Customs and Border Protection and the U.S. Immigration and Customs Enforcement helps keep our Southern and Northern borders safe each and every day. We ensure that the officers that are protecting the border points of entry are informed of the necessary intelligence to tailor their operations to the risks poised from overseas.

One of Secretary Johnson’s earliest Departmental initiatives was directing development of a Southern Border and Approaches Campaign Planning effort that is putting together a strategic framework to further enhance the security of our southern border. The Plan will contain specific outcomes and quantifiable targets for border security and will address improved information sharing, continued enhancement and integration of sensors, and unified command and control structures as appropriate. The overall planning effort will also include a subset of campaign plans focused on addressing challenges within specific geographic areas, all with the goal of enhancing
our border security. I&A is participating in this effort to ensure threat information drives
efficient use of border resources and likewise, that our border analytic focus meets the
operational needs of the Department.

**Countering Violent Extremism**

The individualized nature of the radicalization process for homegrown violent extremists (HVEs)
makes it is difficult to predict the triggers that will contribute to them attempting acts of
violence. Since the Boston Marathon bombings, the Department has evolved to address the need
to counter violent extremism (CVE) from an interagency perspective. Mindful of the potential
for homegrown violent extremism inspired by radical ideology overseas, we continue to take
steps to counter that potential threat, both through law enforcement and community outreach.
Beyond the intelligence and information sharing with SLTTs and the private sector, the
Department is also committed to training, through the Federal Law Enforcement Training
Center, the Federal Emergency Management Agency, the National Protection and Preparedness
(NPPD) Office of Infrastructure Protection and I&A. We have a commitment to training to
prevent and respond to domestic attacks. Lessons learned from the Boston Marathon bombing
highlighted the value in prevention and incident training.

**Cybersecurity**

Growing cyber threats are an increasing risk to critical infrastructure, our economy and thus, our
national security. As a nation, we are faced with pervasive threats from malicious cyber actors.
They are motivated by a range of reasons that include espionage, political and ideological
beliefs, and financial gain. Certain nation-states pose a significant cyber threat as they
aggressively target and seek access to public and private sector computer networks with the goal
of stealing and exploiting massive quantities of data.

Some nation-states consistently target Government-related networks for traditional espionage,
thief of protected information for financial gain, and other purposes. Increasingly, SLTT
networks are experiencing nation-state cyber activity similar to that seen on federal networks. In
addition to targeting government networks, there is a growing threat of nation-states targeting
and compromising critical infrastructure networks and systems. Such attacks may compromise
the infrastructure or control system network and provide persistent access for potential malicious
cyber operations which could lead to cascading effects with physical implications.

DHS takes a customer-focused approach to information sharing, in which our desired outcome is
to help prevent damaging cybersecurity incidents, such as the theft of personal information or
physical disruption of critical infrastructure, and utilizes information in an operational
environment to directly reduce cybersecurity risk. DHS uses information to detect and block cybersecurity attacks on federal civilian agencies and shares information to help critical infrastructure entities in their own protection; to provide information to commercial cybersecurity companies so they can better protect their customers; and to maintain a trusted information sharing environment for private sector partners to share information and collaborate on cybersecurity threats and trends. This trust derives in large part from our emphasis on privacy, confidentiality, civil rights, and civil liberties across all information sharing programs, including special care to safeguard personally identifiable information. DHS law enforcement agencies also make substantial contributions to these cyber information sharing efforts.

I&A and NPPD work closely together every day to recognize and reduce risks posed by cyber threats. DHS' National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 operational organization that responds to, and coordinates the national response to, significant cyber incidents. NCCIC is the centralized location where federal departments and agencies, SLTT partners, private sector and international entities all form an operational nexus from which to respond. This centralized location generates collaboration and knowledge dissemination among stakeholders to provide a much greater understanding of cybersecurity vulnerabilities, intrusions, incidents, mitigation, and recovery actions.

Supporting the operational cyber mission of NPPD, I&A provides all-source analysis of cyber threats to the '.gov' domain, state and local networks, and critical infrastructure networks and systems to assist owners and operators in protecting their cyber infrastructure. I&A's cyber intelligence products and briefings are tailored to classification levels appropriate for our customers, and include For Official Use Only- and classified-level products and briefings specifically for the state and local audience.

The NCCIC actively collaborates with public and private sector partners every day, including responding to and mitigating the impacts of attempted disruptions to the Nation's critical cyber and communications networks. So far this Fiscal Year, the NCCIC has processed over 612,000 cyber incidents, issued more than 10,000 actionable cyber alerts that were used by recipients to protect their systems, detected more than 55,000 vulnerabilities through scans and assessments, and deployed 78 onsite teams for technical assistance. In one recent example, the United States Secret Service (USSS) shared information on malware observed in recent Point-of-Sale intrusions with the NCCIC for analysis. In partnership with the Financial Services Information Sharing and Analysis Center, the results of this analysis were published and enabled U.S. businesses to identify and stop ongoing cyber intrusions, thereby protecting customer data and mitigating losses.
Cybersecurity Information Sharing

While many sophisticated companies currently share cybersecurity information under existing laws, there is a continued need to increase the volume and speed of cyber threat information sharing between the government and the private sector — and among private sector entities — without sacrificing the trust of the American people or individual privacy, confidentiality, or civil liberties.

The Administration continues to take steps through executive action and public-private initiatives that incentivize and enable information sharing under existing laws. For example, Executive Order 13636 issued by President Obama in February 2013 directed intelligence agencies to increase the speed and quantity of declassified cyber threat information that the government shares with the private sector. Moreover, in February 2014, the Department of Justice and Federal Trade Commission, the two agencies charged with enforcing our antitrust laws, issued guidance that they do not believe “that antitrust is — or should be — a roadblock to legitimate cybersecurity information sharing.”

While progress continues under existing law, the Administration has consistently stated that carefully updating laws to facilitate cybersecurity information sharing is one of several legislative changes essential to improve the Nation's cybersecurity. Accordingly, the Administration continues to emphasize three fundamental priorities for information sharing legislation:

1. Carefully safeguard privacy, confidentiality, and civil liberties;
2. Preserve the long-standing, respective roles and missions of civilian and intelligence agencies. Newly authorized cyber threat information sharing should enter the government through a civilian agency; and,
3. Provide for appropriate sharing with targeted liability protection.

DHS Cybersecurity Authorities

Information sharing is only one element of what is needed. We also need to update laws guiding Federal agency network security; give law enforcement the tools needed to fight crime in the digital age; create a National Data Breach Reporting requirement; and promote the adoption of cybersecurity best practices within critical infrastructure.

We urge Congress to continue efforts to modernize the Federal Information Security Management Act to reflect the existing DHS role in agencies’ Federal network information security policies; clarify existing operational responsibilities for DHS in cybersecurity by authorizing the NCCIC; and provide DHS with hiring and other workforce authorities.
These provisions are vital to ensuring the Department has the tools it needs to carry out its mission.

**Strengthening the Security and Resilience of Critical Infrastructure**

Because the majority of the Nation’s infrastructure is owned and operated by the private sector, DHS works with owners and operators, primarily on a voluntary basis, to understand evolving threats, share information on these threats and hazards, and promote best practices, training, and tools to help mitigate risks. By leveraging its core capabilities, such as information and data sharing, capacity development, vulnerability assessments, and situational awareness, DHS is effectively using its skills and resources to assist with building the Nation’s resilience to physical and cybersecurity risks.

DHS works to ensure relevant information on current threats is disseminated as widely and appropriately as possible. Information sharing efforts leverage the existing partnership framework, allowing DHS to discuss threats, protective measures and joint industry/government initiatives with the private sector in order to reduce risk. For instance, DHS and FBI have engaged more than 400 major malls across the United States to facilitate 56 tabletop exercises based on a Westgate Mall, Nairobi-style attack involving coordinated active shooters and use of improvised explosive devices, and requiring a sustained response and deployment of federal resources. In addition, DHS and the Department of Energy, through the Sector Coordinating Council and in collaboration with other interagency partners, provide classified and unclassified threat briefings to CEOs and industry executives on physical and cyber threats. This frequent information sharing allows DHS and DOE to communicate specific threats to the electric sub-sector owners and operators.

The National Infrastructure Coordinating Center (NICC) maintains 24/7 situational awareness and crisis monitoring of critical infrastructure and shares threat information in order reduce risk, prevent damage, and enable rapid recovery. The NICC makes relevant information available to all critical infrastructure owners and operators through the Homeland Security Information Network, DHS’s web-based information sharing platform, bringing together homeland security partners across the spectrum. Finally, the Private Sector Security Clearance Program provides a key support capability to these information sharing efforts, facilitating DHS-sponsored security clearances for critical private sector representatives across the country. This critical ability to share information at the classified level promotes a two-way exchange between the Intelligence and infrastructure protection communities that can directly lead to posturing and protection measures to mitigate risk.
**Conclusion**

Whether securing the Homeland from aviation threats, border threats, homegrown violent extremists, or cyber threats, DHS has matured over its tenure to recognize that it takes the intelligence, planning, training and operations of our combined components to be effective against all nefarious actors. It is through the great work and collaboration of the DHS Counterterrorism Advisory Board (CTAB) that intelligence and mitigation strategies are synthesized across the Department. The CTAB brings together the intelligence, operational and policy-making elements from across DHS to facilitate a cohesive and coordinated operational response so that DHS can deter and disrupt terrorist operations.

While many of the threats I have highlighted for you today may be emerging and evolving, the Department of Homeland Security has been poised to deal with them and remains ready to respond. Our established relationships and information sharing practices enhance our indications and warning. We continue to work closely with our partners – both here at home, as well as our international partners – to aggressively thwart plans and activities that pose a threat to the homeland. Dealing with evolving risk in a changing world is core to the DHS mission, and is carried out by an outstanding team of professionals across the globe each and every day. We will continue to evaluate and adopt serious and prudent homeland security measures as situations warrant.

Chairman Carper, Ranking Member Coburn and distinguished members of the Committee, thank you for this opportunity to testify about threats to the Homeland. We look forward to answering your questions.
Homeland Security Law Institute looks at challenges facing the U.S.

Creating safe and resilient communities where the American way of life can thrive is the core objective of National Protection and Programs Directorate and the Department of Homeland Security, according to NPPD Undersecretary Suzanne Spaulding. Spaulding shared that overview at the opening session of the 9th Annual Homeland Security Law Institute, sponsored by the American Bar Association Section of Administrative Law and Regulatory Practice, held Aug. 21-22 in Washington, D.C.

Spaulding began by thanking former and current DHS officials for their continued help addressing challenges we face as a nation. Spaulding said that she and DHS Secretary Jeh Johnson are "recovering" attorneys, and are well aware and deeply appreciative of the rule of law and the role of lawyers in addressing the challenges that we, as a nation, face.

Spaulding discussed three key elements of how she views the mission of the DHS, and specifically the NPPD.

1. The overarching mission to strengthen the security and resilience of the nation's critical infrastructure is accomplished by looking closely at threats, vulnerabilities, consequences and mitigation.

2. Advances in technology, which is constantly changing.

3. Public/private partnerships, which are evolving every day.

"There are many extraordinarily talented people at DHS and NPPD," Spaulding said. She went on to say that the department is fortunate to be led by Secretary Johnson, who "brings a sense of urgency and unity of effort to the department." She said that the NPPD must be efficient and agile to work as an effective organization. A daily challenge is to make sure the NPPD is in sync with other security efforts.

"We are seeing changes at the department level, and also at the NPPD," she said.

Spaulding went on to describe the focus of each of the five subcomponent areas of the NPPD, and how each has become invaluable in terms of helping the department succeed in its mission.

- The Federal Protective Service (FPS), which provides security to federally owned and leased buildings and other assets.
- The Office of Biometric Identity Management (OBIM), which provides biometric identity services to DHS and its stakeholders, while protecting individuals' privacy and civil liberties.
- The Office of Cyber and Infrastructure Analysis (OCIA), which provides all-hazards analysis of cyber and physical critical infrastructure.
- The Office of Cybersecurity and Communications (CS&C), which assures the security, resiliency and reliability of the nation's cyber and communications infrastructure.
- The Office of Infrastructure Protection (IP), which leads the coordinated national effort to reduce risk to our critical infrastructure posed by acts of terrorism.

"All of us understand that we have limited resources (and) limited time, and we've got to make decisions about how we prioritize the allocation of resources, both during 'steady state,' and particularly in the case of an incident or crisis, whether it's a Superstorm Sandy or a cyber attack or (some other type of threat)," Spaulding said.

Technological advances bring increasing challenges and opportunities. "Our adversaries are not slowing down in their evolution of technology and techniques, and we have to be equally agile," Spaulding said. "In the cyber context ... we are constantly weighing destructive intent vs. capacity. The threat picture is very dynamic."

Technology is also impacting the law, she said. "There's a disconnect between the incredibly rapid pace of technological change and the deliberate speed that the law develops," Spaulding said, adding that lawyers must not ignore cyber security issues, but must be mindful to better ensure the protection of client information and data.

"Law firms are increasingly targeted for cyber thefts of information, and must be diligent about the 'cyber hygiene' (steps taken to improve cyber security) of their systems to protect clients," she said. This means not only making sure your technological security is up-to-date, but being wary of acquisitions. What is the cyber hygiene of companies you merge with?

Search ABA News

Stay Connected for ABA News

Media

Contact Media Relations at abanews@americanbar.org or call (202) 662-1090

- View a full list of media contacts

Articles and videos from the the 2014 ABA Annual Meeting in Boston

About the ABA

- Reporter Alerts
- Media Credentials
- Officer Bios

ABA News Sections

- Top Stories
- Multimedia
- News Releases

Key Issues

ABA President William C. Hubbard:

- Biography
- Stories, Releases and Statements
- 2014 Annual Meeting
- ABA House of Delegates
- 2014 Annual Meeting House Resolutions

- Section of Legal Education and Admissions to the Bar
- Immigration
- Criminal Justice Section
- Section of Litigation
- Law Practice Management Section

Spaulding said she's working with the ABA to encourage lawyers to include cyber security in their risk assessments during mergers and acquisitions. She said some companies that have grown through mergers have discovered much later, after "the wires are all connected," that they have a significant security problem.

Speaking to lawyers who work with clients in the critical infrastructure arena, Spaulding said to "remember that when NPPD knocks at the door and offers to do a vulnerability assessment, it's only to help you. The mission of the NPPD is just about helping enhance your security efforts and reducing risk."

The 9th Annual Homeland Security Law Institute was co-sponsored by the following ABA entities: Commission on Immigration, Committee on Disaster Response and Preparedness, Criminal Justice Section, Government and Public Sector Lawyers Division, Section of Environment, Energy and Natural Resources, Section of Intellectual Property Law, Section of Public Utility, Communications and Transportation Law, and Standing Committee on Law and National Security.

This entry was posted on Tue Aug 26 16:19:00 CDT 2014 and filed under Section of Administrative Law and Regulatory Practice and Top Stories.
Congress must help DHS combat rising cyberattacks

By Homeland Security Undersecretary Suzanne Spaulding - 10/08/14 06:00 AM EDT

When Congress returns after the elections, lawmakers have a great opportunity to pass cybersecurity legislation that already has strong bipartisan support.

Should this be a congressional priority during the lame-duck session? The answer is an emphatic yes.

Our shared cyberspace is vulnerable to an ever-evolving range of threats, and we need to respond with the same alacrity demonstrated by our adversaries. This means legal authorities need to be clearly defined to avoid unnecessary delays. Congress should codify and clarify the Department of Homeland Security’s (DHS) existing responsibilities to help protect not only the dot-gov networks but to better support the efforts of the private sector as well.

In the last three weeks only, the DHS issued alerts for “Shellshock,” a new vulnerability that could allow attackers to remotely execute certain commands on millions of affected computers, and a vulnerability discovered within the Mozilla network that runs the Firefox Internet browser many people use. Earlier this year, legal uncertainty caused a delay in how quickly the DHS could address the “Heartbleed” vulnerabilities within the dot-gov system.

This year, President Obama has again proclaimed October as National Cyber Security Awareness Month to increase awareness and understanding of the important role each of us plays in securing cyberspace. Our nation’s cyber networks have become indispensable to modern life in America. They’re the very backbone of our 21st century economy and a major nerve center of our national security. But the threats to those networks include criminals and nation states, ranging in purpose from identity and data theft to espionage and disruption of critical functions. Vulnerable networks might hold the key that processes your paycheck or medical claim or brings electricity to your home. Increasingly, they handle myriad behind-the-scenes functions we rarely think of: the routing of train cars, monitoring of a safe water supply, and verification of airline passenger information.

Helping to safeguard our cyber networks is a critical element of DHS’s mission to protect the nation. To achieve this mission, the DHS requires the help of Congress.

The Homeland Security committees of the House and Senate have made real, bipartisan progress on important cyber legislation. Those clarify the responsibilities of the Department of Homeland Security in working with civilian federal agencies and the private sector to mitigate cyber risks. They also enhance the department’s authority to hire cybersecurity talent.

I urge Congress to seize the opportunity created by all of the hard work to date. The department and the Obama administration continue to stand ready at the front lines of cyber defense. Congress must pass these bills and show the American people that Congress can and will help solve the nation’s challenges.

Spaulding serves as undersecretary for the National Protection and Programs Directorate at the Department of Homeland Security.
Panel III:

The Future of Foreign Intelligence

Moderator: Laura Donohue
FISA Reform
Laura K. Donohue

I. INTRODUCTION

On October 4, 2001, President Bush authorized the National Security Agency (NSA) to collect two different types of bulk information: telephony and Internet metadata, and telephone and Internet content. The former gave the NSA the


This paper can be downloaded free of charge from:
http://scholarship.law.georgetown.edu/faspub/1318
http://ssrn.com/abstract=2395526

ability to identify terrorist-related activity through contact chaining—i.e., the process of building a network graph that modeled communication patterns of targets and their associates. Within a month, the President’s Surveillance Program, renewed thereafter at 30-60 day intervals, became operational.

Over the next twelve years, the contours of—and the legal basis for—the classified program and its component parts shifted. The Administration initially grounded FSP in the President’s Article II Commander-in-Chief authorities, the 2001 Authorization for the Use of Military Force (AUMF), and the War Powers Resolution. Gradually, key portions of the program were either eliminated or moved to the Foreign Intelligence Surveillance Act (FISA). Critical statutory changes contributed to the process. Despite these changes, calls for reform of FISA persisted. For the most part, however, they met with little success.

It was not until Edward Snowden’s releases, in June 2013 et seq., the court-ordered release of documents in a Freedom of Information Act (FOIA) case, and the declassification of additional documents by the Obama Administration that calls for significant reform took hold. With FISA considered by Congress to be


1 W. J. HAYWOOD, supra note 1, at 13.
2 W. J. HAYWOOD, supra note 1, at 13 (“Within 30 days, the FSP was fully operational. Private sector partners began to send telephony and Internet content to NSA as of October 2001. They began to send telephony and Internet metadata to NSA as early as November 2007.”)


7 See, e.g., Elec. Frontier Found. v. Dep’t of Justice, No. 04-cv-05231-TOR (N.D. Cal. 2013); Declasification Press Release, supra note 1. See also Nasser Madhavi, DNA releases more documents to justify NSA surveillance, USA TODAY, Dec. 21, 2011, http://www.usatoday.com/story/news/politics/2013/12/21/usa-today-documents-bulk-data4157873/ ("In the face of growing skepticism over the National Security Agency’s practice of collecting bulk phone and Internet records, the director of national intelligence on Saturday declassified several documents detailing the program. The latest declassification of documents comes during a week in which a federal judge ruled the NSA’s bulk collection was likely unconstitutional and a White House task force questioned the effectiveness of the program.").
this entity is constructed, (3) the scope of the approval, (4) verification, and (5) potential partial emergency exceptions.

Turning to the back-end framework, the Article addresses implementation as manifest through (1) analysis, (2) use, (3) retention, and (4) transfer of information. The second half of the back-end, transparency and oversight, emphasizes (1) who reports, (2) what is reported, (3) to whom such reports are made, (4) penalties for violations, and (5) alternative reporting channels.

Part V concludes by noting that the purpose of building the typology is to provide a framework for different considerations to be taken into account in constructing a comprehensive reform package. This Article does not take a substantive position on the categories put forward. Instead, it identifies potential ways to proceed in developing an approach to foreign intelligence gathering that is cognizant of new and emerging technologies, as well as other, competing needs, such as intelligence gathering, threat assessments, economic stability, civil liberties, the right to privacy, and protections against the misuse of information.

II. LEGAL UNDERPINNINGS

From the beginning, information about the existence of, and the legal basis for, the President’s Surveillance Program (PSP) was tightly controlled. Subjected to broader scrutiny, PSP’s legal foundations altered. Eventually, the constituent portions of PSP were either eliminated or transferred to FISA’s overarching framework. As more information became public, statutory and constitutional concerns emerged. Central to the debate has been the sufficiency of the existing statutory language in light of new and emerging technologies and the First and Fourth Amendment implications of the current programs. Resultantly, calls for reform are gaining ground.

A. The President’s Surveillance Program and its Transfer to FISA

In March 2004, a classified review of the program by the Office of Legal Counsel (OLC) determined that there was legal support for three of the four types of collection included in PSP: (a) bulk telephony metadata, and the contents of (b) telephone and (c) Internet communications. OLC found that, in contrast to the three programs, the bulk Internet metadata collection appeared to be prohibited by the terms of FISA and Title III. Based on OLC’s findings, President George W. Bush rescinded the authority to collect bulk Internet metadata and gave the NSA one week to terminate the program. DOJ and NSA subsequently transferred the process to FISA’s Pen Register/Trap and Trace Provisions (PRTT), with the first order approved July 14, 2007 and renewed thereafter at 90-day intervals. The program appears to have operated until December 2011, when it was discontinued for failure to deliver sufficient operational value to the NSA. The three remaining PSP programs reviewed by OLC (bulk telephony metadata, and the contents of international telephony and Internet communications) appear to have been known only to a small number of people within the executive branch. It was not until a New York Times article was published in December 2005 that their existence reached the public domain. At that time, only a narrow part of PSP emerged: the NSA’s interception of (at least some) telephone content between the United States and overseas. Some months later, the media reported further on the collection of domestic telephony metadata.

Pressured in late 2005 and early 2006 for the legal rationale behind the interception of international communications, a program that the Administration referred to as the Terrorist Surveillance Program (TSP), the government cited the President’s constitutional authorities as Commander-in-Chief, the 2001 Authorization for the Use of Military Force (AUMF), and the War Powers Resolution (WPR). Congress and others offered three principal legal objections. First, that the legislature had intended the 1978 Foreign Intelligence Surveillance Act, which restricted electronic surveillance and required judicial approval for the granting of orders, to be the sole means through which the executive branch could conduct domestic surveillance for foreign intelligence and international counter-terrorism

---

12. See WORKING DRAFT, supra note 1, at 34, 39; Declaration Press Release, supra note 1; Filing Declaration, supra note 1.
13. See Declaration Press Release, supra note 1; Filing Declaration, supra note 1.

Laura K. Donohue 4 FISA Reform

Laura K. Donohue 4 FISA Reform
purposes. FISA contemplated the advent of war, allowing a 15-day grace period, at the expiration of which the statute’s provisions would be in effect. 

Second, while the AUMF gave the President the authority to “use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks,” neither the legislative history nor the text of the 2001 AUMF made explicit reference to electronic surveillance.20

Third, Congress (and the Courts) had previously considered and declined to recognize claims to Article II authority to conduct foreign intelligence gathering within domestic bounds absent a warrant—this had been the basis on which FISA had been introduced.21

In the face of mounting public pressure, a company providing telephony metadata expressed concern to the NSA about the voluntary nature of the program, requesting that the process be, instead, one of government compulsion.22 Resultantly, on May 24, 2006, the NSA transferred the bulk collection of telephony metadata to FISA’s tangible good provisions in Section 501 (as amended by USA PATRIOT Act Section 215).23

During passage of FISA, some members of the House of Representatives warned the statute to read that it was the “exclusive statutory means for the Executive to conduct electronic surveillance, implying in the process that the President had inherent surveillance powers outside the statute. The Senate rejected this notion, suggesting that if the President were to engage in electronic surveillance outside the parameters of FISA, on judicial review, they wanted the Supreme Court to treat the President’s actions as under Article I, Section 8, as Authorization against the expressed intent of Congress. The Senate view carried. See 50 U.S.C. §1811 et seq.

50 U.S.C. §1811 (2006) (electronic surveillance); 50 U.S.C. §1829 (2006) (physical searches); 50 U.S.C. §1844 (2006) (open taps) (“Notwithstanding any other law, the President, through the Attorney General, may authorize [electronic surveillance, physical search, or pen/trap] to acquire foreign intelligence information for a period not to exceed 15 calendar days following a declaration of war by Congress.”). It provided for a 15-day grace period, to “allow time for consideration of any amendment to [FISA] that may be appropriate during a wartime emergency.” H.R. Rep. No. 95-770, at 34 (1978) (Conf. Rep.) (reprinted in 1978 U.S.C.C.A.N. 4048, 4060). At the expiry of the 15 days, absent any amendments, ordinary FISA provisions would have to be followed. Congress recognized that this had been a carefully-constructed compromise position: during the debates on FISA, the House of Representatives had sought a complete abatement of FISA during periods of declared war. The Senate objected, and the House of Representatives changed its position.


In 1972, the Court held that government officials were obliged to obtain a warrant prior to electronic surveillance, even where domestic security might be on the line. The court cited the “intensely personal and sensitive nature of the conduct and the resulting invasion of personal privacy” by the government, to underscore the importance of Fourth Amendment protections. United States v. U.S. Dist. Court, 407 U.S. 297 (1972).

55 WORKING DRAFT, supra note 1, at 28-40.

56 USA PATRIOT Act, Sec. 215, amending FISA Sec. 501, codified at 50 U.S.C. §1860 (Access to certain business records for foreign intelligence and international terrorism investigations). For the original order for Venues, see 54. Amendment of the Federal Bureau of Investigation for an Order Requiring the Prodc of Tangible Things from Telecommunications Providers Relating to [REDACTED]; Order No. BR-05 (FISA C, Op. Mem. 24, 2005), available at https://www.sfp.gov/doc/defaultfile/filendi/files/doc/06-05_hdc040_001_relatiedex_ver_5.pdf (referred by court order as part of the Electronic Frontier Foundation’s FISA litigation). Note that the specific telecommunications company from which such records were sought was redacted, as well as the remaining title; however, the government also released a NSA report that provided more detail on the title of the Order. OFFICE OF THE INSPECTOR GEN., NAVY’S EIC ASSISTANT/CONT. Sect. 315X, ST-94-018R, REPORT ON THE ASSESSMENT OF MANAGEMENT CONTROLS FOR IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE COURT ORDER: TELEPHONY BUSINESS

Laura K. Donohue 6 FISA Reform

Laura K. Donohue 7 FISA Reform

The remaining FSP collection programs, which focused on international telephone and Internet content, could not so easily be transferred to FISA.24 To do so, DoJ and NSA decided to find a legal theory to support the NSA’s addition and withdrawal of thousands of foreign targets for content collection.25

The solution ultimately turned on a new definition of "facility"—no longer would it be understood in relation to a particular telephone number or email address, but instead, it became defined in a manner that included general gateways used for communications.26 In January 2007, FISC approved the new theory with regard to foreign selectors but rejected it for the domestic realm, signing two separate orders.27

The former change immediately and negatively affected the number of foreign selectors that could be used with regard to collection.28 It also placed a higher administrative burden on the NSA. In April 2007, the Director of National Intelligence, J.M. McConnell, submitted a proposal to Congress to amend FISA to make it easier for the executive branch to target U.S. interests abroad.

Four months later, Congress passed the Protect America Act (PAA), raising restrictions on the surveillance of foreigners where one (or both) parties were located overseas.29 The statute removed the Foreign Intelligence Surveillance Court (FISC) from supervising the interception of communications that began or ended in a foreign country. In its place, the Attorney General and the Director of National Intelligence could authorize, up to one year, the acquisition of communications concerning "persons reasonably believed to be outside the United States," where five criteria were met.30 The PAA required the Attorney General to submit the targeting procedures to FISC and to certify that the communications to be intercepted were not purely domestic in nature.31 Once


Telephone content collection came to be known as the Terrorism Surveillance Program (TSP).

WORKING DRAFT, supra note 1, at 40.

The Working Draft, supra note 1, at 41.


Unlike the Foreign Content Order, the Domestic Content Order issued by FISA in January 2007 did not have an immediate, dramatic impact on collection. Nevertheless, it required the present to the point where, in January 2009, only a single selector was directed towards collection. The FBI subsequently took responsibility for the domestic order before the FISC. WORKING DRAFT, supra note 1, at 42.


Reasonable procedures were in place for determining that the acquisition concerned persons reasonably believed to be located outside the United States. 2. The acquisition did not constitute electronic surveillance (i.e., it did not involve the interception of telecommunications). 3. The acquisition involved obtaining the communications data from or with the assistance of a communications service provider who had access to telecommunications. 4. A significant purpose of the acquisition was to obtain foreign intelligence information; and 5. Minimization procedures outlined in the FISA would be used.

certified. FISC was required to grant the order. If intended to operate for six months, the PAA gave retroactive immunity to service providers to insulate them from civil liability. Congress continued the PAA until February 17, 2008, eventually replacing it with a more permanent measure: the FISA Amendments Act (FAA).

Consistent with this statute, FISA Section 702 empowers the Attorney General and the Director of National Intelligence jointly to authorize, for up to one year, “the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.” FISC annually reviews the certification for the order, to which certain limitations apply. The FAA also brought the targeting of U.S. persons overseas, previously addressed via Section 2.3 of Executive Order 12335, within FISA, providing greater protections for U.S. persons.

B. Reform Efforts

The Snowden releases in June 2013 or req set off a storm of criticism of the NSA’s use of its authorities under FISA and the F.A.A. Forced on the defensive, the Obama Administration responded by declassifying FISC orders, targeting and minimizing procedures, and other documents. Freedom of Information Act litigation initiated by the Electronic Frontier Foundation contributed further to the amount of information in the public domain, resulting during autumn 2013 in the monthly release of previously classified materials.

Cases challenging the legality of these programs are working their way through the courts. Some, directed at FISC, seek to obtain more information about the programs underway. Others focus on the statutory and constitutional questions. It appears that, for now, the Supreme Court is content to let the cases work their way through the lower courts. It is too early to tell how these suits will progress—not least because of difficult issues related to standing, jurisdiction, and Supreme Court precedent. What is clear is that the programs are highly contentious, with the circuits, just nine months, into the process, already divided.

Many observers suggest that the best solution to the lack of clarity surrounding the intelligence community’s authority to use new and emerging technologies to collect digital information is to amend the current statutory framework governing foreign intelligence and international counterterrorism investigations. Towards these ends, in 2013 Congress held numerous hearings.

90 Present FISA Act of 2007, Pub. L. 110-55, § 3, 121 Stat. 552 (Aug. 5, 2007) (amending FISA § 105C). Twice a year the Attorney General would be required to inform the Intelligence and Judiciary Committees of the House and Senate of incidents or noncompliance with the directive issued by the Attorney General or Director of National Intelligence regarding noncompliance with FISC-approved procedures, and the numbers of certifications or directives issued during the reporting period.

91 Present FISA Act of 2007, § 46.

92 Provisions were proposed in the interim. See, e.g., FISA Amendments Act of 2010, S. 2244 (111th Cong. 2007).


95 Five limitations apply to the order issued by the AG and DNI: (first) it must not intentionally target any person known to be located in the United States; § 1881b(3). Second, it must 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; § 1881b(2). Third, it may not intentionally acquire any communications to which the sender and intended recipient are known to be located in the United States; § 1881b(4). Fourth, it may not intentionally acquire any communication in which the sender and intended recipient are known at the time of the acquisition to be located in the United States; § 1881b(5). Fifth, the collection of such information "shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States." § 1881b(6). In exigent circumstances, the Attorney General and the DNI may authorize an immediate acquisition under Section 702; however, they must then submit a certification to the FISC as soon as practicable, but in no event later than seven days after they determine the exigency ceases.

96 The FISA required, for instance, that the government adopt targeting and minimization procedures for review by FISC. The minimization procedures, in particular, restrict handling information concerning U.S. persons initially acquired under Section 702—including the retention and dissemination of such information.

97 For a relatively complete list of key media reports and the Administration’s response, see American Civil Liberties Union, NSA Documents Released to the Public Since June 2013, available at https://www.aclu.org/nsa-documents-released-public-since-2013.

98 Laura K. Donohue

99 FISA Reform

100 Freedom of Information Act litigation initiated by the Electronic Frontier Foundation contributed further to the amount of information in the public domain, resulting during autumn 2013 in the monthly release of previously classified materials.

101 Cases challenging the legality of these programs are working their way through the courts. Some, directed at FISC, seek to obtain more information about the programs underway. Others focus on the statutory and constitutional questions. It appears that, for now, the Supreme Court is content to let the cases work their way through the lower courts. It is too early to tell how these suits will progress—not least because of difficult issues related to standing, jurisdiction, and Supreme Court precedent. What is clear is that the programs are highly contentious, with the circuits, just nine months, into the process, already divided.

102 Many observers suggest that the best solution to the lack of clarity surrounding the intelligence community’s authority to use new and emerging technologies to collect digital information is to amend the current statutory framework governing foreign intelligence and international counterterrorism investigations. Towards these ends, in 2013 Congress held numerous hearings.
and members of both Houses introduced dozens of bills centered on FISA reform.\textsuperscript{42} 2014 began in much the same manner.\textsuperscript{43}

As these reform efforts have gained momentum, the Obama Administration has indicated a willingness to amend the current law. In September 2013 the President appointed a Review Group on Intelligence and Communications Technologies.\textsuperscript{44} Their final report, issued in December 2013, made forty-six recommendations that incorporated a series of significant statutory reforms—ranging from repeal of key surveillance authorities to the creation of the Privacy and Civil Liberties Oversight Board. The Review Group recommended that future access to metadata be mediated by third parties, with telecommunications providers, or other entities, retaining the information, to which access could be granted only through specific orders from FISA.\textsuperscript{45}

In December 2013, in hearings before the Senate, the Deputy Attorney General, the Director of the NSA, and the NSA’s General Counsel issued a joint statement supporting limited reform of the current system.\textsuperscript{46} The following month, the President issued a new Presidential Policy Directive (PPD-28), laying out the current principles guiding SIGINT, such as the integration of privacy and civil liberties considerations in the collection of intelligence, limits on the collection of commercial information and trade secrets, and the tailoring of SIGINT to areas where the information is not otherwise available.\textsuperscript{47} The document restricts the use of bulk SIGINT data.\textsuperscript{48} It draws attention to the policies and procedures in place with regard to minimization (both dissemination and retention of personal data), data security and access, data quality, and oversight.\textsuperscript{49} PPD-28 announced the appointment of a Privacy and Civil Liberties official to assist key parties in their development of policies and procedures, as well as a coordinator for International Diplomacy to serve as a point of contact with foreign governments wishing to raise concerns about U.S. intelligence gathering.\textsuperscript{50}

In his speech accompanying the directive, the President stated his intent to “reform the programs and procedures in place to provide greater transparency to our surveillance activities and fortify the safeguards that protect

---


\textsuperscript{43} See, e.g., Senate Judiciary Committee Hearing on the Report of the President’s Review Group on Intelligence and Communications Technologies, 113th Cong. (Jan. 14, 2014); Senate Intelligence Committee Hearing on National Security Threats, 113th Cong. (Jan. 29, 2014) (discussing section 215 and raising concerns about revenue or misleading statements from government officials during previous hearings on NSA surveillance); Senate Judiciary Committee Hearing on Ongoing Recommendations to Reform FISA Authorities, 113th Cong. (Feb. 4, 2014); Senate Judiciary Committee Hearing on Privacy in the Digital Age: Preserving Data Broader and Controlling Cybercrime, 113th Cong. (Feb. 4, 2014); House Intelligence Committee Hearing on World Wide Threats, 113th Cong. (Feb. 4, 2014).

the privacy of U.S. persons.\textsuperscript{57} For the bulk collection program, this meant ordering a transition to end it, as it currently exists, and establishing an alternative collection structure—potentially along the lines of that recommended by the Review Group. To facilitate a transfer to a new system, the President instructed the intelligence community to develop options for a new approach, with a report due back to the President prior to FISA’s reauthorization consideration March 28, 2014.\textsuperscript{79}

The President’s remarks and issuance of PPD 28 minimized but did not eliminate the impact of the Privacy and Civil Liberties Oversight Board (PCLOB) Section 215 report, which was slated for publication the following week.\textsuperscript{80} That report made clear that the PCLOB considered the bulk collection of metadata to be illegal as both a statutory and a constitutional matter. The 28-page document called for an end to current program. Two of the board’s five members (Rachel L. Brand and Elizabeth Collins Cook, both of whom served in the Department of Justice during the George W. Bush Administration) supported modifications to the program to take account of privacy concerns. The three remaining members (David Medine, who was a Federal Trade Commission official during the Clinton Administration; James X. Dempsey, a public policy specialist at the Center for Democracy and Technology; and Patricia M. Wald, a former federal appeals court judge nominated by President Jimmy Carter), considered it necessary to end the program altogether.\textsuperscript{81}

Four days before the deadline, President Obama announced that, notwithstanding a further, 90-day extension of the program, he planned to ask Congress to end bulk collection altogether.\textsuperscript{82} In its place, telephone companies will retain the records for the usual amount of time, with the NSA only having access to particular records with FISA approval.\textsuperscript{83}

The President’s proposal goes some way towards meeting widespread criticism of the Section 215 program. It does not, however, address either of the critiques, nor does it affect the programs that continue under Section 702.\textsuperscript{84}


\textsuperscript{61} Id.


Part of the problem is that the conversation has proceeded in a piecemeal fashion. The president’s proposal will thus become yet another bill for Congress to consider. What has been missing from the discourse is a comprehensive framework for how to think about potential reforms.\textsuperscript{63}

If ever there were a time to re-think how to approach foreign intelligence gathering in a blue-skies fashion, that time is now. Technology has radically altered the landscape from both a threat perspective and from the vantage of privacy and civil liberties. A fragmented approach risks ignoring the potential effects of alterations in the law and opportunities to create a sustainable structure. In constructing such an approach, the first step is to consider how new and emerging technologies have altered the environment in which we now operate. This fundamentally shifts the conversation from an historically-laden approach to one that begins from a different point of analysis: namely, the technologies that now dominate the electronic communications sphere.


III. THE IMPACT OF TECHNOLOGY ON THE INFORMATION RANGE AVAILABLE

The evolution of technology has had a profound impact on how information is generated, transferred, and stored. New types of information are now available. Novel analytical tools allow for the generation of deeper insight into traditional and emerging forms of information. Technology has also affected the geographic assumptions underlying traditional foreign intelligence gathering (i.e., that a simple line can be drawn between domestic and international information flows, with heightened protections afforded the former).

Overlaid by the changing landscape has been the creation of additional protections afforded to U.S. persons. The problem is that this approach assumes that the identity of the individual (a) is known, and (b) may be closely aligned with the targeted information. New technologies, however, allow for identity masking and anonymity, as well as for the existence of significant amounts of information associated at the front end and from individual targets.

In considering potential changes to FISA, it is necessary to first consider how one should think about new and emerging forms of information, and the method by which such information is generated, transmitted, and stored.

A. Types of Information

Consider first different types of information. At the most general level, over the past four decades, the law has recognized three principal areas: content, personally-identifiable information (PII), and business records (including, inter

\textsuperscript{64} See generally Section 1055 of the USA Freedom Act, Pub. L. No. 113-293, 128 Stat. 2764, 2764-A37 (2014)


Wakeman, Matt Danzer, Wells Bennett, Peter Margolies, Jack Goldhagen, Tim Edgar, Joel Brenner, Sean Mirkil, and others on the topic.)
also, banking and financial records). These categories have been provided with different levels of protection.

The Supreme Court, for example, has traditionally applied a higher level of protection to content and, in the context of third party doctrine, a lower level of protection to customer records held by companies. Accordingly, traditionally FISA created a more stringent regime for electronic communications or physical searches, wherein content would be obtained, and a lower level of protection for the use of pen registers and trap and trace devices.

As new technologies have been presented, particularly in a post-9/11 environment, there have been efforts to apply the rules accompanying these categories to new areas. Developed in a different context, though, such statutory requirements may be ill suited to the task. As a result, institutional design may fail, courts may be unable to monitor implementation, Congressional oversight may be lacking, and civil liberties and privacy protections carefully considered in a different context may be bypassed. Continued reliance on these categories also risks masking the impact of emerging technologies on the evolution of each category, as well as preventing recognition of the expansion in the different types of information available.

In light of the current state of technology, it is thus worth considering at least five categories of information that have emerged: personal, transactional, relational, geolocational, and content-based. (See Figure 1) A brief discussion helps to illustrate the distinction between these areas.

The first category, personal information, relates to a single individual whose identity can be obtained from the information itself, or from that information and other information that is in the possession of, or is likely to come into the possession of, the person controlling the information. Traditionally this category has included information such as one's social security number, home address, credit card number, health or medical records, insurance information, and educational records. New technologies, however, have extended this category to include areas like biometric identification markers (e.g., facial recognition, DNA, and iris patterns), habit identification, and pattern matching.

The second category, transactional information, incorporates commercial transactions—i.e., the process of buying or selling something. It suggests a contractual relationship between two or more entities in which goods, services, or money are passed from one entity to another. Historically, this category was limited to banking or financial records or the purchase of property—and, again, differing levels of protection were provided, particularly as it was extended to areas like billing records. But transactional information also includes contractual agreements between entities and records pertaining thereto.

The third category, relational information, has emerged as an independent area as technology related to social network analysis has evolved. Using both visual and mathematical tools, new technologies allow individuals to map and to analyze various types of flows between people, groups, organizations, geographic regions, computers, URLs, and other connected entities. Relational information gives insight into not just the existence of connections between individuals, but their various roles and groupings within a network—i.e., who are the key connectors, leaders, bridges, and isolates, where the key clusters are and who comprises them, who is in the core of the network, and who is on the periphery. Social network analysis yields additional insight into the distribution of resources (both material and nonmaterial), and potential constraints on individual actions. 15

The fourth category, locational information, identifies the specific physical location of an object or an individual. It thus relates to the geography of the real world. Geolocational data in particular has come to be associated with technologically-enhanced methods of ascertaining physical placement (e.g., radar, GPS devices in automobiles or mobile phones, or internet connections). This category also incorporates the more traditional mode of ascertaining

15 For further discussion see S. Wasserman and K. Faust. Social Network Analysis (1994).
individuals’ locations—i.e., the simple observation of individuals in public space. The fifth category, content, is perhaps the most traditional category in its close association with both the First and Fourth Amendments. Technology, however, has expanded the range of materials that may provide what can be considered substantive information. At the broadest level, content includes the substance of communications, writings, and other materials. As a form of communication, it conveys information through the exchange of ideas, thoughts, or other information, such as through speech, writing, or symbolic representations. It incorporates media content as well, such as pictures, videos, auditory files, and writing. It thus relates to the nature of individual experience.

Each of these categories has privacy interests associated with it that are particular to that type of information. This suggests that consideration of each category, vide generis, may be necessary to construct the most appropriate structures to protect such privacy interests. An added layer of complexity here is that the manner in which such information presents in each category—i.e., the way it is accessed, transmitted, or stored—differs.

B. Method of Access, Transmission, and Storage

Each of the different forms of information (personal, transactional, relational, locational, and content) may be accessed, transmitted, and stored in different ways. Some of these may be non-digital, such as simply observing another’s actions or reading a hand-written letter. Others, such as accessing information held on a server, may be technology-dependent. Simply extending the existing rules from hard copy to hard drives, though, misses the enhanced privacy implications of broader information exchanges. Six categories here deserve notice: audiovisual (AV) observation; communications networks; papers, hard drives (HDD) and device-specific storage; remote server/cloud technologies; and social media. (See Figure 1)

The first category, AV observation, is one of the most traditional ways in which information is accessed. Under this approach, information is obtained by observing a particular target or entity’s actions. Traditional modes of information collection in this area are similar to the use of cameras in public places. However, technology has expanded the ways in which one can observe such actions. Electronic bugs represented one of the early expansions. Placed in an individual’s office or home, such devices allow investigators to monitor conversations that are occurring within, thus giving them access to the content of communications. Kair dealt with such an “amplifying device,” attached to the outside of a phone booth. The Court recognized the time that new technologies applied to traditional areas could have a deeper impact on the right to privacy.

Other types of technologies are similarly relevant to enhanced AV observation, and they cross information categories. CCTV, for instance, may allow for remote surveillance even where the information obtained is not recorded. This extends beyond content information to include locational data: individuals may be followed in public space via traffic cameras, surveillance equipment on drones, satellite cameras, or other technologies. Such tracking may similarly reveal meetings, actions in the workplace, and social interactions—all forms of relational information. Observations of commercial exchanges, such as individuals shopping or withdrawing money from the ATM, represent transactional information. And in the realm of personal communication, AV observation may track individuals by appearance (e.g., using facial recognition), or by license plate (e.g., via automatic license-plate recognition (ALPR) or car plate recognition (CPR) systems). Such tracking through public space may identify individuals’ habits, their home address, their movements, and common patterns in which they engage.

The second category, communications networks, incorporates wire, cable, and satellite communication systems. This is the realm of electronic surveillance—which was one of the central areas addressed by FISA in 1978. The purpose was to provide a heightened level of protection for the content of individuals’ communications. But technology has progressed significantly beyond the telephone and wire communications originally considered. Communications networks may be accessed via telephones, computers, or other devices that link up to the Internet. Content information may be conveyed through telephone conversations, Face Time, texts, emails, or voice over Internet protocol (VoIP).

Much more than content is now involved in information carried through communications networks. Locational data, such as GPS transmissions, may be transferred. Relational data based on telephone and internet content may yield insight into social networks. Transactional information also may be conducted via automated telephone systems: post-cut-through-dialed digits (PCTID) (numbers dialed on a phone once a call has been put through) allow customers to buy airline tickets, transfer money between accounts, and sell stock. In the criminal law realm, efforts have been made to apply PRIT to this area. The problem is that PCTID also reveals content—suggesting a deeper privacy interest than mere envelope information. To the extent that automated systems reveal personal data, such as social security numbers (SSNs), credit card or bank account numbers, address information, and passwords (such as mother’s maiden name, place of birth, name of first pet), personal information is similarly implicated.

Laura K. Donohue
FISA Reform
16

Laura K. Donohue
FISA Reform
17
Notably, neither of the first two categories (A/V observation and communications networks) record what has historically been considered content. Instead, they record process and movement. Individual A goes to Place 1, then Place 2, and then Place 3. Or number X dials number Y. Or person A uses Credit Card 2. The recording of process and movement is what generates information.

Critics of the bulk collection programs point to the generation of information premised on structural connections, and the ability of the government to amass this information in large quantities, at reduced cost, and over extensive periods, to make the significant privacy implications. It may also be prospective, which shifts the question from how to access stored information or already-existing data, to how to control access to information generated in this manner in the future.

The third category, papers, is the one most closely associated with Fourth Amendment jurisprudence—not least because of the wording of the provision itself. Content information located in papers has thus traditionally been afforded the highest level of protection. Since obtaining one's letters, books, and writings, has generally required entry into one's domicile, a warrant, or something approaching a warrant in the realm of foreign intelligence, has typically been required.

FISA, accordingly, includes within its auspices special provisions for physical search that, along with electronic communications (also content-based), are afforded the highest level of protection.

Lines between categories may, of course, be somewhat permeable. The substance of one's papers may demonstrate an individual's location at a particular time, such as via receipts. Relational information may be ascertained from correspondence, and transactional information from financial records. Simultaneously, papers may provide personal information, such as one's health/medical, or educational records.

Notably, scientific advances have deepened the type of information that may be found in one's personal papers. DNA technologies, for instance, may reveal a host of information about individuals that was not previously known. But minimization procedures have failed to account for the qualitative differences in types of personal information obtained. Instead, they are rather crudely based on whether an individual is a U.S. person or a non-U.S. person.

The digitization of this information has not lessened the privacy interests involved. If anything, its presentation in an analyzable format has deepened the privacy implications. Simultaneously, the increased volume of information means that much more about an individual and his or her movements can be ascertained. Whereas before an individual's prior location might be determined by a receipt, mobile devices now include maps that can be queried for directions and that archive all of the places on which the individual movement. The pictures taken on an iPhone may include embedded data with the precise location at which the image was snapped. To the extent that mobile devices reflect the owner's actions (and not others of whom who use or borrow the device), they create a digital map of an individual's activities as well as that—indeed, the Court's jurisprudence—has failed to acknowledge this equal, or deeper, privacy intrusion.

As a result, in the fourth category, hard drives and electronic devices, we find varied applications of the existing rules. This category encompasses information held in electronic format on individual electronic devices, as well as other forms of local storage, such as memory sticks and stand-alone external hard drives. Content may thus take a number of forms—e.g., documents, spreadsheets, audio/visual files, and raw code.

Recent court documents suggest that there is confusion about what level of protection to give to electronic devices in the face of steadily expanding government capabilities. Confounded by requests by the FBI to place malware on a suspect's computer and to access a wide range of information held by the device in the course of an investigation, for instance, district court judges have come out on different sides of the issue. Network investigative techniques (NIT) allow the FBI to covertly download files, photographs, and stored emails, or even to activate cameras located on computers, allowing the government to obtain real-time images. The privacy interests involved in NIT are substantial. As the Ninth Circuit sitting en banc recognized in U.S. v. Cotterman in the context of a border search of a laptop:

"The amount of private information carried by international travelers was traditionally circumscribed by the size of the traveler's luggage or automobile. That is no longer the case. Electronic devices are capable of storing warehouses full of information. The average 400-gigabyte laptop hard drive can store over 200 million pages—the equivalent of five floors of a typical academic library. Even a car full of packed suitcases cannot hold a candle to the three- and ever-increasing, capacity of digital storage."

"Part posta, the amount of information that can be obtained from any individual's laptop is staggering. Recent media reports suggest that the NSA has inserted malware into computer networks, as well as, like the FBI, into individual computers, to collect information. In other words, the agency has compromised encryption technologies by arranging for secret "back doors" to be built into software, by making secret agreements with private companies, and by using supercomputers to overcome barriers using brute force."

---

81 Early reports about law enforcement use of malware emerged in 2001 with discussion of Magic Lantern. MEMRIC. The programs have since become increasingly sophisticated.


84 Cotterman. 709 F.3d at 964.


The location of the devices in question, which is one of the traditional ways to think about procuring foreign intelligence, seems to be a matter of concern, when compared to the privacy implications of access to such broad swathes of data.

The fifth category, centered on server and cloud technologies, recognizes that the same type of information that may be held on individual devices may be stored on a remote server, such as IBM Cloud, Amazon Cloud, or Amazon Cloud. Some companies, such as Dropbox, ZipCloud, SugarSync, and Google Drive, offer the ability to store all data remotely, so that the information can be shared and accessed at any time. Other companies, such as LiveDrive, Mozy, and BackupGenie, operate primarily as an online backup to individual devices. Yet others, such as MyPCBackup and JustCloud offer both services.

The cloud, though, does more than just offer ways to store information. Cloud computing uses a network of remote servers hosted on the Internet to manage and process data, extending these functions beyond individual hard drives or personal devices. Because of the sophistication of analytical techniques, the amount of data available, and the potential multi-sourcing of data involved, cloud computing changes what individuals and companies can actually do. It provides an opportunity for users to increase their capacity and to add capabilities without extensive, new investments in infrastructure, software, and personnel. And the market is exploding. As of July 2013, for instance, approximately 30 public companies represented more than $100 billion in market capitalization and $12.5 billion in estimated 2013 revenue.

The same techniques that may be used to exploit hard drives and individual, stand-alone electronic devices may be employed to obtain content, as well as location, relational, transactional, and personal information, from remote servers. The amount of information available—and insight into—the thoughts and actions of the target may be significantly enhanced—not least because more information can be uploaded and more powerful analytical software may be marshaled in relation to the cloud. In addition, there are some functions, such as online gaming, that are unique to the world of servers in that they take place (in part) on servers located outside the immediate electronic device. Efforts to communicate with others inside the gaming world may be subject to interception with (under traditional foreign intelligence provisions) little or no structure, oversight, or control. Yet this, too, is a form of access to the content of one’s communications—an area traditionally afforded the highest, not the lowest, level of protection to ensure that foreign intelligence gathering comport with the Fourth Amendment.

The sixth category, social media, is a form of electronic communication where users can create virtual communities to share information, ideas, personal messages, photographs, videos, and other data. Websites like Facebook, Twitter, Google+, Instagram, and Snapchat have become a critical form of networking and microblogging. They cross different types of information categories, simultaneously generating content, location, information, and relational information. The companies hosting the sites, in turn, maintain billing records, metadata, and other forms of transactional information, even as they have access to a host of personally-identifiable information about their account holders.

Each of these six categories, as it intersects with the five types of information that now exist, present opportunities for agencies looking to learn information about potential targets. Yet not all information is equal; the substance and techniques employed may yield different levels of value as well as different levels of insight into individuals’ private actions, thoughts, and beliefs.

From a value perspective, at one extreme, programs that fail to provide meaningful intelligence in the manner anticipated, may be voluntarily ended by the IC. According to James Clapper, for instance, “[I]n December 2011, the Government decided not to seek reauthorization of the bulk collection of Internet metadata.” ODNI explained, “the program was no longer meeting the operational expectations that NSA had for it.”

Reliance, however, on the value of a program to the intelligence agency involved for whether it will or will not operate would be misplaced. Individuals who have insight into the program’s extent may disagree about its worth. The bulk collection of telephone metadata has been challenged by individuals on the Senate Intelligence Committee, who have substantial access to the inner workings of the program, on the grounds that it does not yield significant benefits. But not all members of the committee—much less officials in the agencies themselves—agree with that position.

Regardless of how useful a program may be, underlying social, political, and constitutional concerns remain. To the extent that the different categories of information and related access, transmission, and storage yield differing levels of confidential information, different privacy interests come into play. Traditional models, based on, for instance, geography (i.e., whether the object, device, or target is located within U.S. bounds or outside the country), rather than the point. It is thus crucial to build an expanded understanding of the types of information in question into the statutory framework. These categories fold into the proposed taxonomy, below.

IV. TAXONOMY FOR REFORM

An unsystematic approach to reforming FISA risks masking the ways in which technology has altered the underlying landscape—particularly assumptions built

---


The top 15 cloud computing companies include: VMware, Equinix, Amazon, Google, Yahoo!, Microsoft, Facebook, Salesforce.com, IBM, and NetSuite.

Laura K. Donohue 20 FISA Reform

Laura K. Donohue 21 FISA Reform
into the statute in 1978. It also imparts the recognition of opportunities to respond more effectively to a shifting threat environment, as well as ways in which these new technologies carry with them unique incursions into civil liberties and the Fourth Amendment right to privacy. Minor shifts in statutory construction risk creating imbalance in institutional design. A system, for instance, that is built on placing electronic intercepts on traditional telephone lines may raise the importance of assigning a science and technology expert to FISC in order to help the court to understand new and emerging technologies. Similarly, geographic emphasis may fail to take account of global information flows.

A systemic re-evaluation of foreign intelligence gathering has not occurred since 1978. Statutory changes implemented in 1993, 1998, 2001, 2006, 2008, and 2011 failed to take a universal approach, instead altering the statute in limited or tangential ways. The most significant changes expanded current sections or added new provisions to the statute—such as the addition of business records in 1998 and their expansion in 2001 to tangible goods, or the inclusion of Sections 702, 703, and 704 in 2008. These amendments did not contemplate ways in which technology is changing how we should think about foreign intelligence gathering writ large. They did not consider the broader statutory design. And, for the most part, they did not explicitly deal with new and emerging technologies.

For these reasons, a comprehensive taxonomy is helpful now for thinking through changes that could be put into place. Where might we start if, in light of current technologies, we were to begin constructing a framework for foreign intelligence from the ground up? This question puts some of the assumptions that undergird FISA back on the table for discussion even as it introduces potentially new approaches.

Structurally, the proposed taxonomy can be thought of in two parts: a front-end and a back-end. The former framework deals with the authority to collect information and the latter the implementation of the authorities—i.e., the manner in which such information is obtained, analyzed and used. Both frameworks subdivide into two sections that exist in equilibrium: the first deals with the positive grant of authority, and the second with a check on the exercise of such powers. The latter thus balances the former, providing a counterpoise to potential authorities. Although the typology is designed to be cognizant of the need to create avenues for the collection and analysis of foreign intelligence information, as well as the need for protections on the exercise of these authorities, it does not in and of itself take a position on where these lines should be drawn. Instead, the purpose is to highlight the types of provisions that could be taken on board in building a comprehensive framework.

A. Front-End Framework to Collect Foreign Intelligence Information

Front-end considerations relate to the acquisition of information. They divide into (1) the manner of collection, and (2) requirements for approval of the authorities thereby created. (See Figure 2) The structure thus reflects a positive grant of authority under certain conditions (1), and structures to ensure that the appropriate processes are followed prior to government entities acting on those powers (2). While (2) thus acts primarily as a limitation on (1), it would be too simplistic to say that each category only performs these functions. For there are a number of ways in the sub-divisions in (1) could be constructed to provide checks on the system. Nevertheless, approaching the question in this manner allows for attention to be drawn to the different functions of the relevant entities.

**Figure 2**

<table>
<thead>
<tr>
<th>Master of Collection</th>
<th>Requirements for Approval</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Type of information</td>
<td>1. Identity Accessing Collection</td>
</tr>
<tr>
<td>a. Content</td>
<td>a. Executive</td>
</tr>
<tr>
<td>b. Locational</td>
<td>- agency-internal</td>
</tr>
<tr>
<td>c. Relational</td>
<td>- agency-external</td>
</tr>
<tr>
<td>d. Transactional</td>
<td>b. Judicial</td>
</tr>
<tr>
<td>e. Personal</td>
<td>- special court (e.g., FISC)</td>
</tr>
<tr>
<td>f. Temporal</td>
<td>- ordinary Act. 311 court</td>
</tr>
<tr>
<td>g. Social media</td>
<td>- Art. 1 court</td>
</tr>
<tr>
<td>h. Other (e.g., private industry)</td>
<td>2. Construction of entity</td>
</tr>
<tr>
<td>i. Selection of decision-makers</td>
<td>a. Originate entity (e.g., Circuit division, regional division, etc.)</td>
</tr>
<tr>
<td>i. Number of selection (e.g., President, Chief Justice, SCOTUS, Congress)</td>
<td>b. Lengthy prayer of terms (period of years, staggered terms, term limits)</td>
</tr>
<tr>
<td>j. Advancement process</td>
<td>c. Rights of challenge</td>
</tr>
<tr>
<td>k. Rights of appeal</td>
<td>d. Third party rights</td>
</tr>
<tr>
<td>l. Other (e.g., private industry)</td>
<td>- Constitutional advocate</td>
</tr>
<tr>
<td>m. Societal expert</td>
<td>- Technical expertise</td>
</tr>
<tr>
<td>a. Private industry</td>
<td>a. Application format</td>
</tr>
<tr>
<td>b. Data collection and storage</td>
<td>b. Standards (e.g., particularized, RAS)</td>
</tr>
<tr>
<td>c. Data security</td>
<td>c. Duration</td>
</tr>
<tr>
<td>d. No government entities</td>
<td>d. Removal requirements</td>
</tr>
<tr>
<td>e. No international partners</td>
<td>4. Verification</td>
</tr>
<tr>
<td>f. No international partners</td>
<td>a. Third-party data holder requirements</td>
</tr>
<tr>
<td>g. No international partners</td>
<td>b. Encryption keyholder requirements</td>
</tr>
<tr>
<td>h. No international partners</td>
<td>5. Emergency exceptions</td>
</tr>
<tr>
<td>i. No international partners</td>
<td>a. Substantive requirements</td>
</tr>
<tr>
<td>j. No international partners</td>
<td>b. Timeline for subsequent approval</td>
</tr>
<tr>
<td>k. No international partners</td>
<td>c. Use of information</td>
</tr>
</tbody>
</table>

---


Laura K. Donohue
22
FISA Reform
1. Manner of Collection

The first two considerations in the manner of collection center on the type of information in question and the method of access thereto, as well as the way in which such information is transmitted and stored. Part III of this article has already considered these areas in some depth. A short discussion will help to illustrate how using these demarcations would significantly depart from the current orientation of FISA, which relies on the target and the location of the information, and help to construct a new approach to foreign intelligence.

Consider first the type of information. It may be that personal and/or transactional information (e.g., the association of particular credit card numbers or billing records in relation to specific individuals) should be considered in a category apart from relational information, which in turn could be distinguished from locational or content-based information.

In other words, the associated structures may depend upon the type of information being sought. The number and types of entities from whom personal and/or transactional information may be obtained, the process for obtaining the information, what information may be retained, the manner and length of time of retention, and the use of such provisions would then revolve around the information itself, thus allowing the provisions to be tailored to the specific privacy interest involved.

This approach allows for more careful consideration of the type of information in question. For relational information, for instance, in addition to the threshold issue, perhaps the most important question is how to treat different levels of social connectedness—e.g., it may be a lesser privacy intrusion to obtain information that an individual is a member of an organization, than to look at relationships within organizations to consider the role one plays within the entity. Similarly, it may be that there are greater (or fewer) privacy interests in building social networks of geographic regions versus looking at individuals with similar political, economic, or religious subject-matter-interests. The more observation of individuals’ involvement, moreover, may be less intrusive than the digitization of such information and the combination of such data with other information—suggesting heightened privacy protections as one moves outward along the digitization axis (see Figure 1).

To the extent that locational information reveals substantive data, perhaps it should be placed within a framework similar to content-based approaches. Again, the outward movement along the digitization axis may trigger further protections as the data changes form or is incorporated into recombinant systems (i.e., systems that combine data with other information that allows the user a greater level of insight into individuals’ private lives).

Beyond the first two categories (the type of information, and the method of access, transmission, or storage), the manner of collection may be constrained with reference to other data. First, the form in which information is transferred may be considered as part of the front-end collection. The data, for instance, may be anonymized before it is provided to the government agency, with only certain data points meeting a pre-set selection criteria then subjected to real-time analysis. Alternatively, a third party data-holder may pre-screen the results of any searches. Thus, for instance, if a search returns 600 numbers, those relating to non-concerning entities could be screened out prior to government examination of the data.

Second, contours may be built around access to information based on the agency obtaining the information. This, in turn, has three components: (a) broad institutional design (e.g., deciding to separate NSA/CYBERCOM or requiring civilians to lead particular agencies); (b) prior authorization (e.g., authorizing the FBI but preventing the CIA (as in Exec. Order 12333) from engaging in certain activities); and (c) restrictions required (e.g., requiring the Attorney General or the Assistant Attorney General of the National Security Division to sign off on applications to obtain information).

The third consideration is the target about whom information is sought. Traditionally, FISA has focused on U.S. versus non-U.S. persons, presenting higher barriers to collection of information on the former, versus the latter. It has overlaid this with two additional categories—namely, whether individuals are foreign powers or agents thereof, involved in international terrorism. These categories are decided individually, requiring a nexus between the target of the information and the category. Discussion thus may turn on the level of suspicion required to collect information related to a target, for instance requiring a statement of facts supporting reasonable, articulable suspicion. (Note that one would then expect parity between this and the scope of approval, addressed, below)

A fourth, associated area may be the source of the information itself. FISA has only tangentially considered this in relation to business records and, substantially, tangible goods. But there are numerous sources that could be considered. Private industry may generate and/or store information. Different approaches that could be taken here include possibly introducing data retention requirements, which gives rise to considerations of cost. Data security prior to government access could be statutorily addressed. Attention also could be drawn to voluntary or compulsory compliance and associated risks of litigation borne by the companies. Alternatively, reform efforts may want to focus on constructing new, third-party data holders, which might be linked in some way to either government or to industry—or to neither. Under this approach, further thought may be given to dividing information between entities for additional protection of data. In this case, the security of the data would also be relevant, as would the potential for introducing yet another third party in the form of encryption key holders—the purpose of which is to divide the process via which the information is accessed. Encryption key holders may also be built into the independent entity holding the data, much like an IG office is part of the institutional framework of a government entity.

Information may also be obtained from other government agencies, in which case inter agency MOUs, standards, and procedures will have to be taken into consideration. Or it may be derived from non-governmental entities. If obtained from international partners, further verification of the information may be required. If this is the favored approach, the type of framing used alters. For example, lower levels of reliance may be assumed when information comes from foreign entities, in relation to which the U.S. has limited control, suggesting greater minimization procedures until information is verified. Alternatively, to protect other agencies’ missions, it may suggest limiting intra-governmental

---

84 But see Phil Osim, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. Rev. 1701 (2010).

transfer of information. Or, in the interests of privacy, it may mean creating higher barriers to obtaining information from a target’s employer, requiring a higher showing before a neutral arbiter before obtaining certain records.

The fifth additional area associated with the manner of collection is location. Traditionally, FISA has considered international versus domestic. But the possibility of having a mixed category (e.g., where information flows across borders), or one focused on the border itself may sharpen the analysis.

2. Requirements for Approval

Having considered the manner of collection, attention then turns to checks on the authorities in the form of what is required for approval prior to the collection of the information—essentially, the process that must be followed in order for collection to commence. Here, there are four principal considerations: the entity(ies) approving the collection, how that entity is constructed, what the scope of the approval is, and emergency exceptions. Underlying this demarcation is the time-honored understanding that having a neutral arbiter provides an important check on the exercise of authority.

The entity approving collection may be one of three forms. Within the executive branch, it may be internal or external to the intelligence agency that has been authorized to collect the data. In the judicial realm, there are three types of arbiters that may be constructed: a special court (like FISC), an ordinary Article III court, or an Article I court. There may, in addition, be a way to construct a board or independent arbiter from other sources, such as private industry or quasi-governmental organizations.

The construction of the entity itself also offers numerous options. The manner in which decision-makers are selected may include requirements with regard to the originating entity (for instance requiring a division among certain circuits, regions, or types of industry), as well as the manner of selection (e.g., by the President with the advice and consent of the Senate, by the Chief Justice of the Supreme Court, by members of the Supreme Court, by the Appellate Courts, or by particular committees in Congress). The length of the terms, or their progression (e.g., the period of years, staggered terms, and term limits) may also be considered. Adversarial processes, in turn, may involve rights of challenge to the orders, rights of appeal, third party rights, or the creation of a constitutional advocate, while technological expertise similarly may be built into the statutory design.

The scope of approval contributes further to the potential requirements that must be met prior to acquisition of information. This category highlights the form that the application or request must take, standards that the entity must follow in approving or disapproving of the applications, the duration for which applications may be granted, and the contours of any requirements for renewal.

Although not currently required under the statute, depending upon the final form of data storage and access, it may be desirable to include an additional verification stage—i.e., requirements that must be met by certain actors in verifying that the requesting agency has gone through the appropriate steps. These may apply to third party data holders, such as telecommunications companies, or independent entities established for the purpose of holding the data for intelligence purposes. It may be equally relevant for encryption key holders, prior to allowing access to the information.

A final area to highlight relates to emergency exceptions that could be constructed to take account of national security crises. Three principal areas (substantive requirements, the timeline for subsequent approval, and the subsequent use of information obtained during the exercise of the emergency provisions) provide the focus. Taken together, these various approaches suggest a more comprehensive view of ways to provide access to new types of information.

B. Back-End Framework to Analyze and Use Foreign Intelligence Information

Like front-end considerations, a range of categories could be used to explore the construction of a back-end framework centered on implementation of the authorities thereby granted. This framework also divides into two parts, reflective of the positive grant of authority and subsequent checks on the same powers, even as considerations within each category may consider both aspects as well. These realms relate to implementation, on the one hand, and transparency and oversight, on the other. (See Figure 3)

<table>
<thead>
<tr>
<th>Implementation</th>
<th>Transparency and Oversight</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Analysis</strong></td>
<td><strong>Who reports</strong></td>
</tr>
<tr>
<td>a. Raw data</td>
<td>a. Agency executing foreign intelligence authorities</td>
</tr>
<tr>
<td>b. Analysis (e.g., data mining, social network analysis)</td>
<td>b. IC entity’s Inspector General</td>
</tr>
<tr>
<td>c. Levels of analysis (e.g., primary, secondary, tertiary)</td>
<td>c. Administration (e.g., NSA, NGA, NRO, IG)</td>
</tr>
<tr>
<td>d. Required standards and processes to be followed</td>
<td>d. Statutory (e.g., CIA IG, DOJ IG)</td>
</tr>
<tr>
<td><strong>Collection</strong></td>
<td>e. IC entity’s privacy officer</td>
</tr>
<tr>
<td>a. Collection</td>
<td>f. Appraisal entity (e.g., FISC)</td>
</tr>
<tr>
<td>b. Provenance</td>
<td>g. External Agencies (e.g., ODNI, OMB)</td>
</tr>
<tr>
<td>c. Database (e.g., inter-agency and inter-agency, governmental and private databases)</td>
<td>h. Entities providing the information to the IC (e.g., private sector, NGOs)</td>
</tr>
<tr>
<td>d. Verification</td>
<td>i. Independent oversight body (e.g., PLOCB)</td>
</tr>
<tr>
<td><strong>Use</strong></td>
<td><strong>What is reported</strong></td>
</tr>
<tr>
<td>a. Minimization</td>
<td>a. Execution of authorities (e.g., storage of orders, programs, beneficiaries of seizures)</td>
</tr>
<tr>
<td>b. Judicial processes (e.g., prosecution, use of information as evidence in trial, etc.)</td>
<td>b. Application under the law (e.g., novel or significant legal interpretation, application to new technologies)</td>
</tr>
<tr>
<td>c. Consequential actions (e.g., further targeting, watchlist entries, etc.)</td>
<td>c. Noncompliance (willful and non-willful)</td>
</tr>
<tr>
<td><strong>Retention</strong></td>
<td>d. Non-standard (specifically requested) information</td>
</tr>
<tr>
<td>a. Length of time</td>
<td>e. Non-standard (specifically requested) information</td>
</tr>
<tr>
<td>b. Who holds the information (e.g., NSA, FBI, DOD, CIA)</td>
<td>f. Non-standard (specifically requested) information</td>
</tr>
<tr>
<td>c. How is the information held (e.g., digital vault, classified, shared with FCI or other data), including</td>
<td>g. Non-standard (specifically requested) information</td>
</tr>
<tr>
<td>d. Access (e.g., which individuals within agency, which agencies, under what conditions)</td>
<td>h. Non-standard (specifically requested) information</td>
</tr>
<tr>
<td><strong>Transfer</strong></td>
<td>i. Subsequent use of information obtained during the exercise of the emergency provisions</td>
</tr>
<tr>
<td>a. To whom</td>
<td>j. Subsequent use of information obtained during the exercise of the emergency provisions</td>
</tr>
<tr>
<td>b. Restrictions on use, access, and sharing</td>
<td>k. Subsequent use of information obtained during the exercise of the emergency provisions</td>
</tr>
<tr>
<td>c. Verification</td>
<td>l. Subsequent use of information obtained during the exercise of the emergency provisions</td>
</tr>
</tbody>
</table>

Laura K. Donahue 26 FISA Reform

Laura K. Donahue 27 FISA Reform
1. Implementation

Implementation centers on how the authorities granted to the intelligence community are actually used. There are four categories to consider: analysis, use, retention, and transfer. Traditionally, emphasis has only been placed on the second and third areas and, even within these, on only a few components (e.g., minimization procedures and the length of time data is retained). The taxonomy thus allows more careful scrutiny of different aspects of the implementation phase and expands the ways in which Congress could approach each area.

Under analysis, for instance, a new foreign intelligence framework could focus on how raw data is treated. Emphasis on the type of analysis, such as what sorts of data mining or social network analyses can be performed could be considered, as well as levels of analysis (e.g., primary, secondary, and tertiary “hops”). Attention may be drawn to the requisite standards and processes to be adopted prior to progressing from one stage to the next.

Consideration could also focus on what I call “recombining information”—namely, the combining of information from different sources in a way that generates new knowledge. Attention can be paid to combining substantively distinct information, such as biometric and geographic data. It may center on programmatic combinations. For instance, agencies may want to combine information from different programs run under the same legal authorities (e.g., Sections 215, or from programs run under different legal authorities (e.g., Sections 702). Alternatively, agencies may want to combine databases held in different areas of the agency with databases held outside the agency, or government databases with publicly-available databases. Another consideration in looking at the analysis of the data centers on information verification. This becomes particularly important when subsequent intrusions into civil liberties and individual privacy may flow from the initial analysis. This approach would help to highlight new and emerging ways in which data analysis is progressing.

The use of such information also presents an opportunity for statutory construction. Minimization procedures have historically been considered (and still offer) an opportunity for further inspection. But prosecutorial limits, the use of such evidence in trial, and other judicial process-related concerns may be taken on board, as well as the extent to which consequences that follow from initial analyses, such as further targeting or watch listing, raise civil liberties concerns.

Retention has historically been limited to considerations about time, but there are other questions that could also be statutorily addressed. Once obtained (and not just at the outset), who should hold the information? Should it be held by the

NSA? The FBI? The CIA? Different government entities have different missions, and so the placement of the data is of consequence. Beyond the entity responsible for the data, how is the information being held? It may be in digital form or hard copy. It may be combined with other data or personal identifiers, or it may be isolated. Additionally, access may be considered—not just who has access within the intelligence agency in question (e.g., on a need to know basis, by level of clearance, or by programmatic assignment), but which other agencies have access to the information as well.

The final consideration relates to transferring the data. This incorporates the recipient of the information, further restrictions on use, access, and sharing, and ways in which the information may be verified in the future.

2. Transparency and Reporting

The flip side of the design for implementing the authorities granted to the intelligence community is considering how such use is to be monitored. As with requirements for approval at the front end, this area acts as a counterpoise, balancing the power to collect foreign intelligence with protections to prevent improper use of the same. It sub-divides into five primary considerations: who reports, what is reported, to whom the report is made, penalties for violations, and alternative reporting channels.

The first area, who reports, incorporates entities internal and external to the entity exercising the authorities. A good way to think about this area is in terms of concentric circles. (See Figure 4) In the core, the specific agency engaged in foreign intelligence collection may be required to report. One level out, the IC entity's inspector general may be brought on board. Of relevance is the underlying structure of this position—i.e., either administrative (e.g., the current
IGs of the NSA, NGA, and NRO, or statutorily required (e.g., the current IGs of the CIA and OMB). The abetting loop focuses on entities that provide information to the IC—such as the private sector or NGOs. On the outermost ring we then find independent oversight bodies, such as the Privacy and Civil Liberties Oversight Board (PCLOB).

The question of who reports falls then into the second area, which is what is reported. Entities may be required to report on the execution of authorities (e.g., the number and range of orders, programs underway, and benefits or rates of success). They may address how the programs have been applied under the law, detailing novel or significant legal interpretations, or the extension of prior legal analysis to new technologies. Noncompliance requirements (either willful or non-willful) are included here. Finally, of importance will be the manner in which non-standard (specifically requested) information will be handled.

Having looked at who reports and what is reported, the third area to consider is to whom such information is made available. For logical reasons, the potential list of recipients is to some measure co-extent with the entities considered for who makes the report (to ensure access to information necessary for them to fulfill their statutory duties). But there are some differences. Thus, reports may be required under certain circumstances to (a) the head of the agency executing the foreign intelligence authorities, (b) the entity’s inspector general or privacy officer, (c) the OMB or other executive branch agencies, or (d) independent bodies. In addition, (g) Congress, and (h) the public may also be considered for receiving reports from specific programs. While the latter reports would necessarily be unclassified, the reports to the preceding areas [(a)–(g)] may be classified or unclassified.

Crossing the first three categories are questions related to the burden such reporting may place on the agencies involved, in terms of time, personnel, and money. Special appropriations may be made, for instance, to account for the need to develop new technologies to allow for auditing programs, or to hire additional analysts to act in an internal capacity. Alternatively, consideration of reporting requirements as a whole may help to streamline the overall process.

The fourth consideration in transparency and oversight focuses on what to do about misuse of authorities. Penalties for violations may include administrative measures, such as reprimands, loss of security clearances, suspension, or termination. Civil remedies such as fines may be awarded, or criminal measures may be attached.

The fifth and final consideration focuses on what to do when the regular reporting channels are not working. How should one conceive of alternative reporting channels? Here, there appear to be two divisions. The first, relating to fraud, waste, and abuse, tends to be programmatic in that it focuses on specific programs in place. Questions to address include (a) the path that individuals concerned about fraud, waste, and abuse should follow (e.g., within the agency, relating to supervisors, going to ODNI, or approaching congress), as well as (b) protections against retribution. The second division emphasizes public interest—representing a systemic (not a programmatic) concern about the exercise of foreign intelligence gathering authorities. Here, attention may be paid to the role of external bodies as well as potential criminal defenses available in the event that the matter goes to trial (ex post v. ex ante considerations).

V. CONCLUDING REMARKS

Public knowledge of PSP has generated widespread calls for FISA reform. Proponents of change point to the general approach adopted by Congress in passing FISA, as a statutory language itself, and Fourth and First Amendment constitutional concerns as a basis for introducing alterations.

The trouble with many of the proposals is that they fail to adopt a fresh start to the question of foreign intelligence, instead, looking for fixes to specific problems. The quandary, however, is much bigger than, for instance, the lack of adversarial counsel, or the five year retention of data by the NSA. The problem is that technology has radically altered, and the approach on which FISA rests, centered on targets and geography, is now woefully inadequate for the world in which we now live.

It is for this reason that this Article has sought to look at how technology itself has altered since 1978, in terms of the types of information that are now available (i.e., personal, transactional, relational, locational, and content) and in the methods by which such information can be accessed, transmitted, and stored (namely, observation, communications networks, papers, hard drives and stand-alone devices, remote servers and cloud technologies, and social media).

Using these divisions as a basis for the first part of the front-end framework, the proposed taxonomy builds on them to add considerations related to the form in which such information is transferred, the agency seeking the information, the target about whom information is sought, and the source and location of information. Set against the manner of collection at the front-end, are the requirements for approval. Here, the entity approving the collection, the construction of that entity, the scope of the approval to be granted, potential verification regimes, and exceptions in times of emergency may be considered.

For the back-end framework to analyze and use foreign intelligence information, implementation divides into four primary areas: analysis, use, retention, and transfer. The check on these authorities primarily takes the form of transparency and oversight, which further sub-divided into five areas: who reports, what is reported, to whom they report, penalties for violations, and alternative reporting channels.

While the taxonomy does not represent a radical re-conception of intelligence collection, it does expand the scope of the current reform efforts addressed in Part II to include the range of potential areas that could be brought on board. In doing so, it builds on the country’s experience over the past 36 years even as it recognizes changed circumstances. Although the Article takes no normative position on the specific reforms to be given effect, it clarifies areas critical for discussion and, in so doing, their complex relationship with other elements in the framework. The hope is that the taxonomy may serve as a way to move the conversation forward in developing an approach to foreign intelligence gathering that is cognizant of the need to obtain foreign intelligence, even as it recognizes the changing privacy interests implicated by new and emerging technologies.

Laura K. Donohue
Georgetown University Law Center, lbdonohue@law.georgetown.edu

SSRN: http://ssrn.com/abstract=2497022

This paper can be downloaded free of charge from:
http://scholarship.law.georgetown.edu/cong/119

I. INTRODUCTION

Documents released over the past year detailing the National Security Agency's telephony metadata collection program and interception of international content under the Foreign Intelligence Surveillance Act (FISA) directly implicated U.S. high technology companies in government surveillance. The result was an immediate, and detrimental, impact on U.S. firms, the economy, and U.S. national security. The first Snowden documents, printed June 5, 2013, revealed that the U.S. government had served orders on Verizon, directing the company to turn over telephony metadata under Section 215 of the USA PATRIOT Act. The following day, The Guardian published classified slides detailing how the NSA had intercepted international content under Section 702 of the FISA Amendments Act. The type of information obtained ranged from E-mail, video and voice chat, videos, photos, and stored data, to Voice over Internet Protocol, file transfers, video conferencing, notifications of target activity, and online social networking details. The companies

1. Professor of Law, Georgetown Law and Director, Center on National Security and the Law, Georgetown Law.
7. Id.
involved read like a who’s who of U.S. Internet giants: Microsoft, Yahoo, Google, Facebook, Twitter, PayPal, YouTube, Skype, AOL, and localization.1

More articles highlighting the extent to which the NSA had become embedded in the U.S. high tech industry followed. In September 2013 ProPublica and the New York Times revealed that the NSA had enjoyed considerable success in cracking commercially-used cryptography.2 The following month the Washington Post reported that the NSA, without the consent of the companies involved, had obtained millions of customers’ address book data: in one day alone, some 444,743 email addresses from Yahoo, 105,068 from Hotmail, 8,287 from Facebook, 132,697 from Gmail and 22,881 from other providers.3 The extent of upstream collection stunned the public — as did slides demonstrating how the NSA had bypassed the companies’ encryption, intercepting data as it transversed between the public Internet and the Google cloud.4

Further documents suggested that the NSA had helped to promote encryption standards for which it already held the key or whose vulnerabilities the NSA understood but not taken steps to address.5 Beyond this, press reports indicated that the NSA had at times posed as U.S. companies — without their knowledge — in order to gain access to foreign targets. In November 2013 Der Spiegel reported that the NSA and the United Kingdom’s Government Communications Headquarters (GCHQ) had created bogus versions of Socialst and LinkedIn, so that when employees from the telecommunications firm Belgacom tried to access the sites from corporate computers, their requests were diverted to the replica sites that then injected malware into their machines.6

As a result of growing public awareness of these programs, U.S. companies have lost revenues, even as non-U.S. firms have benefited.7 In addition, numerous

countries, concerned about consumer privacy as well as the penetration of U.S. surveillance efforts in the political sphere, have accelerated localizations. Initiatives, began restricting U.S. companies’ access to local markets, and introduced new privacy protections — with implications for the future of Internet governance and U.S. economic growth. These effects raise attendant concerns about U.S. national security.

Congress has an opportunity to redress the current situation in at least three ways. First, and most importantly, reform of the Foreign Intelligence Surveillance Act would provide for greater restrictions on NSA surveillance. Second, new domestic legislation could extend better protections to consumer privacy. These shifts would allow U.S. industry legitimately to claim a change in circumstance, which would help them to gain competitive ground. Third, the integration of economic concerns at a programmatic level within the national security infrastructure would help to ensure that economic matters remain central to national security determinations in the future.

II. ECONOMIC IMPACT OF NSA PROGRAMS

Billions of dollars are on the line because of worldwide concern that the services provided by U.S. information technology companies are neither secure nor private.8 Perhaps nowhere is this more apparent than in cloud computing. Approximately 50% of the worldwide revenues previously came from the United States.9 The domestic market more than tripled in value 2008-2014.10 But within weeks of the Snowden documents, reports had emerged that U.S. companies such as Dropbox, Amazon Web Services, and Microsoft’s Azure were losing business.11 By December 2013, ten percent of the Cloud Security Alliance had cancelled U.S. cloud services projects as a result of the Snowden information.12 In January 2014 a survey of Canadian and British businesses found that one quarter of the responders were moving their data outside the United States.13 The Information Technology and Innovation Foundation estimates that declining revenues of corporations that focus on cloud computing and data storage alone could reach $35 billion over the next three years.14 Other commentators, such as Forrester Research analyst James Stone, have put actual losses

their customers only when required under law and not knowingly through a back door — the perception that they enabled the spying program has lingered.”


8 Id.

9 David Gibert, Companies Turn to Switzerland for Cloud Storage Following NSA Spying Revelations, [V1], BUSINESS TIMES, July 4, 2013, available at http://www.bstimes.co.uk/business-timesswitzerland-is-the-new-us-cloud-providers-turn-to-switzerland-for-cloud-storage-following-nsa-revelations/

10 See, e.g., Sam Ganz, NSA Spying Scandal Could Cost U.S. Tech Giants Billions, Truth. Dec. 10, 2013, available at http://business.time.com/2013/12/09/usa-spying-scandal-could-cost-u-s-tech-giants-billions/; "The National Security Agency spying scandal could cost the top U.S. tech companies billions of dollars over the next several years, according to industry experts. In addition to consumer Internet companies, hardware and cloud-storage giants like IBM, Hewlett-Packard, and Oracle could suffer billions of dollars in losses."; Ellis Muennich, U.S. High-Tech Industry Jeopardized From Edward Snowden Leaks, NETWORKWORLD, July 19, 2013 ("The disclosures about the National Security Agency’s massive global surveillance by Edward Snowden, the former information-technology contractor who was now wanted by the U.S. government for treason, is hitting the U.S. high-tech industry hard as it tries to explain its involvement in the NSA data-collection program."); Claire Cain Miller, Revelations of N.S.A. Spying Cost U.S. Tech Companies, N.Y. TIMES, Mar. 21, 2014, available at http://www.nytimes.com/2014/03/22/business/foreign-firms-find-themselves-in-middle-of-tech-companies-battle.html?_r=0 (writing: ‘‘Despite the tech companies’ assertions that they provide information on
as high as $180 billion by 2016, unless something is done to restore confidence in data held by U.S. companies.8

The economic impact of the NSA programs extends beyond cloud computing to the high technology industry. Cisco, Qualcomm, IBM, Microsoft, and Hewlett-Packard have all reported declining sales as a direct result of the NSA programs.9

Server, a webhosting company based in Virginia, reported in June 2014 that its international clients had dropped by 50% since the leaks began.10 Also in June, the German government announced that because of Verizon’s complicity in the NSA program, it would end its contract with the company, which had previously provided services to a number of government departments.11 As a senior analyst at the Information Technology and Innovation Foundation explained, “It’s clear to every single tech company that this is affecting their bottom line.” The European commissioner for digital affairs, Neelie Kroes, predicts that the fallout for U.S. businesses in the EU alone will amount to billions of Euros.12

Not only are U.S. companies losing customers, but they have been forced to spend billions to add encryption features to their services. IBM has invested more than a billion dollars to build data centers in London, Hong Kong, Sydney, and elsewhere, in an effort to reassure consumers outside the United States that their information is protected from U.S. government surveillance.13 Salesforce.com made a similar announcement in March 2014.14 Google moved to encrypt terms entered into its browser.15 And in June 2014 the company released the source code for End-to-End, its newly-developed browser plugin that allows users to encrypt email prior to it being sent across the Internet.16 The following month Microsoft announced Transport Layer Security for inbound and outbound email, and Perfect Forward Secrecy encryption for access to OneDrive.17 Together with the establishment of a Transparency Center, where foreign governments could review source code to assure themselves of the integrity of Microsoft software, the company sought to put an end to both NSA back door surveillance and doubt about the integrity of Microsoft products.18

Foreign technology companies, in turn, are seeing revenues increase.19 Runbox, for instance, an email service based in Norway and a direct competitor to Gmail and Yahoo, almost immediately made it publicly clear that it does not comply with foreign court requests for its customers’ personal information.20 Its customer base increased 34% in the aftermath of the Snowden revelations.21 Matteo Meier, CEO of Armotivision (Switzerland’s biggest offshore data hosting company), reported that within the first month of the Snowden releases, the company saw a 45% rise in revenue.22 Because Switzerland is not a member of the EU, the only way to access data in a Swiss data center is as a result of an official court order demonstrating guilt or liability; there are no exceptions for the United States.23 In April 2014, Brazil and the European Union, which previously used U.S. firms to supply underscores cables for transoceanic communications, decided to build their own cables between Brazil and Portugal, using Spanish and Brazilian companies in the process.24 OpenText, Canada’s largest software company, now guarantees customers that their data remains outside the United States. Deutche Telekom, a cloud computing provider, is similarly gaining more customers.25 In sum, numerous foreign companies are marketing their products as “NSA proof” or “safer alternatives” to those offered by U.S. firms, gaining market share in the process.26

III. FOREIGN GOVERNMENT RESPONSES

The Snowden documents revealed not just the extent to which high technology companies had become coopted, but that the targets of NSA surveillance include both allied and non-allied countries. The resulting backlash has led some commentators to raise concern that “the Internet will never be the same.”27 Jurisdictional questions and national borders previously marked the worldwide Internet discussions.28 Countries, however, are now using the disclosures to restrict data storage to national borders, making it more difficult for the United States to gain access.29 As risk is the balkanization of the Internet, undermining its traditional culture of open access, and increasing the cost of doing business.30

9 This number includes domestic customers who may go elsewhere to find greater privacy protections. See Guastella, supra note 11.
13 Andrea Pearman, German Government to Drop Verizon over NSA Spying Fear, WASH. POST, June 26, 2014.
14 Id.
15 Ewing et al, supra note 16.
16 Miller, supra note 11.
17 Id.
18 Ewing et al, supra note 16.
19 Id.
24 Id.
A. Data Localization and Data Protection

Countries around the world are increasingly adopting data localization laws, restricting the storage, analysis, and transfer of digital information to national borders.46 To some extent, the use of barriers to trade as a means of incubating tech-based industries predates the Snowden releases.47 However, in the aftermath of the leaks, the dialogue has accelerated. The asserted purpose is to protect both government data and consumer privacy.

As of the time of writing, China, Greece, Malaysia, Russia, South Korea, Venezuela, Vietnam, and others have already implemented local data server requirements.48 Turkey has introduced new privacy regulations preventing the transfer of personal data (particularly locational data) overseas.49 Others, such as Argentina, India, and Indonesia are actively considering new laws, even as Brazilian president Dilma Rousseff, has been promoting a law that would require citizens’ personal data to be stored within domestic bounds.50 Germany and France are considering a Schengen routing system, retaining as much online data in the European Union as possible.51

As a regional matter, the EU Commission’s Vice President, Viviane Reding, is pushing for Europe to adopt more expansive privacy laws.52 And in March 2014 the European Parliament passed the Data Protection Regulation and Directive, imposing strict limits on the handling of EU citizens’ data. Regardless of where the information is based, those handling the data must obtain the consent of the data subjects to have their personal information processed. They also retain the right to later withdraw consent. Those violating the directive face steep fines, including up to five percent of revenues.

In addition, the Civil Liberties, Justice, and Home Affairs Committee of the European Parliament passed a resolution calling for the end of the US/EU Safe Harbor agreement.53 Some 2000 U.S. companies rely on this framework to conduct business with the EU.54


50 Lexis, supra note 10.


54 NSA Spying: MEPs Take Proposal to Protect EU Citizens’ Privacy, EUROPEAN PARLIAMENT, Feb. 12, 2014

55 Alex Broy, Tech Safe Harbor Under Fire in Europe, POLITICO MORNING TECH. Nov. 6, 2013.

In May 2014 the EU Court of Justice ruled that users have a “right to be forgotten” in their use of online search engines. The case derived from a complaint lodged against a Spanish newspaper, as well as Google Spain and Google Inc., claiming that notice of the plaintiff’s repressed home on Google’s search engine infringed his right to privacy because the incident had been fully addressed years before. He requested that the newspaper be required to remove or alter the pages in question to exclude data related to him, and that Google Spain or Google Inc. be required to remove the information. The EU court found that even where the physical server of a company processing information is not located in Europe, as long as the company has a branch or subsidiary and is doing business in a Member state, the 1995 Data Protection Directive applies.56 Because search engines contain personal data, they are subject to such data protection laws. The Court recognized that, under certain conditions, individuals have the “right to be forgotten”—i.e., the right to request that search engines remove links containing personal information. Data that is inaccurate, inadequate, irrelevant, or excessive may be removed. Not absolute, the right to be forgotten must be weighed against competing rights, such as freedom of expression and the media.

Various country-specific privacy laws are similarly poised to be introduced. Their potential economic impact is not insignificant: the Information Technology and Innovation Fund estimates that data privacy rules could retard the growth of the technology industry by up to four percent, impacting U.S. companies’ ability to expand and force them out of existing markets.55

The current dialogue is merely the latest in a series of growing concerns about the absent of effective privacy protections within the U.S. legal regime. High tech companies appear to see this as a potential step forward. As Representative Justin Amash (MI-R), has explained, “Businesses increasingly recognize that our government’s out-of-control surveillance hurts their bottom line and costs American jobs.” It violates the privacy of their customers and it robs American businesses’ competitive edge.57

It is with concern about the impact of lack of privacy controls on U.S. competitiveness in mind that in December 2013 some of the largest U.S. Internet companies launched a campaign to pressure the government to reform the NSA surveillance programs. Microsoft General Counsel Brad Smith explained: “People won’t use technology they don’t trust.” He added, “Governments have put this trust at risk, and government need to help restore it.” Numerous high technology CEOs supported the initiative, such Google’s Larry Page, Yahoo’s Marissa Mayer, and Facebook’s Mark Zuckerberg.58 The aim is to limit government authority to collect user data, to institute better oversight and accountability, to ensure greater transparency about what the government is requesting and (obtaining), to increase respect for the free flow of data across borders, and to avoid political clashes on a global scale. Mayer explained, “Recent revelations about government surveillance activities have shaken the trust of our users, and it is time for the United States government to act to restore the confidence of citizens around the world.”59

46 Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

47 Michael Hindle, AMERICAN SPYING STHS TECH Firms, WALL STREET J. Feb. 18, 2014

55 MEMRI, supra note 11

56 Id.

57 Id.
B. Global Initiatives Regarding Internet Governance

Apart from economic considerations, the backlash raises question about the future of Internet governance. From the inception of the Internet, the U.S.-based Internet Corporation for Assigned Names and Numbers (ICANN) has governed the web. As time has progressed, and the Internet has become part of the global infrastructure, there have been calls from several nations to end U.S. dominance and to have the International Telecommunication Union (ITU), an entity within the UN, become the governing body. The revelations have not only contributed further to such calls, but they have spurred increased discussion of the need for regional Internet control.

Over the past decade, three main groups have emerged to vie for control of the Internet. The first is centered on states, who consider the question in light of national sovereignty. It is comprised of developing countries as well as large, emerging economies like China, Russia, Brazil, and South Africa. It overlaps significantly with the Group of 77 (consisting of more than 100 countries which emerged from the non-aligned movement in the Cold War). These states are critical of the United States and its dominant role in Internet governance and oppose private sector preeminence, on the grounds that they are patrons of the United States. Emphasis instead is placed on the UN and the ITU as potential repositories of Internet authority.

The second group is civil society. The third is the private sector. These groups both tend to support what is referred to as a “multistakeholder model,” i.e., native Internet governance institutions that are generally nonprofit entities in the private sector. Membership includes both technical experts (e.g., ICANN and Regional Internet Registries), as well as multinational corporations (e.g., Microsoft, Facebook, and AT&T). Prior to the Snowden releases, Japan, the EU, and the US found themselves in this camp. Civil society organizations emphasize Internet freedom, consumer privacy, and user rights—often bringing them into conflict with the states who comprise the G77-type group.

As one commentator explains, “This alignment of actors has been in place since the 2003 World Summit on the Information Society (WSIS) meetings. But the Snowden revelations seem to have destabilized this settled political alignment.”

In brief, ICANN and Brazil have formed an alliance, condemning U.S. actions. Concern about the latest revelations spurred a major conference in April 2014: i.e., the Global Multistakeholder Conference on the Future of Internet Governance. The purpose of the meeting, which was held in Sao Paulo, was “to produce universal internet principles and an institutional framework for multistakeholder Internet governance.”

It is not clear how the newest shifts will be resolved—either temporarily or in the future. But significant, and enormously important, questions have been raised by the Snowden revelations. How should the Internet governance be structured to ensure legitimacy and compliance? Who gets to make the decision about what such governance looks like? Which bodies have the authority to establish future rules and procedures? How are such bodies constituted and who selects their membership?

These questions are fundamentally at odds with the decentralization tendencies in the Internet—tendencies that have been exaggerated post-Snowden as a result of regional efforts to expand the local sphere of influence and to protect consumer and state privacy from U.S. surveillance.

The U.S. government’s failure to address the situation domestically has undermined the tech industry. Despite calls from the companies for legislative reform to address the breadth of the NSA programs, there has been no significant shift that would allow companies to approach their customers to say, with truth, that the situation has changed. Resultantly, American companies are losing not just customers, but the opportunity to submit proposals for contracts for which they previously would have been allowed to compete. And the future of Internet governance hangs in the balance.

IV. ECONOMIC SECURITY AS NATIONAL SECURITY

The NSA programs illustrate lawmakers’ failure to recognize the degree to which economic strength is central to national security, as well as the importance of the high technology industry to the U.S. economy. The concept of economic security as national security is not new: the Framers and the generations that followed acknowledged the importance of economic strength as central to national security. Our more recent understandings, however, have gotten away from the concept, in the process clearing important interests out of the calculations required to accurately understand the implications of government actions. Unintended consequences have resulted: the NSA revelations, for instance, may have driven bad actors to seek non-U.S. companies for ISP services, creating gaps in insight into their operations. They have also undermined U.S. efforts to call other countries to heel for their exploitation of international communications to gain advantages over U.S. industry. In sum, the expansive nature of the programs may well have acted to undermine U.S. national security in myriad ways linked to the country’s economic interests.

A. Economic Security from the Founding

Despite its appearance throughout U.S. history, the term “national security” is rarely defined. The 1947 National Security Act, for instance, which, inter alia, constituted the National Military Establishment (later the Department of Defense), and the National Security Council, refers to “national security” more than 100 times, yet it does not define the term. The Foreign Intelligence Surveillance Act of 1978 employs the term nearly a dozen times, to ascertain what matters fall within the Foreign Intelligence Surveillance Court’s (FISC) purview, who can certify an application to FISC, and under what conditions in camera and ex parte proceedings can be held. Where the Attorney General assures that a national security threat exists, officials may secret search and seize property—wanting notice otherwise required under the Fourth Amendment. But no definition is provided in FISA.
does the USA PATRIOT Act prove more illuminating—despite referring to national security more than two dozen times. Where we do find definitions in the U.S. Code, they tend to limit consideration to foreign affairs and matters related to military strength. Thus, under the Classified Information Procedures Act, "national security" is understood as involving matters related to the "national defense and foreign relations of the United States." Nowhere does the definition reference U.S. economic security.

In the amended National Security Act, the term could potentially be understood to encompass U.S. economic security, the actual definition does not specify a precise link to economic vitality. Instead, "intelligence related to national security" refers to:

all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that

(a) pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and
(b) that involves:

(i) threats to the United States, its people, property, or interests;
(ii) the development, proliferation, or use of weapons of mass destruction; or
(iii) any other matter bearing on United States national or homeland security.71

The Federal Information Security Management Act of 2002 provides for government-wide information security—simply fails to consider the economic underpinnings of national security, instead, understanding national security systems as any system:

(i) the function, operation, or use of which

(ii) involves intelligence activities;

(iii) involves cryptologic activities related to national security;

(iv) involves command and control of military forces;

(v) involves equipment that is an integral part of a weapon or weapons system; or

(vi) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.72

While there may be room in the definition for economic considerations, they are not front and center. Executive Branch articulations prove little better. President George W. Bush's five-page National Security Presidential Directive 1 referred to "national security" thirty-three times, without any definition. President Barack Obama's Presidential Policy Directive 1 (PPD-1), in turn, addressing the National Security Council, referred to "national security" thirty-three times—without ever defining it. And like the Executive Branch, Courts tend to look to the military and diplomatic aspects of national security, instead of their economic concomitants.73

Despite the lack of emphasis on economic strength, the Founders were well aware of the importance of the economy in fostering international independence. The Articles of Confederation failed in significant part because the national government lacked the resources, and the country’s economic strength, to protect the Union. For Alexander Hamilton, absent military might, diplomatic stature, and commercial success, the country would cease to exist.74

One of the first expansions of the executive, accordingly, was to include a Secretary of the Treasury, which, along with the Secretary of War and the establishment of the office of Attorney General, reflected the purposes for which Union had been sought: foreign relations, military strength, economic growth, and the rule of law.75 In his Farewell Address, President George Washington called for U.S. energies to be directed towards strengthening the U.S. economy: "[T]he great rule of conduct for us in regard to foreign nations is to extend our commercial relations, to have with them as little political connection as possible."76

The federal government was willing, from a very early date, to set in support of its commercial interests with whatever diplomatic, legal, and military power it could muster. The Monroe Doctrine was premised largely on this approach. In 1837, President Martin Van Buren came to office determined to continue Washington's legacy, underscoring the importance of avoiding entangling alliances while pursuing America's economic interests abroad. President Zachary Taylor came to office in 1849 determined to continue the course, emphasizing the importance of bolstering trade as a means of securing the country.77 The 1950 Clayton-Bulwer Treaty ensured that future canal access through Central America would be open to international trade.78 As Millard Fillmore succeeded Taylor, he considered commerce central to U.S. interests abroad—for this reason, the Navy would require further resources to protect trade along the Pacific Coast.79 Upon taking office, President Franklin Pierce reiterated the same policies: of the complicated European tumults and atrocities, the

73 See e.g. See N.Y. Times Co., 403 U.S. at 719 (Black, J. concurring).
74 FEDERALIST No. 19, Alexander Hamilton.
76 For a discussion of every military intervention in support of U.S. commercial interests, see William Appleman Williams, Empire as a Way of Life: An Essay on the Causes and Character of America's Peaceful Preeminence Along with a Few Thoughts About an Alternative (1st ed. 1940).
77 President Martin Van Buren, Inaugural Address (Mar. 4, 1837).
78 President Zachary Taylor, Inaugural Address (Mar. 5, 1849).
United States was to be exempt, "But the vast interests of commerce are common to all mankind, and the advantages of trade and international intercourse must always present a noble field for the moral influence of a great people." The United States went on to emphasize its dealings with Asia and to sign an historic trade agreement with Japan. Expansionism, and the economic benefits it brought, similarly proved central to U.S. national security. "Should [new possessions] be obtained," Pierce asserted during his Inaugural Address, "it will be through no grasping spirit, but with a view to obvious national interest and security, and in a manner entirely consistent with the strictest observance of national faith." From the 1998 Spanish-American War forward, the country promoted its national interests through formative political, military, and economic engagement in the international arena.

2. National Security Infrastructure

The National Security Council (NSC) is "the principal forum for consideration of national security policy issues requiring Presidential determination." The President looks to the forum for advice and assistance in matters ranging from domestic, foreign and military, to intelligence and economic. It is thus somewhat surprising that the 1947 National Security Act includes neither the Secretary of the Treasury, nor the Secretary of Commerce, as permanent (statutory) members of the NSC. Instead, the entity is chaired by the President, with formal membership extended to the Vice President, the Secretary of State, and the Secretary of Defense. The Chair of the Joint Chiefs of Staff acts as the statutory military advisor, the Director of National Intelligence the statutory intelligence advisor, and the Director of National Drug Control Policy as the statutory drug control policy advisor.

Under PDD-1, the NSC includes the Secretary of Treasury, and "When international economic issues are on the agenda of the NSC, the NSC's regular attendees will include the Secretary of Commerce, the United States Trade Representative, the Assistant to the President for Economic Policy, and the Chair of the Council of Economic Advisers." When the emphasis, however, is not international economic issues, the structure does not cement economic concerns into the discussion. Nor does it contemplate the inclusion of Treasury or Commerce as an operational matter—i.e., when the intelligence community is deciding whether to develop a surveillance program. Such matters are not brought directly to the NSC.

To the extent that the failure to include these members at the most basic level reflects a perspective that potentially sidelines economic concerns, the continued failure to build strong representation at a programmatic level underscores the concern. Economic concerns may be treated with seriousness, but they are not meaningfully integrated into the national security infrastructure.

3. Intended Consequences

There are various ways in which the failure to fully take account of the impact of the programs on U.S. industry may have acted to undermine U.S. security beyond weakening the economy. The revelations, for instance, may well have driven enemies of the United States to use other countries' Internet Service Providers, thus creating a gap in one insight into their operations. They may also spur the initiation of encryption techniques that the NSA will have no means to address—making the country less secure because of the perceived overreach of the agency. The revelations have also undermined U.S. credibility in challenging other countries' efforts to obtain trade secrets and other information through state surveillance. China provides one of the strongest examples.

Online warfare between China and the United States has simmered in the background, until in early 2013 the Obama Administration began to make it center stage. In January 2013 the New York Times reported that Chinese hackers had infiltrated its computers following a threat that if the paper insisted on publishing a story about its prime minister, consequences would follow. The following month a security firm, Mandiant, revealed that the Chinese military unit 61398 had stolen data from U.S. companies and agencies. In March 2013 President Obama's national security advisor publicly urged China to reduce its surveillance efforts—following which classified documents leaked to the public demonstrated the extent to which China had infiltrated U.S. government servers. In May 2013 the National Security Adviser flew to China to lay the groundwork for a summit, in which cyber surveillance would prove center stage. Two days before the Obama-Xi meeting was scheduled to take place, The Guardian ran the first story on the NSA programs. On June 7, when Obama raised the question of Chinese espionage Xi responded by quoting the Guardian and suggesting that the U.S. should not be lecturing the Chinese about surveillance.

Although differences may mark the two countries approaches to surveillance (e.g., in one case for economic advantage, in the other for political or security advantage), the broader translation for the global community has been one in which the United States has lost high ground to try to restrict cybersurveillance by other countries.

V. STEPS REQUIRED TO REDRESS THE CURRENT SITUATION

Numerous steps could be taken by Congress to address the situation in which U.S. industry currently finds itself. The most effective and influential decision that legislators could take would be to curb the NSA's authorities under the Foreign Intelligence Surveillance Act. This action has two components: first, ending the telephony metadata collection program and, second, restricting the use of to/from, or about collection under upstream interceptions. Both programs would further benefit from greater transparency, to make it clear that their aim is to prevent foreign aggression and to prevent threats to U.S. national security—not to engage in the interception of trade secrets or to build dossiers on other countries' populations.

The second most effective change that could be undertaken would be to introduce stronger privacy controls on U.S. companies, in the process bringing the United States into closer line with the principles that dominate in the European Union. The two entities are not as far apart as the dialogue might have one assume, and so changes required in this sphere would be minimal. Together, these two alterations—curbing the NSA surveillance programs and providing increased consumer protections for...
privacy—would allow U.S. industry to argue changed circumstance to allow companies to again become competitive for contracts and markets to which they seek access.

A third alteration that would make a substantial difference over the longer term relates to the national security infrastructure. The current failure of the United States to integrate economic concerns creates a vulnerability for the country in terms of the breadth and depth of programs subsequently adopted. New thought needs to be given to how to take on board—and mitigate—potentially devastating economic consequences of government surveillance efforts.

A. FISA Alterations

In addition to the economic impact of NSA telephony metadata collection (discussed infra), the program runs contrary to Congressional intent in introducing the Foreign Intelligence Surveillance Act, contradicts the statutory language, and violates the Fourth Amendment. In 2013 the Privacy and Civil Liberties Oversight Board came to a similar conclusion, as did the President’s own appointed Review Group, charged with considering the telephony metadata collection program, in 2013.

Accordingly, the President announced on January 17, 2014 that he was “ordering a transition that will end the Section 215 bulk metadata program as it currently exists, and establish a mechanism that preserves the capabilities we need without the government holding this bulk metadata.” The alternative approach was to be developed by March 28, 2014. Nine months later, on September 13, 2014, the Foreign Intelligence Surveillance Court approved DUS’s request to extend the program for another 90 days—without any transition program in place.

Although the President issued a new presidential directive in January 2014 for U.S. signals intelligence activities both at home and abroad, the classified nature of parts of the document, international skepticism about the Administration’s commitment to privacy, and the failure of the Administration to achieve its homogenization of the global community, have already caused a question whether anything has really changed. No new legislation is in place that would provide limits on the Executive Branch beyond those that operated for the duration of the bulk collection program.

As a matter of Section 702 and the interception of international content, both PRISM and upstream collection present global concerns—neither of which have been addressed through any legislative change.

communications, where the individual is reasonably believed to be located outside the United States, as a policy matter, goes some way towards undermining international confidence in U.S. companies.

The Fourth Amendment does not reach non-U.S. persons based overseas who lack a substantial connection to the United States. Writing for the Court in United States v. Verdugo-Urquidez, Chief Justice Rehnquist concluded that “the people” referred to in the Fourth Amendment indicate a particular group—not merely people qua people. His reading stems from a deeply Aristotelian approach: i.e., one that emphasizes membership in the polis (nousia), or political community, as a concomitant of forming a structure of government. As members of the polis, U.S. persons, both distributively and collectively, obtain the protections of the constitution.

Looked at in this regard, the Constitution itself embodies the collective organization of “the people” into one entity. “U.S. persons” and “the people” are therefore one and the same. The “right of the people” thus refers to a collective group of individuals who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community.

Very few cases address precisely what constitutes sufficient contact with the United States to satisfy the “substantial connections” aspect of the majority’s decision. Those that do point in seemingly different directions. At minimum, however, it would be extraordinary to assume that simply because an individual’s company, he or she thereby gains the protections of the Fourth Amendment. This was the basic argument underlying the “modernization” of FISA at the first place, to take account of bad actors, communicating overseas, who would suddenly fall within the more protective FISA regime merely because their communications happened to come within U.S. territory by nature of the carrier in question. Even recognizing, however, that few constitutional barriers may apply to the programmatic use of Section 702 so far as it is applied to non-U.S. persons (leaving aside the questions that accompany the incidental collection of U.S. persons’ information, as well as entirely domestic conversations), as a matter of policy, certainly both PRISM and the use of to/from or about collection in upstream gathering has dramatically undermined U.S. industry. As a matter of policy, therefore, greater restrictions, more transparency, and more effective oversight of the international collection of content may help to alter the situation with regard to the skepticism expressed towards U.S. companies.

B. Privacy Law Harmonization

Much ink has been spilled on the cultural and practical differences between the U.S. and EU with regard to data protection and privacy law. These differences have been over-blown.
There are myriad ways in which the two regions reflect a similar approach. Just as the United States' Fourth Amendment protects the right to privacy, for instance, Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms embraces the same. These documents constitutionally ground two fundamental liberty interests in the respective regions' governing frameworks: (a) the right to privacy, and (b) freedom from arbitrary invasion of one's private sphere. In the European Union, these liberties are supported by EU-wide directives, such as the 1995 European Data Protection Directive and the EU Internet Privacy Law of 2002. Further, in both the EU and the U.S., such liberty interests are protected through national legislation, in which each remedy is provided for breach of the right to privacy. The manner in which these rights are treated is similarly consistent. In both spheres, these rights are offset against the obligations owed by the data holder to the individual to whom the information relates.

As a substantive matter, the two regions have adopted similar provisions. In both the EU and the U.S., for instance, heightened protections are provided for what is known as personally-identifiable information. A series of exceptions to the dominant structure is provided in two central areas: security (including, e.g., criminal law, public security, defense, and national security) and freedom of expression (such as with regard to journalism, literary pursuits, artistic expression, and political opinions). To ensure that the substantive measures reflect the underlying constitutional principles, both regions insist on minimization—i.e., that the information collected on individuals be limited to what is strictly necessary for the purposes delineated by statute.

Both the U.S. and the EU have established a set of substantive requirements related to individuals' knowledge that data about them is being collected, stored, and possibly shared with others. Consent, for instance, is central to both systems. Much has been made in regard to the distinction between the opt-in (European approach) versus the opt-out (American approach). What has been lost, however, is that both approaches rely on the consent of the subject (subject to specific exceptions, above), in order to proceed with data gathering, analysis, and distribution. To facilitate this structure, both regions also require that notice be provided to targets and that individuals have the right to access information that is held about them. Individuals, in both systems, have the right to object to particular information, and in both systems, the data holder has a duty to ensure that the information is accurate and kept up to date.

Keeping in mind the consistencies between the two systems, and the benefits to be gained for U.S. industry from emphasizing harmony, there are two areas where the two regions depart could be addressed through legislative reform: namely, recognition of residual rights in third party data, and the creation of a comprehensive, privacy-protective regime, as opposed to the piecemeal approach that currently marks U.S. law.

1. Residual Rights in Third Party Data

One central question that divides the United States from numerous other countries and regions—including the European Union—centers on who owns an individual's data. In the United States, since Smith v. Maryland (addressing pen registers and trap and trace devices), and U.S. v. Miller (focusing on financial records), all three branches have treated information held by third parties as lacking an individual right to privacy. In contrast, the European Union considers that the individual who has provided data to a third party to still have a privacy interest in the information. The recent European Court decision, recognizing the right to anonymity, necessarily presupposes a continued interest in data, even once it is obtained by a third party.

The difference between the approaches is central to understanding how new technologies, such as social network analysis, cloud computing, and data mining, have deepened the privacy interests implicated in third party handling of data. New technologies allow information to be generated about which even those to whom the data relates are unaware. To say that individuals do not have a reasonable expectation of privacy in this information rather flies in the face of common sense. The Supreme Court appears to be coming to this conclusion as well. In United States v. Jones, the Court considered a case involving 28-day surveillance involving the placement of a GPS chip on a vehicle. Although ultimately decided on grounds of trespass, a shadow majority expressed strong concern about the implications of long-term surveillance. Justice Alito, joined by Justice Ginsburg, Justice Breyer, and Justice Kagan, suggested that in most criminal investigations, long-term monitoring "implies on expectations of privacy." The nature of new technologies maddened: 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 their convenience. Many motorists purchase cars e.g., 1995 EU Directive, Registration No. 38 (notes) and 41 (right of access), and U.S. law. supra note 5.

12 Compare, e.g., 1995 EU Directive, Article 14 (right to object) and Art. 5 (accuracy data), and U.S. law. supra note 5.


14 See, e.g., 1995 EU Directive, Registration No. 47.


16 Id. at 949 (Alito, J., concurring).
that are equipped with devices that permit a central station to ascertain the
car's location at any time so that roadside assistance may be provided if
needed and the car may be found if it is stolen.116

Justice Sotomayor went one step further, calling into question the entire basis for
third party doctrine. Specifically, in light of the level of intrusiveness represented by
modern technology, "it may be necessary to reconsider the premise that an individual
has no reasonable expectation of privacy in information voluntarily disclosed to third
parties."117 Sotomayor pointed out.

This 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. People disclose the phone numbers that they dial or text
to the 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.118

She continued, "I would not assume that all information voluntarily disclosed to some
member of the public for a limited purpose is, for that reason alone, dispossessed to
Fourth Amendment protection."119

Congress has an opportunity to take the lead by recognizing the right to privacy
still held by data holders when information is collected by third parties. It can then
craft statutes accordingly, ensuring that U.S. companies offer greater protections for
consumers, in the process allowing industry to offset the claims of its overseas
competitors.

2. Legal Framework

Thus far, U.S. high technology companies have been subject to a very different
statutory and regulatory structure than that which prevails in the European Union. In
the United States, privacy rights have largely been protected via a series of vertical
statutes dealing with specific areas, such as children using the Internet, driver-related
information, and medical data.

In the EU, in contrast, privacy has been protected by a more omnibus-type
approach, which horizontally reaches across a number of areas. This approach is
reflected in the 1995 Directive as well as the national legislation implementing the
directive on a country-by-country basis.120

The vertical statutory scheme has been successful in addressing particular,
discrete areas where privacy interests reside. However, outside of these narrow
exceptions, in the interests of encouraging innovation, the high technology sector has
been left largely unregulated by federal statute. The assumption has been that market
forces would adjust to protect privacy interests.

The advantage of this approach has been to give high tech companies a significant
amount of flexibility, allowing them to independently gauge the appropriate level of
privacy protections to give to consumers.

The drawback has been that privacy itself has become commoditized, with
companies actively making money off of selling consumers' privacy interests.

Consider Google and its email service, Gmail, for instance. The company reads and
analyzes all of its customers' e-mails, it watches what people read, it looks at web
sites people visit, and it records what people purchase. The company then sells access
to customers' private lives to companies who want to advertise. Thus, the mother
who sends an e-mail to her son raising concern about depression may receive an ad
within hours for psychiatric services, even as a pregnant woman merely looking at
cribs, may within days receive mail through the U.S. post, advertising sales at Babies
R'Us.

In September 2013 Google lost an effort in the 9th Circuit Court of Appeals for
judicial review of a lower court's refusal to dismiss multiple class action lawsuits
accusing Google of violating the Wiretap Act. U.S. District Judge Lucy Koh
determined that the case is too far along to suffer delays. Koh's interpretation of the
Electronic Communications Privacy Act limits the "ordinary course of business"
exception—not least because Google's practice violates its own policies.121 The
lawsuits, filed in California, Florida, Illinois, Maryland, and Pennsylvania, at great
expense, are proceeding.

Capitalizing on private data represents a significant breach of the right to privacy.
Instead of protecting privacy, the market has exploited it for monetary gain. In
the United States and overseas, individuals are concerned about the lack of protections
afforded. Congressional legislation could fix this problem by bringing high
technology within the broader statutory framework and thus closing a gap in the
existing law.

3. Safe Harbor Considerations

In the wake of the Snowden documents, the EU Commission issued a report
recommending the retention of Safe Harbor, but recommending significant changes,
including required disclosure of cloud computing and other service provider contracts
used by Safe Harbor members.

The Safe Harbor provisions, developed 1999-2000 by the U.S. Commerce
Department, the Article 31 Committee on Data Privacy, and the European Union,
created a narrow bridge between the United States and EU. At the time, the European
Parliament, which did not bind the European Commission, rejected the Safe Harbor
provisions by a vote of 279 to 259, with twenty-two abstentions. Chief amongst
European concerns was the failure of the agreement to provide adequate protections.

In light of the massive data breaches we have had over the past five years in the
United States, the practices of a largely unregulated high technology industry, and the
ubiquitous nature of NSA surveillance, Europeans are even less supportive of the Safe
Harbor provisions. They amount to a self-regulated scheme in which the Federal
Trade Commission merely looks at whether a company, which has voluntarily opted-in
to the program, fails to do what it has stated it will do, within the bounds of its own
privacy policy. Stronger measures are necessary to restore European confidence in
U.S. high technology companies.

116. Id. at 963.
117. Id. at 957 (Sotomayor, J., concurring).
118. Id.
119. Id.
     Data Protection Act of 1978 (revised in 2004), Finland's Act on the Amendment of the Personal Data
     2472 on the Protection of Individuals with Regard to the Processing of Personal Data, April 1997.
121. In Re: Google Inc. Gmail Litigation, Case No. 5:13-md-02430, N.D.C.A.
C. Establishing Economic Security as National Security

Economic strength as national security, as was previously discussed, is not a new concept. The Founding itself was premised, in part, on the importance of economic security as being vital to U.S. national interests. In 1787 the Articles of Confederation were written out of existence on economic security grounds, as the country sought to reassure the international community that it was a viable trading partner. Since that time, the United States has at times had to remind itself of the importance of the economy to U.S. national interests. We are once again at such a time.

High technology is a vital part of the U.S. economy. It is both a symbolic and actual manifestation of the country's commitment to innovation in every sphere of life. It plays to the United States' strengths as a nation. It has the potential to change regimes, to alter political relationships, and to shape the daily lives of people around the globe. And it deserves special attention. The danger is that U.S. industry will become less competitive and that the U.S. will thus lose its dominance in the Internet economic sphere.

To some extent, we do, structurally, pay some attention to the importance of the economy. But many consequential decisions are thus not aired in full light of the possible implications for U.S. national security. One way Congress could rectify this would be to take a look at how to integrate economic concerns, as a statutory matter, into the national security infrastructure.

V. CONCLUDING REMARKS

To redress the negative effects that have followed from public awareness of the NSA programs conducted under Section 215 of the USA PATRIOT Act and Section 702 of the FISA Amendments Act, the most important step that Congress could take would be to reign in the surveillance authorities themselves, in the process providing greater transparency and oversight. An alteration in U.S. privacy law would also help to reassure U.S. customers and individuals located outside domestic bounds that consumer privacy is protected, thus allowing industry accurately to assert that the circumstances have changed. Consideration of how to integrate economic concerns into the national security infrastructure would further help to emphasize the importance of taking account of the impact of new initiatives on the United States.

12 Id.
2014

Bulk Metadata Collection: Statutory and Constitutional Considerations

Laura K. Donohue
Georgetown University Law Center, ldonohue@law.georgetown.edu

INTRODUCTION ........................................................................... 759
I. BULK COLLECTION IN THE CONTEXT OF FISA'S
A. General Approach ............................................................... 766
   1. Prior Domestic Surveillance ........................................ 767
      a. NSA Programs ....................................................... 770
         b. Project MINARET ............................................... 772
      2. Operation SHAMROCK ............................................ 773
         a. Broad Context ..................................................... 776
   B. Protections Built into FISA ........................................... 782
      1. Entity Targeted Prior to Acquisition ....................... 784
      2. Probable Cause and Showing of Criminal Wrongdoing Prior to Collection ...................... 786
      3. Minimization Procedures for Acquisition and Retention .......................................... 791
      4. Establishment of the Foreign Intelligence Surveillance Court and Court of Review ........ 792
   C. Subsequent Amendment ............................................ 793
      1. ,Physical Search, Pen-Traps ..................................... 794

*Professor of Law, Georgetown University Law Center. Christine Gambella was invaluable in obtaining research materials. My appreciation also extends to the members of the Harvard Journal of Law & Public Policy for their entry on the final Article. Special thanks to Hope Babcock, Bill Banks, Julie Cohen, George Jameson, Allegro MacLeod, Julie O'Sullivan, Milton Regan, Tasia Pobst, Kim Lane Schepel, and Mike Sicherman, for their comments on an earlier draft of this Article. In October 2013 an early version of this Article was placed online: Steve Yeadon, Laura Donohue's Comprehensive Case Against Bulk Metadata Collection, J.L.S. Security (Oct. 23, 2013, 6:32 PM), http://cybersecurity.org/2013/10/23/laura-donohue's-comprehensive-case-against-bulk-metadata-collections/, http://pew.org/security-fmds/ on the Combined Oversight of the Foreign Intelligence Surveillance Act Hearing Before the S. Cars. On the Judiciary, 113th Cong. (2013) (statement of Laura K. Donohue, Professor of Law, Georgetown University Law Center).

This paper can be downloaded free of charge from: http://scholarship.law.georgetown.edu/facpub/1350
http://ssrn.com/abstract=2344774


This open-access article is brought to you by the Georgetown Law Library. Printed with permission of the author.
Refer this and other works at: http://scholarship.law.georgetown.edu/
No. 3] Bulk Metadata Collection

III. CONSTITUTIONAL CONSIDERATIONS

A. The Problem with Smith v. Maryland

B. More Intrusive Technologies and Their Impact on Privacy

C. Judicial Tension: Trespass and Katz's Reasonable Expectation of Privacy

1. The Prohibition on General Warrants

2. Search of Metadata and the Reasonable Expectation of Privacy

D. The Proverbial Needle in the Haystack

IV. CONCLUSION

INTRODUCTION

On May 24, 2006, the Foreign Intelligence Surveillance Court (FISC) approved an FBI application for an order pursuant to 50 U.S.C. § 1861, requiring Verizon to turn over all telephony metadata to the National Security Agency.1 The Court subsequently approved similar applications for all major U.S. telecommunication service providers. Over the next seven years, FISC issued orders renewing the bulk collection program thirty-four times.2 Almost all of the information obtained related to

1. In re Application of the Fed. Bureau of Investigation for an Order Requiring the Provd. of Telecommunications Providers to Disclose Certain Records, 68 F. Supp. 2d 41, 43 (D. D. Md. 2000) (Redacted), Order No. BR 9605 (FISA Ct., May 24, 2006), available at https://www.fisc.fbi.gov/sites/default/files/tinedecorder/6f-05_1do965_redacted_ex__oral.pdf. (Note: the FISC order was released by the court after the publication of the Electronic Frontier Foundation's Freedom of Information Act (FOIA) litigation. Note that the specific telecommunication companies from which such records were sought were redacted, as well as the remaining title: the government, however, also released an NSA report that provided more detail on the title of the Order. Office of the Inspector Gen., National Security Agency, ST-06-106, Assessment of Management Controls for Implementing the Foreign Intelligence Surveillance Court Order: Telephony Business Records, available at http://www.dni.gov/files/documents/section9/pdf/J16-20150%20Memorandum%20on%20the%20106%20Assessment.pdf. (Note: the NSA report was released by the court after the publication of the report. For purposes of a more precise citation, I draw from both sources.)

2. ADMINISTRATION WHITE PAPER BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 2 (Aug. 9, 2013), available at https://www.documentcloud.org/documents/750211-administration-white-
the activities of law-abiding persons who were not the subjects of any investigation. This program remained secret until mid-2013, when a combination of leaks by Edward Snowden, a former National Security Agency (NSA) employee, and Freedom of Information Act litigation launched by the Electronic Frontier Foundation, forced key documents into the public domain. In response, the Obama Administration issued statements, fact sheets, redacted FISC opinions, and even a White Paper, acknowledging the existence of the program and arguing that it is both legal and constitutional.

According to these documents, the purpose of the telephone metadata program is to collect information related to counterterrorism efforts and foreign intelligence. These data include all communications routing information, including (but not limited to) session identifying information (for example, originating and terminating telephone number, identity of the communications device, etc.), trunk identifier, and time and duration of the call. The metadata collected as part of this program does not include the substantive content of communications.


As a practical matter, the NSA interprets the primary order as authorizing the agency to retrieve information as many as three tiers away from the initial identifier. The government refers to this process as "automated chaining." These results can then be further queried for "foreign intelligence purposes." In some cases, this information can then be forwarded to the FBI for further investigation, including using the information for an application for an electronic intercept order under Title I of the Foreign Intelligence Surveillance Act. On at least three occasions, the government has obtained authorization to expand the telephone identifiers that the NSA could query.

1. "hop" numbers."
3. Transcript of President Obama's Jan. 17 speech on NSA reform, Wash. Post, Jan. 17, 2014, http://www.washingtonpost.com/politics/transcript-of-president-obamas-jan-17-speech-on-nsa-reform/2014/01/17/54a3594a-7c96-11e3-9556-44df59c7d485_story.html [http://perma.cc/CF57-PVPS] ("Effective immediately, we will only pursue phone calls that are two steps removed from a number associated with a terrorist organization, instead of the current three."). Notably, some changes are not statutory, nor are they statutory changes requiring that the number of hops be changed, be made public.
4. SECTION 215 WHITE PAPER, supra note 2, at 4.
6. SECTION 215 WHITE PAPER, supra note 2, at 4.
7. Id.
9. "Authorization after this matter was initiated in May 2006 required the telephone identification that NSA could query to these identities associated with [REDACTED].
10. As discussed above, the program involves querying to telephone numbers that are at most three "hops" away from the initial number, as defined in the Foreign Intelligence Surveillance Act of 1978. Section 101 of that Act provides that "the term "tangible things" means articles of a physical nature, including electronic communications, in which the situation of the communication is to be determined by the physical location of the thing and not by its legal owner."
12. The program involves querying to telephone numbers that are at most three "hops" away from the initial number, as defined in the Foreign Intelligence Surveillance Act of 1978. Section 101 of that Act provides that "the term "tangible things" means articles of a physical nature, including electronic communications, in which the situation of the communication is to be determined by the physical location of the thing and not by its legal owner."
13. Since the advent of the program FISC has acknowledged "that the vast majority of the call-detail records provided are expected to concern communications that are (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls." The rationale behind collecting this information is that:
14. International terrorist organizations and their agents use the international telephone system to communicate with one another between numerous countries all over the world, including to and from the United States. In addition, when they are located inside the United States, terrorist operatives make domestic U.S. telephone calls. The most analytically significant terrorist-related communications are those with one end in the United States or those that are purely domestic, because those communications are particularly likely to identify suspects in the United States—whose activities may include planning attacks against the homeland.
15. The program is thus designed to obtain foreign intelligence and to protect against international terrorist threats both in the United States and overseas. Under the Foreign Intelligence Surveillance Act (FISA), which governs the program, the data obtained is understood as "presumptively relevant to an authorized investigation" where the government can establish that the information pertains to (a) a foreign power or an agent of a foreign power, (b) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation, or (c) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of an authorized investigation.
16. However important the purpose, the National Security Agency's bulk collection of telephone metadata embodies precisely what Congress sought to avoid by enacting the 1978 Foreign Intelligence Surveillance Act in the first place. In so doing, the program violates the spirit, as well as the letter, of the law. It also gives rise to troubling constitutional concerns.
Part I of this Article begins by pointing out that the reason Congress introduced FISA was to make use of new technologies and to enable the intelligence community to obtain information vital to U.S. national security, while preventing the NSA and other federal intelligence-gathering entities from engaging in broad domestic surveillance. The legislature sought to prevent a recurrence of the abuses of the 1960s and 1970s that accompanied both the Cold War and the rapid expansion of communications technologies.

Congress accordingly circumscribed the NSA’s authorities by limiting them to foreign intelligence gathering. It required that the target be a foreign power or an agent thereof, insisted that such claims be supported by probable cause, and heightened the protections afforded to the domestic collection of U.S. citizens’ information. Initially focused on electronic surveillance, FISA expanded over time to incorporate physical searches, pen registers and trap and trace, and searches of business records and tangible goods. The NSA program reflects neither the particularization required by Congress prior to acquisition of information, nor the role Congress anticipated for FISC and the Foreign Intelligence Surveillance Court of Review (FISC).

The bulk collection program, moreover, as pointed out in Part II of this Article, violates the statutory language in three important ways: (1) it fails to satisfy the requirement that records sought be “relevant to an authorized investigation;” (2) it fails to satisfy the statutory provision that requires that information sought also be obtained via subpoena duces tecum; and (3) it bypasses the statutory framing for pen registers and trap and trace devices.

Part III of this Article suggests that the bulk collection of U.S. citizens’ metadata also gives rise to serious constitutional concerns. Efforts by the government to save the program on grounds of third party doctrine are unpersuasive in light of the unique circumstances of Smith v. Maryland and the significant privacy invasions resulting from the universal use of pen registers and trap and trace devices, the evolution of social norms, and the advent of new technologies. In addition, the role of compulsion with regard to the FISC orders (in contrast to the consent of the telephone company in 1979) implicates the Fourth Amendment.

Further examining the Supreme Court’s jurisprudence, Part III goes on to note that over the past decade, tension has emerged between the view that new technologies should be considered from the perspective of trespass doctrine and the view that Katz’s reasonable expectation of privacy test should apply. Cases involving, for instance, GPS chips, thermal scanners, and highly-trained dogs divide along these lines. Regardless of which approach one adopts, however, similar results mark the application of these doctrines to the telephony metadata program.

Under trespass doctrine, the primary order for the program amounts to a general warrant—the elimination of which was the aim of the Fourth Amendment. In light of social norms, it is also a digital trespass on individuals’ private spheres.

Under Katz, in turn, Americans do not expect that their telephony metadata will be collected and analyzed. Most Americans do not even realize what can be learned from such data, making invalid any claim that they reasonably expect the government to have access to such information. The courts also have begun to recognize, in a variety of contexts, the greater incursions into privacy represented by new technologies.

A variant of the government’s argument suggests that the mere acquisition of data, absent human intervention, cannot constitute a search. There are multiple problems with this approach, not least of which are that the Supreme Court has never carved out an automation exception; that privacy interests are determined from the perspective of the individual, not the government; and that the decision to collect the information is replete with human interaction. Citations to the usefulness of such information fail to extract the program from a constitutional abyss.

Part IV concludes by calling for an end to the telephony metadata program and the implementation of FISA reforms to enable the government to take advantage of new technologies, to empower the intelligence agencies to respond to national security threats, and to bring surveillance operations within the bounds of statutory and constitutional law. Inserting adversarial

I. BULK COLLECTION IN THE CONTEXT OF FISA’S GENERAL APPROACH

In the early 1970s, a series of news stories broke detailing the existence of covert domestic surveillance programs directed at U.S. citizens. These revelations led, inter alia, to the creation of the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Chaired by Senator Frank Church, the Committee uncovered a range of disconcerting domestic surveillance operations—including some conducted by the NSA—prompting Congress to pass the FISA.

In this legislation, Congress purposefully circumscribed intelligence agencies’ authorities by adopting four key protections. First, any information obtained from an electronic intercept had to be tied to a specific person or entity, identified as a foreign power or an agent thereof, prior to the collection of the information. Second, the government had to demonstrate probable cause that the target, about whom information was to be collected, was a foreign power or an agent thereof. For U.S. persons, probable cause could not be established solely on the basis of otherwise protected First Amendment activities, thus providing U.S. citizens with a higher level of protection. Third, Congress adopted minimization procedures to restrict the types of information that could be obtained and retained. Fourth, FISA made provision for the Foreign Intelligence Surveillance Court to oversee the process. Designed to introduce a neutral, disinterested magistrate into the equation, FISC’s role was, narrowly, to ascertain whether the government had met the appropriate requirements for targeting prior to the acquisition of information. All of these limits dealt, specifically, with electronic communications. Over time, the statute expanded to apply a similar approach to physical searches, the placement of pen registers and trap and trace, and business records—as well as tangible goods.

The telephony metadata program runs contrary to the general approach Congress adopted in FISA both with regard to the particularization otherwise required and the role Congress envisioned for the Foreign Intelligence Surveillance Court and the Court of Review.

A. Prior Domestic Surveillance

One of the first public indications that the executive branch was engaging in broad domestic intelligence gathering came in January 1979. Writing in the Washington Monthly, Christopher Pyle charged that the Army was engaged in the surveillance of U.S. citizens. The following year, an organization calling itself the Citizens’ Commission to Investigate the FBI broke into a two-person FBI office in Media, Pennsylvania, stealing 1000 classified documents, all of which WIN Magazine subsequently published. A code word on these documents, “COINTELPRO” (for “counterintelligence program”), prompted Carl Stern, a reporter for NBC, to initiate a Freedom of Information Act lawsuit. On December 6, 1973, Stern

22. Id. § 1824(a).
23. Id. § 1804(x).
24. Id. § 1804(x)(2).
25. See id. § 1801(h).
filed a story that ran on NBC Nightly News, detailing extensive domestic surveillance and disruption undertaken by the FBI for national security purposes.14

In 1974, Seymour M. Hersh, an investigative reporter, published a detailed report in the New York Times catalyzing the conversation forward. Hersh reported that during the Nixon Administration the Central Intelligence Agency (CIA) had conducted a massive intelligence operation "against the antiwar movement and other dissenting groups in the United States."15

A special unit that reported directly to the Director of Central Intelligence had maintained intelligence files on more than 10,000 Americans, including members of Congress.16 The CIA had also engaged in dozens of other illegal operations since the 1950s, such as "break-ins, wiretapping, and the surreptitious inspection of mail."17 One official reported that the requirement to keep files on U.S. citizens stemmed, in part, from the so-called Huston plan.18 Agency officials claimed at the time that, although directed at U.S. citizens, everything they had done had been under the auspices of foreign intelligence gathering.19

These new revelations came as quite a surprise, not least because the 1947 National Security Act forbade the Director of the Central Intelligence Agency from having any "police, subpoena, law-enforcement powers or internal-security functions."20 The report, moreover, came on the heels of a Senate Armed Services Committee report condemning the Pentagon for spying on the White House National Security Council.

30. Memorandum from C.D. Brennan to W.C. Sullivan
433
34. Id. at 16. Named for Tom Charles Huston, the Presidential aide who conceived the project, the plan called for the use of burglars and wiretapping to counter antiwar activities and student turmoil ostensibly "fomented" by black extremists. President Nixon and senior officials claimed that it had never been implemented.
35. Id. at 26.
38. Intelligence Activities: Hearing on S. Res. 21 Before the Select Comm. to Study
39. On Intelligence Activities of the United States, 94th Cong. 4 (1975) [House Select Committee Report].
40. Hearings with Senator Walter Mondale and Senator Gary Hart, in Wash-
41. 11, 94th Cong., 123 CONG. REC. 1416-34 (1977).
42. Id.
introduced seven reports and six supplemental volumes, classifying another sixty reports for future release. The committee found that broad domestic surveillance programs, conducted under the guise of foreign intelligence collection, had undermined the privacy rights of U.S. citizens. The NSA figured largely in these concerns.

1. NSA Programs

Although the NSA maintained a definition of foreign intelligence that focused on threats external to the United States, a key contributor to the agency’s decision to intercept Americans’ communications was the question of whether the definition of foreign communications prevented the acquisition, or merely the analysis, of information not related to foreign intelligence. The NSA adopted—and the Church Committee rejected—the latter approach.

In October 1952, President Truman issued a classified memo that laid out the future of U.S. signals intelligence and created the NSA. Truman’s aims were to (a) strengthen U.S. signals intelligence capabilities, (b) support the country’s ability to wage war, and (c) generate information central to the conduct of foreign affairs. The NSA’s mission, accordingly, was to obtain foreign intelligence from foreign electronic communications.


44. See supra note 38.

45. 5 Church Committee Report, supra note 38, at 6 (citing Memorandum from President Harry Truman (Oct. 29, 1952)).


47. 5 Church Committee Report, supra note 28, at 6 (statement of Lieutenant General Law Allen, Jr., Director, National Security Agency).

48. National Security Council Intelligence Directive No. 6 (Dec. 12, 1947) (National Archives and Records Administration, RG 59, Records of the Department of State, Records of the Executive Secretary, NSC Files: Lot 66 D 168, Dulles-Jackson-Cornelius Report, Annex 12); see also 5 Church Committee Report, supra note 38, at 6.


50. 5 Church Committee Report, supra note 38, at 9.
contained on the NSA's watch list) "conducted intercept operations for the purpose of obtaining the communications of U.S. citizens."51 Whether such communications were incidentally intercepted, however, was another matter. As Lieutenant General Allen recognized, "[S]ome circuits which are known to carry foreign communications necessary for foreign intelligence will also carry personal communications between U.S. citizens, one of whom is at a foreign location."52

Central to Allen's assertion was the understanding that, to constitute foreign communications, and to legitimate the collection of information on U.S. citizens, the target of the surveillance must be a foreign power, or an agent of a foreign power, and at least one party to each communication must be outside the country.

The Senate considered this approach, in light of the broad swathes of information obtained about U.S. citizens, to run afoul of the Fourth Amendment. Two NSA programs in particular generated significant concern. The first, Project MINARET, introduced to collect foreign intelligence information, ended up intercepting hundreds of U.S. citizens' communications. The second, Operation SHAMROCK, involved the large-scale collection of U.S. citizens' communications from private companies.

a. Project MINARET

In the late 1960s, the NSA, like the Internal Revenue Service (IRS), the FBI, and the CIA, constructed a list of U.S. citizens and non-U.S. citizens subject to surveillance.53 The program, which operated from 1967 to 1973 started out by narrowly focusing on the international communications of U.S. citizens traveling to Cuba. It quickly expanded, however, to include individuals (a) involved in civil disturbances, (b) suspected of criminal activity, (c) implicated in drug activity, (d) of concern to those tasked with Presidential protection, and (e) suspected of involvement in international terrorism.54

51. Id.
52. Id.
53. Id. at 3.
54. Id. at 10-11.

55. Id. at 30.
56. Id. at 36.
57. Id.
58. Id. at 46-57, 60-41, 60; see also House Comm. on Gov't Operations, supra note 46, at 3-4 (discussing pressures on the Church Committee from the House side).
59. 9 Church Committee Rep't, supra note 38, at 37 (statement of Senator Frank Church, Chairman, Select Comm't to Study Governmental Operations with Respect to Intelligence Activities of the United States Senate).
Operation SHAMROCK was the cover name given to a program in which the government had convinced three major telegraph companies (RCA Global, ITT World Communications, and Western Union International) to forward international telegraphic traffic to the Department of Defense. For nearly thirty years, the NSA and its predecessors received copies of most international telegrams that had originated in, or been forwarded through, the United States. Operation SHAMROCK stemmed from wartime measures, in which companies turned messages related to foreign intelligence targets over to military intelligence. In 1947, the Department of Defense negotiated the continuation of the program in return for protecting the companies from criminal liability and public exposure.

Like Project MINARET, the scope of the program gradually expanded. Initially, the program focused on foreign targets. Eventually, however, as new technologies became available, the NSA began extracting U.S. citizens' communications. It selected approximately 150,000 messages per month for further analysis, distributing some messages to other agencies.

Senators expressed strong concern at the resulting privacy violations, inviting the Attorney General before the Select Committee to discuss "the fourth amendment of the Constitution and its application to 20th century problems of intelligence and surveillance." Senator Frank Church explained:

In the case of the NSA, which is of particular concern to us today, the rapid development of technology in the area of electronic surveillance has seriously aggravated present ambiguities in the law. The broad sweep of communications interception by NSA takes us far beyond the previous fourth amendment controversies where particular individuals and specific telephone lines were the target.

60. Id. at 57-58.
61. Id. at 58.
62. Id.
63. Id. at 58-59.
64. Id. at 60.
65. Id. at 63.
66. Id.
67. Id. at 59.
68. Id. at 39.
69. 5. Church Committee Report, supra note 38, at 20.
70. Id.
71. Id.
authority to break into and search individuals' homes without cause, the private affairs of every person would be subject to inspection. 73 In contrast, Levi argued, the exercise of electronic wiretaps for foreign intelligence gathering fell subject to Attorney General review. Nevertheless, he recognized the need for new laws to address the ambiguity that attended the use of modern technologies. The senators agreed. 74

2. Broader Context

The NSA was not the only federal entity making use of new technologies to collect significant amounts of information on U.S. citizens. The FBI, CIA, IRS, U.S. Army, and other federal entities similarly engaged in broad domestic intelligence-gathering operations. Details relating to many of these programs, such as the FBI's COINTELPRO and the CIA's Operation CHAOS, were uncovered by the exhaustive investigations of the Senate Select Committee and other entities that looked into the range and extent of programs underway. Both statutory violations and constitutional concerns accompanied these inquiries.

In 1970, for instance, Senator Sam Ervin (D-NC) began investigating the public allegations. After a year of making minimal progress in the face of misleading statements from the Nixon Administration, claims of inherent executive power, and a refusal to disclose information that might damage national security, Senator Ervin called for public hearings to consider "the dangers which the Army's program presents to the principles of the Constitution." 75

In 1975, President Ford issued an executive order establishing the President's Commission on CIA Activities Within the United States (the "Rockefeller Commission"). Ford appointed Vice President Nelson Rockefeller as chairman. 76 The public charges to which the Rockefeller Commission responded included large-scale domestic surveillance of U.S. citizens, retaining dossiers on U.S. citizens, and aiding these activities at individuals who disagreed with government policies. 77 The Commission's aim was further supplemented by allegations that the CIA had intercepted and opened personal mail in the United States for the past twenty years, infiltrated domestic dissident groups and intervened in domestic politics, engaged in illegal wiretaps and break-ins, and improperly assisted other government agencies. 78

Like the Senate Select Committee, the Rockefeller Commission faced the key question of how to define the term "foreign intelligence"—a crucial step in protecting Americans' right to privacy. Accordingly, in its first recommendation, the Rockefeller Commission advised that Section 403 of the 1947 National Security Act be amended to make it explicit that the CIA's activities must be solely related to "foreign intelligence." 79 Any involvement of U.S. citizens could only be incidental to foreign intelligence collection. 80

The Commission reinforced the strict separation between foreign targets and U.S. persons through its second recommendation: that the President, by executive order, "prohibit the CIA from the collection of information about the domestic activities of United States citizens (whether by overt or covert means), the evaluation, correlation, and dissemination of analyses or reports about such activities, and the storage of such information." 81

The House Select Intelligence Committee, created on February 19, 1975, was replaced five months later by a committee headed by Representative Otis Pike (D-NY). 82 The Pike Committee focused on a range of intelligence gathering programs, including those of the National Security Agency. 83 Public hear-

---

73. Id. at 72.
74. See, e.g., Id. at 66-67, 84, 125.
75. See, e.g., Id at 2.
nings on the agency's operations were held in October 1975 and February and March 1976. Its draft report complained of the tension between Congress and the executive branch, noting the "intense Executive branch efforts" to have the NSA hearings curtailed or postponed—both in the Senate and the House. Like the Church Committee, the Pike Committee expressed concern about SHAMROCK and MINARET, noting that the former resulted in the NSA maintaining files on approximately 75,000 U.S. citizens between 1952 and 1974:

Persons included in these files included civil rights leaders, antiwar activists, and Members of Congress. For at least 13 years, CIA employees were given unrestricted access to these files, and one or more worked full time retrieving information that presumably was contributed to the CIA's domestic intelligence program—Operation CHAOS—which existed from 1967 to 1974.

For the Pike Committee, these programs violated both Section 605 of the Communications Act and the Fourth Amendment. The committee expressed particular concern about the NSA's "vacuum cleaner" approach to foreign intelligence gathering. The committee noted that international telephone calls, some twenty-four million telegrams and fifty million telex (telegraph) messages entered, left, and transited the United States each year, and millions of additional messages that traveled over leased lines—"including millions of computer data transmissions electronically entering and leaving the country"—presented further potential sources of intelligence.

Coming on the heels of the Pentagon Papers, which demonstrated that the Johnson Administration had systematically lied to the public and to Congress; the Watergate scandal, in which the Nixon Administration orchestrated a June 1972 break-in at the Democratic National Committee headquarters; and Presi-

90. 438
91. Id.
given exclusive oversight of the CIA and concurrent jurisdiction over the NSA and other elements of the intelligence community. The resolution directed that the intelligence community keep the new entity "fully and currently informed" of their activities, including all "significant anticipated activities." It was to be a "select," rather than a "standing," committee, precisely to allow the Senate majority and minority leaders to decide its composition, and to avoid the same in the party caucuses preceding each new Congress. The chair and vice chair would not be allowed to serve concurrently as chair or ranking minority member of any major standing committee.

Of the fifteen members selected, no more than eight would be drawn from the majority party, ensuring balance between the parties. In addition, the Committee's composition would ensure cross-representation of related committees: Two members each would be drawn from the Appropriations, Armed Services, Foreign Relations, and Judiciary Committees. A limit of eight years was placed on committee membership, to avoid intelligence agency capture. Notably, five of the first fifteen members, Walter Huddleston (D-KY), Gary Hart (D-CO), Robert Morgan (D-NC), Barry Goldwater (R-AZ), and Howard Baker (R-TN), had served as members of the Church Committee. Fourteen members of SSCC's staff had served as staff members to the same, including William Miller, the staff director for both the Church Committee and the newly-minted SSCC.

99. Id.
100. Id.
101. Id.
102. Id.
103. Id.
104. Id.
105. Id.
Fourth, Congress passed the Foreign Intelligence Surveillance Act. The aim was to empower the intelligence agencies to collect information necessary to protect U.S. national security, while preventing agencies from using foreign intelligence gathering as an excuse for engaging in domestic surveillance of U.S. citizens. The process began with the Foreign Intelligence Surveillance Act of 1976, the first bill introduced in Congress, which was supported by the President and Attorney General and would require judicial warrants in foreign intelligence cases.

Its successor bill, S. 1566, became the Foreign Intelligence Surveillance Act of 1978.

B. Protections Built into FISA

From the beginning, Congress made it clear that the legislation was designed to prevent precisely the types of broad surveillance programs and incursions into privacy represented by Project MINARET, Operation SHAMROCK, Cointelpro, Operation CHAOS, and other intelligence-gathering initiatives that had come to light. During consideration of the conference report on S. 1566, for instance, Senator Ted Kennedy (D-MA) noted, "The abuses of recent history sanctioned in the name of national security..."

The Foreign Intelligence Act of 1978 represented the culmination of a multi-branch, multi-year, cross-party initiative directed at bringing the collection of foreign intelligence within a narrowly circumscribed legal framework. Congress consulted the NSA, FBI, CIA, and representatives of interested groups, gaining broad support for the measure. As a result, FISA passed by significant majorities.

Congress purposefully circumscribed the NSA's authorities in the Foreign Intelligence Surveillance Act by adopting four key protections. First, any information obtained from an electronic intercept had to be tied to a specific person or entity, identified...

113. Proponents of the bulk metadata collection program assert that the statute was not intended to protect against invasive surveillance. Indeed, the statute "creates a balance between the criminal system's restrictions on government practices and the broader acceptance of information-gathering during wartime." John Yoo, The Legality of the National Security Agency's Bulk Data Surveillance Program, 35 Harv. J.L. & Pub. Pol'y 901, 906 (2014). There are three problems with this claim. First, the two statements are not in opposition—that is, the program could be toward limiting government surveillance even as it seeks a balance between competing concerns. Second, the 'historical record' does not support the first part of the claim. The entire reason for the FISA was to create a framework to protect against overreaching use of surveillance. Third, FISA does not balance warrant information gathering with criminal law standards. It creates a framework for national security, regardless of whether the country is engaged in hostilities. The legislation specifically contemplates war, creating a short period of suspension, following which the FISA procedures must again be followed. Instead of a "warrantless information gathering scheme!", it would be more accurate to describe FISA as establishing a national security framework that applies regardless of whether or not the country is at war. See id.

115. Id.
116. Id.
117. Id.
as a foreign power or an agent thereof, before the collection of the information. Second, the government had to demonstrate probable cause that the target, about whom information was to be collected, was a foreign power or an agent thereof. For U.S. persons, such probable cause could not be established solely on the basis of otherwise protected First Amendment activities, thus providing U.S. citizens with a higher level of protection.

Third, Congress adopted minimization procedures to restrict the type of information that could be obtained and retained. Fourth, FISA provided for a Foreign Intelligence Surveillance Court (FISC) to oversee the process. Designed to introduce a disinterested magistrate into the equation, FISC’s role was, narrowly, to ascertain whether the government had met the appropriate requirements for targeting before the acquisition of information. All of these restrictions centered on the interception of electronic communications. Over time, the statute expanded to apply a similar approach to physical searches, the placement of pen registers and trap and trace, and searches of business records, as well as tangible goods.

1. Entity Targeted Prior to Acquisition

From the outset, Congress sought to limit the amount of information the NSA and others acquired by requiring that the target of surveillance be identified as a foreign power or an agent of a foreign power prior to the interception of communications. FISA defined a “foreign power” as:

(1) a foreign government or any component thereof, whether or not recognized by the United States;

(2) a faction of a foreign nation or nations, not substantially composed of United States persons;

(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments.

123. Id. § 1804(a).
124. Id. § 1804(b)(2).
125. Id. § 1801(a).
126. Id. § 1805.

No. 3]

 Bulk Metadata Collection

(4) a group engaged in international terrorism or activities in preparation thereof;

(5) a foreign-based political organization, not substantially composed of United States persons;

(6) an entity that is directed and controlled by a foreign government or governments.

Before passage of the bill, the Senate defined “foreign power,” with regard to terrorist groups, to mean a foreign-based entity. The House amendments, in contrast, understood “foreign power” to include groups engaged in international terrorism or activities in preparation thereof. In the end, the Conference adopted the House definition, with the idea that limiting such surveillance solely to foreign-based groups would be “unnecessarily burdensome.”

Throughout the nuanced discussion of the definition of “foreign power” in both houses was the understanding that prior to collection of information, the government would have to establish that the target—in relation to which such information would be obtained—qualified as a foreign power or an agent thereof.

In focusing on the targets of the communications, Congress rejected the NSA’s previous (and current) reading of what constituted a “target” in relation to data collection. That is, the information to be obtained, at the moment of acquisition (not in the context of subsequent analysis—the position Lieutenant General Allen advocated for during the Church Committee hearings, which the NSA has recently resurrected), had to relate directly to the individual or entity believed to be a foreign power or an agent thereof.

127. Id. § 1801(a).
129. 124 CONG. REC. 33,784 (1978).
130. S Church Committee Report, supra note 36, at 16 (testimony of Lieutenant General Lawton S. Collins, Director of National Intelligence, NSA); H Rpt No 95-1412, 95th Cong., 2d Sess., at 39 ("There are no U.S. citizens now targeted by the NSA in the United States or abroad."); Hearing Statement of Bobby R. Inman, Director, NSA, Before the Senate Subcommittee on Intelligence and Human Rights).
2. Probable Cause and Showing of Criminal Wrongdoing
Prior to Collection

A second protection stemmed from concerns evinced in the Senate about how to determine whether the (specific) target was a "foreign power" or "an agent thereof." Foremost in legislators' minds was the need to provide heightened protections for surveillance targets generally and U.S. citizens in particular. The final bill accomplished this in two ways: by adopting a standard of probable cause and, under certain circumstances, requiring a showing of criminal wrongdoing in order to acquire information. These elements underscore the particularity Congress required before foreign intelligence gathering was allowed.

FISA incorporated a standard of probable cause. Unlike criminal law—in which the courts required establishing probable cause that a target had committed, was committing, or was about to commit a particular offense—under FISA, the agency requesting surveillance had to demonstrate probable cause that the entity to be placed under surveillance was a "foreign power" or "an agent thereof," and that the target was likely to use the facilities to be monitored. For some entities, FISA also required a criminal showing for that entity to be considered a "foreign power." Foreign governments are excluded from this rule. When they are directly involved, no showing of crimin-

132. Compare 18 U.S.C. § 2518(1)(a) (2006) (requiring, under Title III, that the court must find "on the basis of the facts submitted by the applicant that . . . there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 3519 of this chapter"); with 20 U.S.C. § 1805(a)(3) (requiring, in contrast, that FISA find "on the basis of the facts submitted by the applicant") that "there is probable cause to believe that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power.") 

133. See, e.g., 50 U.S.C. § 1801(c)(1).

134. For clarity, the terms "foreign power" and "agent thereof" are broader than "foreign intelligence," so that once probable cause exists, the government need only show that the target is a "foreign power" or "an agent thereof." See, e.g., United States v. Ford, 42 U.S.C. § 2518(1)(a) (2006) (requiring, under Title III, that the court must find "on the basis of the facts submitted by the applicant that . . . there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 3519 of this chapter"); with 20 U.S.C. § 1805(a)(3) (requiring, in contrast, that FISA find "on the basis of the facts submitted by the applicant") that "there is probable cause to believe that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power.")


138. Bronson v. United States, 500 U.S. 346, 349 (1995). This is not broadest, however, as the "agent of a foreign power" standard contained in some criminal conspiracy statutes, see, e.g., 18 U.S.C. § 371 (requiring, in contrast, that FISA find "on the basis of the facts submitted by the applicant") that "there is probable cause to believe that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power.")

140. A "United States person" is understood under the statute as "a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(2)(B) of title I, 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 that rule does not include a corporation or an association which is a foreign power, as defined in subsections (a)(1) (A), (a)(1) (B), or (a)(2) of this section.") 50 U.S.C. § 1805(a)).
(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person’s presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities . . . or

(2) any person who—

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;

(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or

(E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).\(^{141}\)

141. 50 U.S.C. § 1801(3).
These provisions reflect criminal law standards.\textsuperscript{145} As the House of Representatives explained in the introduction to FISA:

This standard requires the Government to establish probable cause that the prospective target knows both that the person with whom he is conspiring or whom he is aiding or abetting is engaged in the described activities as an agent of a foreign power and that his own conduct is assisting or furthering such activities. The innocent dupe who unwittingly aids a foreign intelligence officer cannot be targeted under this provision.\textsuperscript{149}

The third category, which considers a U.S. person to be "an agent of a foreign power" for knowingly entering the country under false or fraudulent identity, almost always involves a showing of criminality, simply because it is not possible to legally enter the United States without providing proof of one's identity to a government official.\textsuperscript{146} It is similarly illegal to knowingly assume a false identity under anti-fraud provisions of the U.S. Code.\textsuperscript{147}

FISA's deliberate engagement of criminal law provisions and standards has been acknowledged by the government in defense of bringing down the wall between prosecution and investigation:

[A] U.S. person may not be an "agent of a foreign power" unless he engages in activity that either is, may be, or would be a crime if committed against the United States or within U.S. jurisdiction. Although FISA does not always require a showing of an imminent crime or "that the elements of a specific offense exist," Senate Intelligence Report at 13, it does require the government to establish probable cause to believe that an identifiable target is knowingly engaged in terrorism, espionage, or clandestine intelligence activities or is knowingly entering the country with a false identity or assuming one once inside the country on behalf of a foreign power. Thus, while FISA imposes a more relaxed criminal

\textsuperscript{145} Compare id., at 18 U.S.C. § 2, 271 (2006) (requiring actor to be engaged in the illegal activity himself or working with another to commit the offense); see also Supplemental Brief for the United States, supra note 138.


\textsuperscript{147} 18 U.S.C. § 1014.

\textsuperscript{148} Id. § 1028.

\textsuperscript{149} Supplemental Brief for the United States, supra note 138, at 28.

\textsuperscript{150} 50 U.S.C. § 1809(a)(2).

\textsuperscript{151} Id. § 1804(a)(4).

\textsuperscript{152} Id. § 1801(b) (emphasis added).

\textsuperscript{153} Id.

\textsuperscript{154} Id.
4. Establishment of the Foreign Intelligence Surveillance Court and Court of Review

As a further precaution against executive overreach, Congress provided in FISA for two courts: the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review (FISC). As aforementioned, a key principle throughout the debates was the importance of heightened protections where U.S. persons' information may be involved. The conference was deadlock on how best to accomplish this, until the Senate receded and accepted the House language exempting certain particularly sensitive surveillance (that is, relating solely to foreign powers) from judicial review. The decision rested on the grounds that (1) such surveillance did not involve U.S. persons; and (2) having removed the most sensitive information from external review, the Foreign Intelligence Surveillance Court could be given a greater role in protecting the rights of each U.S. person targeted by the government. The use of a judicial element went some way towards providing for an independent, neutral, disinterested magistrate to review the strength of the government's case supporting the initiation of surveillance.

Initially, the statute provided for seven judges to sit on FISC. That number has since expanded to include eleven judges drawn from at least seven of the federal circuits, three of whom must reside in the Washington, D.C. area. Both the FISC judges and the judges on FISC are selected by the Chief Justice of the U.S. Supreme Court. To avoid agency capture, judges only may serve for up to seven years, at the conclusion of which they are not eligible to serve again as FISC judges.

From the beginning, FISC's role was limited: it was merely to grant or to deny applications for orders. The statute included detailed instructions about what must be included in such applications: the identity of the federal officer making the application; the identity, if known, of the target; a statement of the facts and circumstances relied upon to justify the applicant's belief that the target is a foreign power or an agent of a foreign power and that each of the facilities or places at which electronic surveillance is directed is being (or about to be) used by a foreign power or an agent thereof; a statement of the proposed minimization procedures; a description of the nature of the information sought; a certification from an executive branch official; a summary statement of the means by which the surveillance will be effected; a statement of the facts concerning all previous applications; and a statement of the period of time for which the surveillance is required to be maintained.

Where the government has met the necessary criteria, the judge's role is to enter an ex parte order as requested or to modify it accordingly. Initially, such orders could be issued only in relation to electronic surveillance. Subsequent amendments expanded FISC's jurisdiction to physical searches, pen registers and trap and trace devices, searches of business records, and tangible things. These alterations, however, were in substance and not in form. The function being performed by FISC throughout was the same: to grant or to deny orders prior to the acquisition of information on particular targets.

C. Subsequent Amendment

Since FISA's introduction, Congress has amended the statute to cover physical searches, pen register and trap and trace devices, searches of business records, and tangible goods.

158. Id. § 1803(a)(1)(B).
159. Id. § 1803(c).
160. Id. § 1803(c).
161. Id. § 1801(a).
162. Id. §§ 1821-1824 (orders for physical search); id. § 1862 (pen register and trap and trace devices); id. § 1861 (business records and tangible goods).
165. Id. §§ 402, 412, Stat. at 2405.
166. Various further amendments to these sections have been enacted. The USA PATRIOT Act, for instance, changed the duration of certain FISA authorization orders (§ 207), increased the number of FISC judges to 11 (§ 208), amended FISA pen register and trap and trace provisions (§ 214), changed the purpose of electronic & physical searches (§ 218), and authorized coordination between intelligence and law enforcement (§ 504). Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA
Because of their consistent structure and approach, these provisions have come to be referred to collectively as "traditional FISA." A brief discussion of the subsequent amendments helps to underscore Congress's general approach and to elucidate ways in which the bulk collection of U.S. persons' metadata violates the orientation of the statute and, as addressed in Part II, the statutory language.

I. Physical Search, Pen-Trap

Similar to the electronic surveillance provisions, physical search orders under FISA are limited by the requirement that the government establish the target of the search before acquiring the information. Specifically, physical search orders may be used only to target "premises, information, material, or property used exclusively by, or under the open and exclusive control of, a foreign power or powers." The subsection adopts the same definitions of "foreign power," "agent of a foreign power," "international terrorism," "sabotage," "foreign intelligence information," and "United States person" as used elsewhere in the statute. It provides for FISC to grant or deny orders consistent with FISC's role in electronic surveillance.


367. See, e.g., J. DAVID S. KROWN & D. WILLIAM R. NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS, ch. 12 (3rd ed. 2012). In addition to the aforementioned amendments, in 2001 Congress amended FISA to take account of, among others, USA PATRIOT Act § 202, 115 Stat. at 293 (amending § 105A(2) of the Foreign Intelligence Surveillance Act of 1978, codified as amended at 50 U.S.C. § 1881a(2)(B)). This alteration reflected a change that had been integrated into criminal law measures in 1999. At that time, the House Conference Report explained:

Under current law, judges issue warrant orders authorizing law enforcement officials to place a wiretap on a specific telephone number. Law enforcement officials, including terrorists and spies, know this and often try to avoid wiretaps by using pay phones on the street or public places or by using stolen or disposable cell telephones. As law enforcement officials cannot know the numbers of these telephones in advance, they are unable to obtain a warrant order on those numbers from a judge in time to intercept the conversation, and the criminal is able to evade interception of his communications.


169. Id. § 1822(a)(1).
170. Id. § 1822(b).

No. 3]

Bulk Metadata Collection

The government must make the same showings, particularly describing the target prior to FISC granting the order. Heightened protections are afforded to U.S. persons.

In 1998, Congress amended FISA to allow for the installation and use of pen register (recording numbers dialed from a particular phone) and trap and trace devices (acting as a caller ID record). The Attorney General, or a designated attorney, must submit an application in writing and under oath either to FISC or to a magistrate specifically appointed by the Chief Justice to hear pen register or trap and trace applications on behalf of the FISA court. Similar to the provisions related to electronic communications and physical search, the application must include information to show that the device has been, or will be in the future be, used by someone who is engaging, or has engaged, in international terrorism or is a foreign power or agent thereof. In the event of an emergency, the Attorney General can authorize the installation and use of a pen register or trap and trace device without judicial approval. Nevertheless, a proper application must be made to the appropriate judicial authority within seven days.

Following the 9/11 attacks, Congress relaxed the requirement for factual proof for placement of a pen or trap. The applicant no longer must demonstrate why he or she believes that an individual engaged in international terrorism will use a telephone line. Instead, the applicant must demonstrate only that the information likely to be gained does not directly concern a...
U.S. person and will be relevant to protection against international terrorism.\footnote{United States v. United States District Court for the Eastern District of Virginia (2001).} This provision, hotly contested by civil libertarians, was scheduled to sunset on December 31, 2005,\footnote{Philip Elmer-Dewitt, "The USA PATRIOT Act: A Primer," The New York Times, October 22, 2003.} but in 2006 Congress made it permanent.\footnote{Nathan Weisinger, "The USA PATRIOT Act: A Primer," The New York Times, October 22, 2003.} Although the provision relaxes the standard for obtaining information from particular telephone lines, it still establishes a higher bar for obtaining U.S. person’s information. The statute understands the terms “pen register” and “trap and trace device” consistent with the criminal law standard defining a pen register as:

[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.

A “trap and trace device” is defined as:

[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.

In addition to all dialing, routing, addressing, and signaling information sent from or received by a target, orders may require electronic communication service providers to disclose further information, including:

1. the name of the customer or subscriber;
2. the address of the customer or subscriber;
3. the telephone or instrument number, or other subscriber number or identifier, of the customer or subscriber.

These provisions are consistent with Congress’s approach in FISA: namely, particularized showing in relation to the target, a decision prior to the collection of information, issuance of an individualized order by the court, and heightened protections for U.S. persons.

2. Business Records, Tangible Goods, and Section 215

Following the Oklahoma City bombing, in 1998 Congress amended FISA to authorize the production of certain kinds of business records of those suspected of being foreign powers or agents of a foreign power: namely, documents maintained by common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities.\footnote{30 U.S.C. § 1827(f).} Any records obtained under this provision had to be for “an investigation to gather foreign intelligence information or an investigation concerning international terrorism.”\footnote{30 U.S.C. § 1821(8).} The application had to include “specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power.”\footnote{30 U.S.C. § 1821(8).}

As with the other provisions of traditional FISA, Congress assigned the term “foreign power,” “agent of a foreign power,” \footnote{30 U.S.C. § 1827(f).}
"foreign intelligence information," and "international terrorism" the same meanings as employed in relation to electronic surveillance. Congress also required intelligence agencies to follow the same steps as those taken with regard to electronic surveillance (i.e., to submit an application to FISC to obtain an order, which then compels the companies to hand over the records). Initially, the FBI did not heavily rely on the business records provision. Between 1998 and 2001, the FBI used it only once. Nevertheless, in 2001 Congress expanded the types of records that could be obtained, authorizing intelligence agencies to apply for an order from FISC "requiring the production of any tangible things (including books, records, papers, documents, and other items)." Congress eliminated restrictions on the types of businesses or entities on which such an order could be served. In retained, however, the general contours of FISA, specifying that such items be obtained in the course of "an investigation to protect against international terrorism or clandestine intelligence activities." Congress again added heightened protections for U.S. persons, requiring that such investigations, where directed towards a U.S. person, "not be

187. Id.
188. Id.
189. USA PATRIOT Act, Pub. L. No. 107-56, § 215, 115 Stat. 272, 397. Congress also amended FISA to require that applicants to FISC certify that "a significant purpose of the surveillance is to obtain foreign intelligence." 50 U.S.C. § 1804(a)(c)(B) (2004 & Supp. V. 2011). This shift from the prior language that "the" purpose be to obtain foreign intelligence, had the effect of removing a wall that had built up within the Department of Justice between intelligence officers and criminal prosecutors. The government argued that the latter should be allowed to advise the former concerning the initiation, operation, continuation, or expansion of FISA searches or surveillance. In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 358 F. Supp. 2d 405, 455 (E.D. Va. 2005). The Foreign Intelligence Surveillance Court of Review upheld the change. See In re Sealed Case, 315 F.3d 717 (FISA Ct. Rev. 2002). This alteration, however, simply recognizes parallels between criminal violations and national security threats. It does not suddenly shift the focus of the statute to allow intelligence agencies to collect information on citizens of America not suspected of any wrongdoing.
191. Id.
195. Id.
thirty-eight page document establishing new guidelines for national security investigations—and allowing agents to obtain business records during preliminary investigations.196

Despite the expansion to preliminary investigations, the specificity embedded in the relevance principle remained. To open a preliminary investigation, the Attorney General required in his 2003 guidelines that, inter alia, the individual targeted in the investigation be an international terrorist or an agent of a foreign power, or any individual, group, or organization engaged in activities constituting a threat to national security for, or on behalf of, a foreign power, or may be the target of a recruitment or infiltration effort by an international terrorist, foreign power, or an agent of a foreign power.197

There are two points to make about this novel construction. First, the Attorney General emphasized particular “individuals,” “groups,” or “organizations” as the targets of preliminary investigations. This was consistent with FISA’s traditional approach. Second, only once a preliminary investigation was established could agents then make use of “authorized techniques” to obtain information (e.g., mail opening, physical search, or electronic surveillance requiring judicial order or warrant).198 This meant that the target had to be determined (in the course of which the FBI would open a preliminary investigation) before orders allowing for the acquisition of tangible goods could issue.

Section 215 of the USA PATRIOT Act, the tangible goods provision, was set to expire December 31, 2005.199 Congress has since renewed it seven times.200 It is now set to expire June 1, 2015.201 In 2005, in the course of extending Section 215, Congress added language tying the section more closely to FISA’s overarching structure. It required applicants to submit a statement of facts establishing “reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment).”202 The investigation to which the order is tied must be conducted under guidelines approved by the Attorney General.203 The purpose of the investigation must be “to obtain foreign intelligence information not concerning a United States person or to protect against international ter-

197. Id. at 16.
198. Id. at 15.
rorism or clandestine intelligence activities." The underlying investigation may not be directed at a U.S. person based solely on otherwise protected First Amendment activity.

Tangible things are presumptively relevant to an investigation where they pertain to: (1) "a foreign power or an agent of a foreign power"; (2) "the activities of a suspected agent of a foreign power," themselves the subject of an authorized investigation; or (3) "an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of an unauthorized investigation." For certain materials—namely, "library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records"—with information identifying an individual, only the Director of the FBI, the Deputy Director of the FBI, or the Executive Assistant Director for National Security may make the application; none of these individuals may further delegate their authorities in this respect.

In the 2005 amendments, Congress required "an enumeration of the minimization procedures" related to the retention and dissemination of any tangible things obtained. Any orders issued "may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things." As discussed below, the telephony metadata program, by FISC's own admission, fails to satisfy this statutory requirement.

---

203 See § 1861(b)(2)(A); id. § 1861(h)(1).
204 Id. § 1861(a)(3).
205 Id.
206 Id. § 1861(c)(2)(D).
207 Any individual served with an order is entitled to tell anyone else than individuals to whom disclosure is necessary to comply with the order or an attorney to obtain legal advice or help with regard to producing the items sought. Id. § 1861(d). Under the statute, an individual on whom an order has been served may challenge the legality of the order by filing a petition with the court within a year, requesting that the order be modified or set aside. Id. § 1861(d)(2)(A)(i).

---

D. Broad Surveillance in Place of Particularization

The telephony metadata program lacks the particularization that marks Congress's approach to domestic foreign intelligence gathering in FISA. The statute rejects the wholesale collection of domestic information. It relies on the prior targeting of foreign intelligence targets to justify surveillance. It provides U.S. persons a heightened level of protection. And it seeks to minimize the acquisition (not just the retention and dissemination) of information.

I. Wholesale Collection of Information

Project MINARET, which represented precisely the type of surveillance program that FISA was designed to forestall, was not nearly as extensive as the telephony metadata program. Over the course of Project MINARET, for instance, the watch list included approximately 1650 U.S. citizens in total. At no time were there more than 800 U.S. citizens' names on the list, out of a population of about 200 million Americans.

Today, in contrast, there are approximately 316 million Americans, a significant number of which have access to mobile devices. Verizon, which is only one of the telecommunications companies served with a FISC order, is estimated to have a market share of 31.3% of the total number of wireless subscribers. As of October 2013, this translated into 101.2 million wireless accounts. This number eclipses the total number of U.S. citizens subject to the most egregious programs previously operated by the NSA, which gave rise to FISA in the first place.

The telephony program also goes substantially beyond the previous surveillance operation in its focus on calls of a purely

---

211 5 Church Committee Report, supra note 30, at 33 (testimony of Lieutenant General Lew Allen, Jr., Director, National Security Agency).
212 Id. at 30, 33–34.
214 Kyle Woodyard, Does Verizon Have a Bud Monopoly?, INVESTORPLACE (Jan. 14, 2013), [http://investorplace.com/2013/01/does-verizon-have-a-bud-monopoly/]; id. (UVD+AVN);
local nature. According to the Director of the National Security Agency, Project MINARET did not monitor entirely domestic conversations. The FISC Order issued in April 2013, however, specifically requires the collection of information "wholly within the United States, including local telephone calls."217 Set to expire on July 19, 2013, the Office of the Director of National Intelligence has confirmed that FISC has again renewed the order.218

As discussed above, Congress designed the statute to be used in specific cases of foreign intelligence gathering. By limiting the targets of electronic surveillance, requiring probable cause, disallowing investigations solely on the basis of otherwise protected First Amendment activities, and insisting on minimization procedures, Congress sought to restrict agencies' ability to violate U.S. citizens' privacy. The business records provision built on this approach, adopting the same definitions that prevailed in other portions of the statute and requiring that agencies obtain orders to collect information on individuals believed to be foreign powers or agents of a foreign power. Congress later deliberately inserted "relevant" into the statute to ensure the continued specificity of targeted investigations.

In addition, Congress empowered FISC to consider each instance of placing an electronic wiretap. The NSA's program, in contrast, deleges such oversight to the Executive, leaving all further inquiries of the databases to the agency involved. Once the NSA collects the telephony metadata, it is the NSA (not FISC) that decides which queries to use, and which individuals to target within the database.

This change means that FISC is not performing its most basic function: protecting U.S. persons from incursions into their privacy. Instead, it leaves the determination of whom to target to the agency's discretion. Traditional FISA depends upon the criteria in the statute being met before collection of information.

---

216. See S Church Committee Report, supra note 26, at 26.

---

219. See, e.g., Eric H. Holder, Jr., Acting General of the United States, 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 1 (Jan. 8, 2007), available at http://www.justice.gov/opa/ag/holder/minimization.pdf. (“Acquisition means the collection by NSA or the FBI through electronic means of a non-public communication to which it is not an intended party.”)

220. SECTION 215 WHITE PAPER, supra note 2, at 1.
221. Id. at 4 (“It would be impossible to conduct these queries effectively without a large pool of telephony metadata to search, as there is no way to know in advance which numbers will be responsive to the authorized queries.”).
3. No Higher Threshold for U.S. Persons

In addition, as detailed above, there are myriad ways in which FISA creates extra protections for U.S. persons. In light of the historical context, the reason for this is clear. The statute arose from revelations about the cavalier manner in which the intelligence agencies were treating Americans’ right to privacy. New protections thus centered on creating higher standards for targeting U.S. persons, as well as for later analysis and dissemination of U.S. persons’ information.

Outside of minimization procedures relating to the downstream manipulation and dissemination of information, however, the telephony metadata program does not recognize a higher protection for U.S. persons at the moment of data acquisition. The failure to create higher standards thus runs counter to the approach Congress adopted in passing FISA.

6. Role of the Foreign Intelligence Surveillance Court

In at least three important ways, FISC no longer serves the purpose for which it was designed. First, Congress created the court to determine whether the executive branch had met its burden of demonstrating that there was sufficient evidence to target individuals within the United States, prior to collection of such information. The telephony metadata program demonstrates that FISC has abdicated this responsibility to the executive branch generally, and to the NSA in particular. Continued noncompliance underscores concern about relying on the intelligence community to protect the Fourth Amendment rights of U.S. persons.

Second, Congress did not envision a lawmaking role for FISC. Its decisions were not to serve as precedent, and FISC was not to offer lengthy legal analyses, crafting in the process, for instance, exceptions to the Fourth Amendment warrant requirement or defenses of wholesale surveillance programs.

Third, questions have recently been raised about the extent to which FISC can fulfill the role of being a neutral, disinterested magistrate. Congress went to great lengths, for instance, to try to ensure diversity on the court. To the extent that the appointments process implies an ideological predilection, at a minimum, it is worth noting that almost all of the judges who serve on FISC and FISCR are Republican appointees. The rate of applications being granted, in conjunction with the in cam-

era and ex parte nature of the proceedings, also raises questions about the extent to which FISC serves as an effective check on the executive branch. The lack of technical expertise of those on the court further introduces questions about the judges’ ability to understand how the authorities they are extending to the NSA are being used.

1. Reliance on NSA to Ascertain Reasonable, Articulable Suspicion

In 1978 Congress created FISC to serve as a neutral, disinterested observer. In this capacity, one of its principal responsibilities was to ascertain whether the government had demonstrated probable cause that individuals to be targeted under FISA were foreign powers or agents thereof, and likely to use the facilities to be placed under surveillance. As was previously discussed, consistent with this approach, in 1998 Congress introduced the business records provision, requiring in the process that the government submit a statement of “specific and articulable facts” to the court in support of its application. Although the showing was eliminated in 2001, four years later Congress re-introduced a requirement that the government submit a statement of facts establishing “reasonable grounds to believe that the tangible things to be obtained are ‘relevant to an authorized investigation.’” This language puts the court in the position of verifying whether the government has met its burden of proof prior to intelligence collection. The court, however, no longer serves in this function.

To the contrary, FISC’s primary order authorizing the collection of telephony metadata required that designated NSA officials make a finding that there is “reasonable, articulable suspicion” (RAS) that a seed identifier proposed for query is associated with a particular foreign terrorist organization prior to its use. It is thus left to the executive branch to determine whether the executive branch has sufficient evidence to place individuals or entities under surveillance.

The dangers associated with the court removing itself from the process are clear. Documents recently released under court orders in a related FOIA case establish that for nearly three
years, the NSA did not follow these procedures—
even though numerous NSA officials were aware of the violation. Noncompliance incidents have continued. Collectively, these incidents raise serious questions as to whether FISC is performing the functions for which it was designed.

e. Failure to Report Initial Noncompliance

Although the NSA had been contravening the order since May 2006, it was not until early 2009, when representatives of the Department of Justice met with NSA representatives to be briefed on the NSA’s handling of the telephony metadata, that the illegal behavior was brought to FISC’s attention. President Barack Obama took office on January 20, 2009; it appears that recognition of the noncompliance occurred during the transition. During the briefing and in subsequent discussions, DOJ representatives inquired about the alert process. Learning of the process being used, DOJ personnel expressed concern that the program had been misrepresented to FISC. The NSA had been using identifiers employed to collect information under Executive Order 12,333—not FISA—to search the telephony database. This meant that the standards applying to foreigners were used in relation to U.S. persons.


When executing its SIGINT mission, NSA is only authorized to collect, retain, or disseminate information concerning U.S. persons consistent with Attorney General guidelines. The current procedures approved by the Attorney General are located in the Department of Defense, Regulation 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons 24-37, as well as a classified annex to the regulation overturning the NSA’s electronic surveillance. Declaration of Lieutenant General Keith B. Alexander at 34, In re Prod. of Tangible Things from (REDACTED), No. BR 06-13 (D.C. Cir. Feb. 13, 2009), available at http://www.dni.gov/files/documents/section/pub_f06%2012%2009%20Memorandum%204%20%5F01%20%5F05.pdf [http://perma.cc/07TH/KbJg].

To administer the program, the NSA constructed two lists: the first, an “alert list,” included all identifiers (foreign and domestic) of interest to counterintelligence analysts. Memorandum of the United States in Response to the Court’s Order Dated Jan. 28, 2009 at 10, In re Prod. of Tangible Things from (REDACTED), No. BR 06-13 (D.C. Cir. Feb. 17, 2009), available at http://www.dni.gov/files/documents/section/pub_f06%2012%2009%20Memorandum%204%20%5F01%20%5F05.pdf [http://perma.cc/TJ4U/W9K2]. The second, the “station list,” is a historical listing of all telephone identifiers that had undergone a reasonable, articulable suspicion determination, including the results. In re Declaration of Lieutenant General Keith B. Alexander at 19, In re Prod. of Tangible Things from (REDACTED), No. BR 06-13 (D.C. Cir. Feb. 17, 2009), available at http://www.dni.gov/files/documents/section/pub_f06%2012%2009%20Memorandum%204%20%5F01%20%5F05.pdf [http://perma.cc/TJ4U/W9K2].
The DOJ informed FISC within a week of the meeting that the government had been querying the business records in a manner that contravened both the original order and sworn statements of several executive branch officials. FISC was not amused. Judge Reggie Walton expressed concern "about what appears to be a flagrant violation of its Order in this matter." The NSA had repeatedly misled FISC in its handling of the database. FISC immediately issued an order, directing the NSA to comprehensively review the agency's handling of telephony metadata. It gave the government until February 17, 2009 to file a brief to defend its actions and to help FISC to determine whether further action should be taken against the government or its representatives.

The NSA initially admitted only "that NSA's description to [FISC] of the alert list process... were inaccurate and that the Business Records Order did not provide the Government with authority to employ the alert list in the manner in which it did." It further acknowledged "the majority of telephone identifiers compared against the incoming SR metadata in the rebuilt alert list were not RAS-approved." The actual numbers, reported to FISC in February 2009, were staggering: as of January 15, 2009, "only 1,935 of the 17,835 identifiers on the alert list were RAS-approved."

It was not that the NSA was unaware of the requirements established by the statute and by FISC. The Attorney General had, consistent with the primary order, established minimization procedures, among which was the following:

Any search or analysis of the data archive shall occur only after a particular known telephone number has been associated with [REDACTED] organization; provided, however, that a telephone number believed to be used by a U.S. person shall not be regarded as associated with [REDACTED] solely on the basis of activities that are protected by the First Amendment to the Constitution.

Nevertheless, apparently, neither the Signals Intelligence Directorate nor the Office of the General Counsel had caught the fact...
that nearly ninety percent of the queries to the bulk dataset had been illegal.237 Nor had they realized that their reports to FISC claiming that only RAS-approved numbers were being run against the bulk metadata were false.238

Meanwhile, the NSA had disseminated 275 reports to the FBI as a result of contact chaining and queries of NSA’s archive of telephony metadata.239 Thirty-one of these had resulted directly from the automated alert process.240 In a careful use of language, the government noted, “NSA did not identify any report that resulted from the use of a non-RAS-approved ‘seed’ identifier.”241 The government did not detail how complete the NSA had been in considering the reports; nor did it claim that none of the reports had resulted from non-RAS-approved identifiers.242 The government also did not address the dissemination of metadata reports within NSA and subsequent actions that resulted from the process.

Despite the gross violation of FISC’s order, the government argued that FISC should neither rescind nor modify its order. As required by FISC, the NSA had undertaken an end-to-end system engineering and process review (technical and operational) of its handling of business records metadata; it had undertaken a review of domestic identifiers to ensure that they are RAS-compliant; and it had undertaken an audit of all queries made of the business records metadata repository since November 1, 2008 with the purpose of determining if any queries had been made using non-RAS-approved identifiers.243 The NSA had again trained its employees and adopted new technologies to limit the number of “hops” permitted from an RAS-
approved seed identifier to three. The government offered to take additional steps to avoid having the program shut down, all of which amounted to involving DOJ's National Security Division more deeply in the telephony metadata program.  

b. Further Noncompliance

Although the January 2009 incident represents the first admission of noncompliance that was made public, it is far from the first—or only—time that the NSA acted outside the scope of its authority to collect records under section 215 of the USA PATRIOT Act. Recently released documents provide myriad further examples. In September 2006, for instance, the NSA's Inspector General expressed concern that the agency was collecting more data than authorized under the order. The NSA had been obtaining 16-digit credit card numbers as well as names or partial names contained in the records of operator-assisted calls.

---

245. Id. at 20.

246. See id. at 20-21 (listing under "Additional Oversight Mechanisms the government will implement": (1) NSA's OGC consulting with DOJ's National Security Division (NSD) on "all significant legal opinions that relate the interpretation, scope and/or implementation" of FISC orders related to BR 08-13; (2) NSD's OGC providing NSD with copies of the mandatory procedures; (3) NSD's OGC promptly providing NSD with copies of all formal briefing and/or training materials; (4) arranging meetings among NSA's OGC, NSD, and NSA's Director of Signals Intelligence prior to seeking renewal of the orders; (5) meetings once per period of future orders between NSA's OIG and NSD; and (6) review and approval of all proposed automated query processes prior to implementation).


248. See OFFICE OF THE INSPECTOR GEN., supra note 1, at 2-3 (see page 95-96 of 1446 and 1862 Production, Mar. 5, 2009). ("[M]anagement controls do not provide reasonable assurance that NSA will comply with the following terms of the Order: "NSA may obtain telephony metadata, which includes comprehensive communications, routing information, including but not limited to session identifying information, trunk identifier, and time and duration of a call. Telephony metadata does not include the substantive content of any communications, or the name, address, or financial information of a subject of an inquiry.")

249. See id. at 3 (see page 96 of 1446 and 1862 Production, Mar. 5, 2009).

later emerged that an over-collection filter inserted in July 2008 failed to function. On October 17, 2008, the government reported to FISC that, after FISC authorized the NSA to increase the number of analysts working with the business records metadata, and had directed that the NSA train the newly-authorized analysts, thirty-one (out of eighty-five) analysts subsequently queried the business records metadata in April 2008 without even being aware that they were doing so. The upshot was that NSA analysts used 2373 foreign telephone identifiers to query the business records metadata without first establishing reasonable, articulable suspicion. Despite taking corrective steps, on December 11, 2008, the government notified FISC that an analyst had not installed a modified access tool and, resultantly, had again queried the data using five identifiers for which no RAS standard had been satisfied. Just over a month later, the government informed FISC that, between December 10, 2008 and January 23, 2009, two analysts had used 280 foreign telephone identifiers to query the business records metadata without first establishing RAS. The process initiated in January 2009 identified additional incidents where the NSA had failed to comply with FISC's orders. In February 2009, the NSA brought two further matters...
to FISC’s attention. The first centered on the NSA’s use of one of its analytical tools to query the business records metadata, using non-RAS-approved telephone numbers. This tool had been used since FISC’s initial order in May 2006 to search both the business records metadata and other NSA databases. Also in February 2009, the NSA notified DOJ’s National Security Division that the NSA’s audit had identified three analysts who conducted querying on the business records metadata using fourteen telephone identifiers that had not been RAS-approved before the queries.

In May 2009, two additional compliance issues arose. The first compliance incident is completely redacted. The second notes a dissemination-related problem: that the unminimized results of some queries of metadata had been “uploaded [by the NSA] into a database to which other intelligence agencies . . . had access.” According to the government, providing other agencies access to this information may have resulted in note 2, at 5 (“Since the telephony metadata collection program under Section 215 was initiated, there have been a number of significant compliance and implementation issues that were discovered . . . The incidents, and the Court’s responses, were . . . reported to the Intelligence and Judiciary Committees in great detail.”).


257. Id. at 3.


260. Id. at 3 (quoting Preliminary Notice of Compliance Incident at 2, No. 08-09-06 (FISA Ct. June 16, 2009)).
identified, is to obtain and maintain an archive of metadata that will permit these tactics to be uncovered.\textsuperscript{263}

According to FISC, the NSA had also suggested that

To be able to exploit metadata fully, the data must be collected in bulk.\ldots\ The ability to accumulate a metadata archive and set it aside for carefully controlled searches and analysis will substantially increase NSA's ability to detect and identify members of [REDACTED].\textsuperscript{264}

Because the order being sought meant, if granted, that the NSA would be collecting call detail records of U.S. persons located within the United States, who were not themselves the target of any FBI investigation and whose metadata could not otherwise be legally obtained in bulk, FISC had adopted minimization procedures. It had required, inter alia, that:

[Access to the archived data shall occur only when NSA has identified a known telephone identifier for which, based on the factual and practical considerations of everyday life on which a reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the telephone identifier is associated with [REDACTED]].\textsuperscript{265}

FISC had a difficult time believing the NSA's claim that its non-compliance with FISC's orders resulted from NSA personnel believing that FISC's restrictions on access to the business records metadata only applied to "archived data" (that is, data located in certain databases). "That interpretation of [FISC's] Orders," Judge Reggie Walton wrote, "strains credulity."\textsuperscript{266} The NSA had compounded its bad behavior by repeatedly submitting inaccurate descriptions of how it developed and used the alert list process.\textsuperscript{267}

In support of its claim that the program was vital for U.S. national security, the NSA had offered as evidence the paltry claim that, after nearly three years of sweeping up all telephony metadata, the NSA had generated 275 domestic security reports that, in turn, had spurred three preliminary investigations.\textsuperscript{268}

FISC objected to the government's assertion that FISC "need not take any further remedial action."\textsuperscript{269} FISC has also noted that, until the NSA has completed the review, "[FISC] sees little reason to believe that the most recent discovery of a systemic, ongoing violation—on February 18, 2009—will be the last."\textsuperscript{270}

Accordingly, starting in March 2009, though the NSA could continue to collect data and to test the telephony metadata system, it would only be allowed to query it with a FISC order—or, in an emergency, to query the database and then to inform FISC by 5:00 PM, Eastern Time, on the next business day.\textsuperscript{271} In September 2009, however, FISC lifted the requirement for the NSA to seek approval in every case.\textsuperscript{272}

The second protection FISC introduced was, starting on July 3, 2009, to require the NSA to file a weekly report with FISC, listing each time, over the seven-day period ending the previous Friday, in which the NSA had shared, "in any form, information obtained or derived from the [REDACTED] BR metadata collec-

\textsuperscript{263} Id. at 6.

\textsuperscript{264} Id. at 13 ("The mere commencement of a preliminary investigation, by itself, does not seem particularly significant\ldots\ The time has come for the government to describe to the Court how, based on the information collected and analyzed during the duration of the program, the value of the program to the national security.

\textsuperscript{265} Id. at 3 (emphasis omitted) ("promptly or as soon as practicable, [FISC] will establish a system to allow the Director of National Intelligence to review and approve NSA's classification procedures.

\textsuperscript{266} Id. at 5.
tions with anyone outside the NSA. Again, consistent with traditional FISA, FISC added special protections for U.S. persons:

For each such instance, the government shall specify the date on which the information was shared, the recipient of the information, and the form in which the information was communicated (e.g., written report, email, oral communication, etc.). For each such instance in which U.S. person information has been shared, the Chief of Information Sharing of NSA’s Signals Intelligence Directorate shall certify that such official determined, prior to dissemination, the information to be related to counterterrorism information and necessary to understand the counterterrorism information or to assess its importance. 274

In August 2009, the government submitted its end-to-end assessment of the NSA telephony metadata system. 275 FISC lifted its requirements, leaving future dissemination decisions up to the NSA. Whether the requirements with which the NSA was left effectively check the exercise of authorities is questionable. Before the dissemination of information of U.S. persons’ information outside the Agency, an NSA official must determine that the information is “related to counterterrorism information and is necessary to understand the counterterrorism information or assess its importance.” 276 Because the government already considers all of the information in the database to be relevant to counterterrorism investigations, and has already argued to FISC (and FISC has agreed), that the collection of such data is necessary to understand its counterterrorism information, the degree to which this restriction really prevents such dissemination is open to question.

274. Id.
276. SECTION 215 WHITE PAPER, supra note 3, at 5.

No. 3] Bulk Metadata Collection

d. Technological Gap

A critical part of FISC’s failure to provide effective oversight of the process relates to FISC’s decision to have the NSA perform the targeting decision. Part of the problem also stems from FISC’s discomfort with the technological aspects of the collection and analysis of digital information. For much of the discussion of noncompliance incidents, for instance, it appears that neither the NSA nor FISC had an adequate understanding of how the algorithms operate. Nor did they understand the type of information that had been incorporated into different databases, and whether they had been subjected to the appropriate legal analysis before data mining.

A similar problem may accompany the reporting requirements to Congress. In March 2009, for example, the DOJ submitted several FISC opinions and government filings—relating to the discovery and remediation of compliance incidents in its handling of bulk telephony metadata—to the Chairman of the Intelligence and Judiciary Committees. 277 A subsequent letter noted that the House and Senate Intelligence and Judiciary Committees had received briefings in March, April, and August before receiving a copy of the NSA’s review in September 2009. 278 To the extent that the representatives of the agency are

heavily dependent on technical knowledge, the implications
may not be readily apparent to lawmakers.

2. Issuance of Detailed Legal Reasoning and Creation of Precedent

To enforce the specialized probable cause standard encapsulated
in FISA, Congress created a court of specialized but ex-
clusive jurisdiction. Its job was to ascertain whether sufficient
probable cause existed for a target to be considered a foreign
power, or an agent thereof, whether the applicant had provid-
ed the necessary details for the surveillance; and whether the
appropriate certifications and findings had been made.

It is thus surprising that the government considers these or-
ders now to be evidence of precedent, on the basis of which, it
argues, the programs are legal. In ACLU v. Clapper, for in-
stance, the government responded to the argument that it had
exceeded its statutory authority under FISA by arguing:

[Since May 2006, fourteen separate judges of the FISC have
concluded on thirty-four occasions that the FBI satisfied this
requirement, finding “reasonable grounds to believe’’ that
the telephony metadata sought by the Government “are rele-
vant to authorized investigations . . . being conducted by the
FBI . . . to protect against international terrorism.”

The government went on to cite Judge Eagan’s August 2013
memorandum opinion in further support of its interpretation
of “relevance.” These were the only points of reference that
mattered: “Considering that the Government has consistently
demonstrated the relevance of the requested records to the
FISC’s satisfaction, as Section 215 requires, it is difficult to un-
derstand how the government can be said to have acted in ex-
cess of statutory authority.”

---

275. Theodore W. Ruger, Chief Justice Rehnquist’s Appropriations in the FISA Court:
281. Defendants’ Memorandum of Law in Opposition to Plaintiff’s Motion for a
Preliminary Injunction at 16, Clapper, 959 F. Supp. 3d 724, available at
282. Id.
283. Id.
284. See Eric Lichtblau, In Secret, Court Vitiates Broadest Powers of N.S.A., N.Y.
285. In re Direcns (REDACTED) Pursuant to Section 1(a) of the Foreign Intel-
286. Id.
287. Id. at 1009.
that this type of foreign intelligence surveillance possesses characteristics that qualify it for such an exception.\textsuperscript{288}

The court analogized the exception to the 1989 Supreme Court consideration of the warrantless drug testing of railway workers, on the grounds that the government’s need to respond to an overriding public danger could justify a minimal intrusion on privacy.\textsuperscript{289} The government subsequently cited in its August 9, 2013 white paper, defending the telephony metadata program, in support of an exception to the Fourth Amendment warrant requirement.\textsuperscript{290}

FISC continues to go beyond its mandate. In August 2013, for instance, FISC issued a twenty-nine-page Amended Memorandum Opinion regarding the FBI’s July 18, 2013 application for the telephony metadata program.\textsuperscript{291} Appendixing the seventeen-page order to the opinion, Judge Claire V. Eagan considered Fourth Amendment jurisprudence, the statutory language of Section 215, and the canons of statutory construction to justify granting the order.\textsuperscript{292} Similarly, in a 2002 per curiam opinion, FISC suggested the case raised “important questions of statutory interpretation, and constitutionality” and concluded “that FISA, as amended by the Patriot Act, supports the government’s position, and that the restrictions imposed by the FISA court are not required by FISA or the Constitution.”\textsuperscript{293}

Congress did not design the Foreign Intelligence Surveillance Court or the Court of Review to develop its own jurisprudence. Particularly in light of the secrecy and lack of adversarial process inherent in the court, it is concerning that FISC’s decisions have taken on a force of their own in legitimizing the collection of information on U.S. citizens.

\textsuperscript{288} Id. at 1011.
\textsuperscript{289} Id. at 1010–11.
\textsuperscript{290} SECTION 215 WHITE PAPER, supra note 2, at 15.
\textsuperscript{292} Id. at 28–29.
\textsuperscript{293} In re Sealed Case, 310 F.3d 717, 719–20 (FISA Ct. Rev. 2002).
decisions reached by FISC judges appointed by one party with decisions reached by judges appointed by the opposing party.

Such studies would be almost impossible to conduct. FISC opinions are classified. Beyond this, they are sui generis; in that FISC is the only court that considers FISA applications. It also may be that externalities influence which judges opt for FISC membership. That is, more Republican appointees than Democratic appointees may inquire or make clear that they would be interested in serving on FISC. No studies have yet been conducted demonstrating why the appointments process aligns with political party, making any conclusions as to the effect somewhat arbitrary.

To the extent that political ideology enters into the equation, the way in which it has interacted with the court’s role in establishing precedent deserves notice, as it undermines the appearance of a neutral arbiter and emphasizes deference to and support for greater power for the executive. According to the public record, FISC, for instance, has only met twice: once in 2002 and once in 2003.39 On both occasions, the panels consisted entirely of Republican appointees, some of whom had publicly argued that FISA was an unconstitutional usurpation of executive power.

Judge Laurence Silberman of the D.C. Circuit testified to Congress in 1978 (when FISA was being debated) that the legislation violated the Constitution.40 Judge Silberman, who had previously served as Deputy Attorney General, was "absolutely convinced that the administration bill, if passed, would be an enormous and fundamental mistake which the Congress and the American people would have reason to regret."41 For Judge Silberman, the judiciary’s role in any national security electronic surveillance should be circumscribed. He explained:

---

299. See In re Directive [REDACTED] Pursuant to Section 1058 of Foreign Intelligence Surveillance Act, 551 F.3d 164 (FISA, Ct. Rev. 2008); In re Sealed Case, 310 F.3d 717.
301. Id. at 219.
302. Id.
303. Id.
305. See generally id.
especially in regard to some of the most important and far-reaching secret decisions issued by the court—raises important questions about the extent to which FISC, as conceived by Congress, is serving as a neutral arbiter. Without more detailed information about the judicial process, however, the extent to which this is the case remains in question.

**FIGURE 1: JUDGES APPOINTED TO THE FOREIGN INTELLIGENCE SURVEILLANCE COURT AND COURT OF REVIEW BY ORIGINAL APPOINTMENT TO THE BENCH**

<table>
<thead>
<tr>
<th>District Judge</th>
<th>Court</th>
<th>Dates of appointment</th>
<th>Appointing President</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raymond J. Dzarie*</td>
<td>FISC</td>
<td>7/2/2012–7/1/2019</td>
<td>Ronald Reagan</td>
</tr>
<tr>
<td>William C. Bryson**</td>
<td>FISC</td>
<td>12/1/2011–5/18/2018</td>
<td>Bill Clinton</td>
</tr>
<tr>
<td>Jennifer B. Coffman</td>
<td>FISC</td>
<td>5/19/2011–1/18/2013</td>
<td>Bill Clinton</td>
</tr>
<tr>
<td>F. Dennis Saylor IV*</td>
<td>FISC</td>
<td>5/19/2011–5/18/2018</td>
<td>George W. Bush</td>
</tr>
<tr>
<td>Thomas F. Hogan*</td>
<td>FISC</td>
<td>5/19/2009–5/18/2016</td>
<td>Ronald Reagan</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>FISC/M</th>
<th>Dates</th>
<th>President</th>
</tr>
</thead>
<tbody>
<tr>
<td>Michael J. Davis</td>
<td>FISC</td>
<td>5/18/1999-5/18/2006</td>
<td>Bill Clinton</td>
</tr>
</tbody>
</table>

* Denotes current members of FISC
**Denotes current members of FISCR

b. Order Rate

Augmenting concerns prompted by the lack of diversity in terms of appointments to FISC and FISCR is the rather notable success rate the government enjoys in its applications to the court. Scholars have noted that the success rate is "unparalleled in any other American court."[308] Over the first two and a half decades, for instance, FISC approved nearly every single application without any modification.[309] Between 1979 and 2003, FISC denied only three out of 16,450 applications.[310]

Since 2003, FISC has ruled on 18,473 applications for electronic surveillance and physical search (2003–2008), and electronic surveillance (2009–2012).[311] Court supporters note that a significant number of these applications are either modified or withdrawn by the government prior to FISC ruling. But even here, the numbers are quite low: 493 modifications still only come to 2.6% of the total number of applications. Simultaneously, the government has only withdrawn twenty-six applications prior to FISC ruling.[312] These numbers speak to the presence of informal processes, whereby FISC appears to be influencing the contours of applications. Without more information about the types of modifications that are being required, however, it is impossible to

---

308. Rubes, supra note 266, at 265.
310. No orders were issued which modified or denied the requested authority; every case in which the Court modified an order and authorized an activity for which court authority had not been requested.
311. See supra Figure 2.
312. Id.
gauge either the level of oversight or the extent to which FISC is altering the applications.

Critics also point to the risk of capture presented by in-camera, ex parte proceedings, and note that out of 18,473 rulings, FISC has only denied eight in whole and three in part. Whatever the substantive effect might be, the presentational impact is of note.


<table>
<thead>
<tr>
<th>Year</th>
<th>Applications</th>
<th>Approved</th>
<th>Modified</th>
<th>Denied in part</th>
<th>Denied in whole</th>
<th>Withdrawn</th>
<th>gov't</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003</td>
<td>1727</td>
<td>1724</td>
<td>79</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>2004</td>
<td>1756</td>
<td>1756</td>
<td>94</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>2005</td>
<td>2072</td>
<td>2072</td>
<td>61</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2006</td>
<td>2176</td>
<td>2176</td>
<td>73</td>
<td>1</td>
<td>0</td>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>

313. Starting in 2009, the Department of Justice began providing the breakdown of the number approved, modified, denied in part, denied in whole, or withdrawn by the government prior to the FISC ruling only for those applications involving electronic communications. Prior to that time, these numbers were combined.


315. An additional application was initially denied but later approved.


317. Of 1756 submitted, three were withdrawn prior to FISC ruling and one was readdressed.


319. Of 2072 submitted, two were withdrawn prior to FISC ruling, and one was readdressed.


321. Of 2176 submitted, five were withdrawn prior to FISC ruling.


323. Disclosures in the numbers stem in part from holdover applications and denial. Two applications, for instance, filed in 2004 were not approved until 2007.


325. Disclosures in the numbers stem in part from holdover applications and denial. Two applications filed in 2007 were not approved until 2008.


327. For the fiscal year since 2003, no numbers are available for modifications or denials for the full number of applications submitted (physical search, electronic surveillance, and combined applications). Instead, the report notes that of the 1376 total submitted in the former three categories, 1229 were related to electronic surveillance. Eight of those applications were withdrawn, one denied in whole, one denied in part, and ten were modulated, with 1320 approved. The number of applications in this building the numbers for physical search and physical search combined applications.


329. The total number of electronic surveillance, physical search, and combined applications was 1579. The report, however, notes that the electronic applications (1312), and provides breakdowns for modifications, denials, etc., for the category overall. Of the 1312, five were withdrawn by the government prior to FISC ruling.


331. Note that there were 1745 total applications that included electronic surveillance and physical searches for foreign intelligence purposes. It appears that approximately seventy of the orders related solely to physical searches, or the breakdowns for electronic surveillance is only done for the 1674. Two of the initial orders were withdrawn prior to FISC ruling.
Setting modifications aside for the moment, the deference that appears to exist regarding outright denials or granting of orders seems to extend to FISC rulings with regard to business records. Almost no attention, however, has been paid to this area. It appears that FISC has never denied an application for an order under this section. That is, of 751 applications since 2005, all 751 have been granted, as the following figure shows.

**Figure 3: Orders for the Production of Tangible Goods**

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of applications to FISC under 50 U.S.C. § 1860a(c)(2)</th>
<th>Number of applications granted by FISC</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>155</td>
<td>155</td>
</tr>
<tr>
<td>2006</td>
<td>43</td>
<td>43</td>
</tr>
<tr>
<td>2007</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>2008</td>
<td>13</td>
<td>13</td>
</tr>
</tbody>
</table>

It is important to underscore that the lack of more contextual data cautions against inferring too much from the nonexistent rate of denial. In passing the tangible goods provision, Congress tied the court’s hands, requiring FISC to grant applications once the statutory conditions are met. To the extent, then, that FISC is deferential to the executive, responsibility lies at least in part with the legislature. In addition, it is almost impossible to tell, outside of the classified world, the extent to which the court pushes back on the DOJ—not just in regard to specific orders, but in relation to broader rules and procedures, as well as in an oversight capacity. Two examples come to mind.

In 2010, John D. Bates, Presiding Judge of FISC, issued a declassified **Rules of Procedure**, requiring notice and briefing of nov-

---


el issues before the court. This document suggested that FISC would not, in the future, simply accept applications in new areas of the law without first considering the underlying legal issues.

Second, the recently-released judicial opinions from 2009 suggest that FISC was pressuring the NSA with regard to its failure to ensure that the identifiers run against the database be subjected to a test of reasonable, articulable suspicion. The court was clearly uncomfortable with the pattern of misinformation that had marked the government’s previous representations to FISC. But, these same documents also reveal the extent to which the court relies on the NSA to police its own activities—again raising questions about the extent to which FISC adequately performs its envisioned role. As a final note, it is important to recognize that the sheer volume of the numbers associated with the tangible goods provisions (751) is remarkable in part because any one order could result in the collection of millions of records on millions of people, as we have seen with the telephony metadata program. In light of the in camera, ex parte proceedings, these numbers raise further questions about FISC’s role.

II. BULK COLLECTION AND FISA’S STATUTORY PROVISIONS

The telephony metadata program violates FISA’s express statutory language in three areas: first, with regard to the language “relevant to an authorized investigation”; second, in relation to the requirement that the information sought be obtainable under subpoena duces tecum; and third, in its violation of the restrictions specifically placed on pen registers and trap and trace equipment.

A. “Relevant to an Authorized Investigation”

The government argues that the NSA’s telephony metadata program is consistent with the language of 50 U.S.C. § 1861 in that all telephone calls in the United States, including those of a wholly


464. 5048. UNITED STATES v. ISMAIL, 641 F.3d 1285 (D.C. Cir. 2011).
465. 5049. Id. at 1.
466. 5050. Id. at 2.
467. 5051. Id. at 3.
468. 5052. Id. at 4.

local nature, are “relevant” to foreign intelligence investigations. The word “relevant” itself, the administration states, “is a broad term that connotes anything [b]earing upon, connected with, [or] pertinent to a specified subject matter.” Turning to its “particularized legal meaning,” the government argues:

It is well-settled in the context of other forms of legal process for the production of documents that a document is ‘relevant’ to a particular subject matter not only where it directly bears on that subject matter, but also where it is reasonable to believe that it could lead to other information that directly bears on that subject matter.

That massive amounts of data may be involved is of little import:

Courts have held in the analogous contexts of civil discovery and criminal and administrative investigations that “relevance” is a broad standard that permits discovery of large volumes of data in circumstances where doing so is necessary to identify much smaller amounts of information within that data that directly bears on the matter being investigated.

Applied to the telephony metadata program, though recognizing that the telephony metadata program is “broad in scope,” the government argues that there are nevertheless “reasonable grounds to believe” that the category of data (i.e., all telephone call data), when queried and analyzed, “will produce information pertinent to FBI investigations of international terrorism.” For communications data, the government argues, connections between individual data points can only be reliably identified through large-scale data mining. As DOJ explained to Congress: “The more metadata NSA has access to, the more likely it is that NSA can identify, discover and understand the network of contacts linked to targeted numbers or addresses.”

464. SECTION 215 WHITE PAPERS, supra note 2, at 9 (quoting 13 THE OXFORD ENGLISH DICTIONARY 561 (2d ed. 1989)).
465. Id.
466. Id. at 1-2.
467. Id. at 2.
468. Id. at 3.
There are two sets of responses to the government's arguments. The first centers on the government's claim that all telephony metadata is relevant. The second concerns the connection in the statutory language between the relevance of the information to be obtained and "an authorized investigation."  

1. Relevance Standard

Four legal arguments undermine the government's claim that there are "reasonable grounds" to believe that hundreds of millions of daily telephone records are "relevant" to an authorized investigation. First, the NSA's interpretation of "relevant" collapses the statutory distinction between relevant and irrelevant records, thus obviating the government's obligation to discriminate between the two. Second, this reading renders meaningless the qualifying phrases in the statute, such as "reasonable grounds." Third, the government's interpretation establishes a concerning legal precedent. Fourth, the broad reading of "relevant" contravenes congressional intent.

First, in ordinary usage, something is understood as relevant to another thing when a demonstrably close connection between the two objects can be established. This is also the way in which courts have consistently applied the term to the collection of information—such as grand-jury subpoenas, where the information collected must bear some actual connection to a particular investigation.

In other words, most of the information being collected does not relate to any individuals suspected of any wrongdoing. In defense of its broad interpretation, the government argues that it must collect irrelevant information to ascertain what is relevant. This means that the NSA, in direct contravention of the statutory language, is collapsing the distinction between relevant and irrelevant records—a distinction that Congress required be made before collection. Because of this collapse, the NSA is gaining an extraordinary amount of information. The records the government sought under the telephony metadata program detail the daily interactions of millions of Americans who are not themselves connected in any way to foreign power of multiple filing cabinets "without any attempt to define classes of potentially relevant documents or any limitations as to subject matter or time period.

351. See, e.g., OXFORD AMERICAN DICTIONARY 874 (3d ed. 2010) (defining relevant as "the state of being closely connected or appropriate to the matter in hand"); Merriam-Webster's Collegiate Dictionary 105 (11th ed. 2006) (defining "relevant" as "having significant and demonstrable bearing on the matter at hand"); see also Memorandum of Law in Support of Plaintiff's Motion for a Preliminary Injunction at 9–12, ACLU v. Clapper, No. 13-cv-03994 (S.D.N.Y. Aug. 26, 2013), available at https://www.aclu.org/files/attachments/clapper20130826%20AUL%20%20%20Mem%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%2
ers or agents thereof. They include private and public interactions between senators, between members of the House of Representatives, and between judges and their chambers, as well as information about state and local officials. They include parents communicating with their children's teachers, and zookeepers arranging for the care of animals. Metadata information from calls to rape hotlines, abortion clinics, and political party headquarters are likewise not exempt from collection—the NSA is collecting all telephony metadata.

Second, in addition to collapsing the distinction between relevant and irrelevant records, reading FISA to allow this type of collection would eviscerate the qualifying phrases contained in 50 U.S.C. § 1801(b)(2)(A). The statute requires, for instance, that there be "reasonable grounds" to believe that the records being sought are relevant. Although FISA does not define "reasonable grounds," the Supreme Court has treated this phrase as the equivalent of "reasonable suspicion." This standard requires a showing of "specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant" an intrusion on an individual's right to privacy.

The FISC order requires that Verizon disclose all domestic telephone records—including those of a purely local nature. According to Verizon Communications News Center, as of last year the company had 107.7 million wireless customers, connecting an average of 3 billion calls per day. It is impossible that the government provided specific and articulable facts showing reasonable grounds for the relevance of each one of those cust-
associations.” If all telephony metadata are relevant, then so are all other data—which means that very little would, in fact, be irrelevant to such investigations. If this is the case, then such an interpretation radically undermines not just the limiting language in the statute, but the very purpose for which Congress introduced FISA in the first place.

Fourth, the government’s interpretation directly contradicts Congress’s intent in adopting Section 215. At the introduction of the measure, Senator Arlen Specter explained that the language was meant to create an incentive for the government to use the authority only when it could demonstrate a connection to a particular suspected terrorist or spy. During a House Judiciary Committee meeting on July 17, 2013, Representative James Sensenbrenner (R-WI) reiterated that Congress inserted “relevant” into the statute to ensure that only information directly related to national security probes would be included—not to authorize the ongoing collection of all phone calls placed and received by millions of Americans not suspected of any wrongdoing. Soon afterwards, he wrote:

This expansive characterization of relevance makes a mockery of the legal standard. According to the administration, everything is relevant provided something is relevant. Congress intended the standard to mean what it says: The records requested must be reasonably believed to be associated with international terrorism or spying. To argue otherwise renders the standard meaningless.

Other members of Congress have made similar claims.

266. See, e.g., Oversight of the Administration’s Use of FISA Authorities: Hearing before the H. Comm. on the Judiciary, 113th Cong., 1st Sess. (July 17, 2013) (statement of Rep. Jerrold Nadler) (“[w]e removed that word from the statute, [the government] wouldn’t consider … that it would affect [its] ability to collect metadata in any way whatsoever, which is to say [it] is disregarding the statute entirely.”).

268. Id.
FISA, as noted above, makes it clear that the tangible records in question may not be sought as part of the first level of national security investigations, the assessment stage. There is an important reason for this restriction. It is the most general level and, as such, lacks the factual predicate required for the use of more intrusive techniques of information gathering.

Between 2003 and 2008, for instance, at the threat assessment stage the FBI could collect information on “individuals, groups, and organizations of possible investigative interest, and information on possible targets of international terrorist activities or other national security threats.” But the only techniques allowed, as noted by the Attorney General, were “relatively non-intrusive investigative techniques.” This included:


372. AG’S NSI GUIDELINES, supra note 370, at 3.
373. Id.

No. 3] Bulk Metadata Collection

Obtaining publicly available information, accessing information available within the FBI or Department of Justice, requesting information from other government entities, using online informational resources and services, interviewing previously established assets, non-prioritizing interviews and requests for information from members of the public and private entities, and accepting information voluntarily provided by governmental or private entities.

Nowhere in the discussion of the threat assessment stage did the 2003 guidelines contemplate the use of court-ordered surveillance.

In 2008, the Attorney General expanded the tools that could be used during the assessment stage to include: publicly available information; all available federal, state, local, tribal, or foreign governmental agencies’ records; online services and resources; human source information; interviews or requests for information from members of the public and private entities; observation or surveillance not requiring a court order; and grand jury subpoenas for telephone or electronic mail subscriber information. The addition of the last two items broadened the type of information that could be obtained. Similarly, whereas the previous guidelines noted that mail covers, mail openings, and nonconsensual electronic surveillance or any other investigative technique covered by 18 U.S.C. §§ 2510–2521 “shall not be used during a preliminary inquiry,” the 2008 guidelines dropped any equivalent language.

Even with the broadening, however, under FISA, tangible goods may not be obtained under section 215 during the assessment stage. The purpose is to place a higher burden on the government to justify the use of more intrusive surveillance. If such methods are to be used, and the related information collected,
there must be a factual predicate establishing a higher level of suspicion as to the presence of criminal activity or a threat to national security.\footnote{The guidelines explain: "A predicated investigation relating to a federal crime or threat to the national security may be conducted as a preliminary investigation or a full investigation. A predicated investigation that is based wholly on the authority to collect foreign intelligence may be conducted only as a full investigation." U.S. DEP'T OF JUSTICE, ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS, supra note 370, at 21.}

For preliminary investigations, this means that the government must have information or an allegation indicating the existence of criminal activity or a threat to U.S. national security prior to initiating the investigation.\footnote{Id.} For a full investigation, there must be "an articulable factual basis for the investigation that reasonably indicates" criminal activity or a threat to U.S. national security.\footnote{Id. at 21-22.} For an enterprise investigation (a variant of a full investigation), there must be an articulable factual basis for the investigation reasonably indicating "that the group or organization may have engaged or may be engaged in, or may have or may be engaged in planning or preparation or provision of support for" racketeering, international terrorism or other threats to U.S. national security, domestic terrorism, furthering political or social goals wholly or in part through activities that involve force or violence and a violation of federal criminal law, or a closed range of other offenses.\footnote{Id. at 23.} The guidelines thus distinguish between the different levels based on a factual predicate of wrongdoing, which then acts as a valve on the level of intrusiveness that the government can adopt in collecting more information.

In contrast, the primary order for the telephony metadata program does not follow this approach. Instead, it authorizes the collection of data for 90-day periods without any factual predicate supporting the acquisition or collection of data. It is thus incompatible with the approach adopted in the Attorney General's guidelines. The order also shifts the emphasis to the analysis of such data—which is to be conducted in connection with an authorized investigation. This is not, however, what is required by the FBI's own guidelines. It is the collection of such information that is premised on the existence of an authorized investigation—not the subsequent analysis of data in the course of the same.

b. Specificity

According to the Attorney General's guidelines, for predicate investigations (for which tangible items orders under Section 215 may be sought) specificity is required before the collection of information—namely, the investigation must be premised on the past or present wrongdoing or foreign intelligence activities of specific individuals, groups, or organizations. The telephony metadata program, in contrast, collects all call records, without specifying the individuals, groups, or organizations of interest.

For the past decade, specificity has been integral to the guidelines' approach. Under the 2003 Attorney General's guidelines, for instance, preliminary investigations were authorized "when there is information or an allegation indicating that a threat to the national security may exist."\footnote{Id. at 22.} Such investigations were particular, in that they related to specific individuals, groups, and organizations.\footnote{Id. at 23.}

Under the 2008 guidelines, a preliminary investigation must relate to "a" federal crime or threat to national security.\footnote{Id. at 4.} For foreign intelligence gathering, the guidelines require that only full investigations be used.\footnote{Id. at 22.} These are defined in singular terms, such as "[a]n activity constituting a federal crime or a threat to national security."\footnote{Id. at 21.} Alternatively, the circumstances may indicate that "[a]n individual, group, organization, entity is or may be a target of attack, victimization, acquisition, infiltration, or recruitment in connection with criminal activity."\footnote{Id. at 23.} For enterprise investigations, the text of the guidelines clearly refers to "the group or organization."\footnote{Id. at 23.}

Not only are the investigations specific regarding the targets, they are specific regarding the facts that support the initiation of
the predicate investigation. For enterprise investigations, this means that there must be an articulable factual basis for the investigation that reasonably indicates that the group or organization was involved in the commission of certain crimes and activities.\textsuperscript{388} Full investigations, in turn, require specific and articulable facts giving reason to believe that a threat to national security may exist.\textsuperscript{389} Like preliminary investigations, such inquiries are specific in that they may relate to individuals, groups, and organizations.\textsuperscript{390} In contravention of the Attorney General guidelines, the telephony metadata program collects data, using precisely those tools that are limited to preliminary and full investigations, absent the specificity otherwise required.

c. Future Authorized Investigations

Third, FISA contemplates the relevance of information to an investigation already in existence at the time the order is granted. The statutory language is very specific. Applications must include a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation.\textsuperscript{391} The placement of the word "are" before the word "relevant" suggests that at the time the records are being sought, their relevance to an investigation must be established.

The orders issued by FISC, however, depart from the statutory language, empowering the NSA to obtain the data in light of their relevance to future "authorized investigations"—and requiring telecommunications companies to indefinitely provide such information in the future.\textsuperscript{392} How can the court know that all such telephony data will be relevant to investigations that are not yet opened? As noted by amici in In re Electronic Privacy In-
terrorist groups or targets, and their sponsors, some or all of which could underlie the bulk telephony metadata collection applications and orders. The United States authorizes the collection of third country communications to identify and prevent the movement of such funds, in support of al Qaeda, for example, a terrorist organization deemed a terrorist organization under U.S. law. In this sense, the United States may have a legitimate interest in the collection of communications data from third countries. However, the United States should ensure that the collection of communications data from third countries is consistent with international law and respects the rights and freedoms of individuals.

2. Subpoena Duces Tecum

The only express limit on the type of tangible item that can be subject to an order under 50 U.S.C. § 1861 is that it “can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things.” Although it may be said as a general matter that Congress intended intelligence collection to be subject to different standards than those that apply in a criminal context, in at least the provisions relevant to tangible goods, it is clear that a criminal standard governs the type of information that can be obtained via order. Specifically, the collection must be consistent with a subpoena duces tecum.

The government argues that the telephony metadata program is consistent with this provision, and that its determinations must be given the highest level of deference by the courts. FISC has expressed its agreement with the government’s position.

403. 3 William Blackstone, Commentaries 382.
408. 408. 408 U.S. 683 (1972).
409. See id. at 699–700.
The Nixon standard, however, does not apply in the context of grand jury proceedings. In 1991 the Court explained:

The multifactor test announced in Nixon would invite procedural delays and detours while courts evaluate the relevance and admissibility of documents sought by a particular subpoena. . . . Requiring the Government to explain in too much detail the particular reasons underlying a subpoena threat to compromise the "indispensable secrecy of grand jury proceedings." Broad disclosure also affords the targets of investigation far more information about the grand jury's workings than the Rules of Criminal Procedure appear to contemplate.

The Court went on to note that this does not mean that the grand jury's investigatory powers are limitless; to the contrary, they are still subject to Rule 17(c). Nevertheless, grand jury subpoenas are given the benefit of the doubt, with the burden of showing unreasonableness on the recipient seeking to avoid compliance. For claims of irrelevancy, motions to quash "must be denied unless the district court determines that there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation."

At the broadest level, then, the government's assertion, at least with regard to the burden of proof regarding the information to be obtained and the deference afforded a grand jury subpoena, appears to be valid. But there are three critical flaws in the government's reasoning: first, subpoenas may not be used for fishing expeditions; second, they must be focused on specific individuals or alleged crimes prior to the collection of information; and third, the emphasis is on past wrongdoing—not on potential future relationships and actions. In addition, remarkably, FISC has admitted that the telephony metadata order it issued violates the statutory language requiring that the information to be obtained comport with the requirements of a subpoena.

410. R. Ent. ex rel. APAC, 499 U.S. at 297–99.
411. Id. at 298–99 (citations and quotations omitted).
412. Id. at 300.
413. Id. at 301.
414. Id.

415. See Defendants' Memorandum of Law in Opposition, supra note 401, at 18–19.
416. R. Ent., 499 U.S. at 297.
418. Id.
419. Id. at 13–14.
420. Id. (quotation marks omitted); see also Hale v. Henkel, 203 U.S. 43, 76–77 (1906) (finding a subpoena duces tecum "far too sweeping in its terms to be regarded as reasonable," where it did not "require the production of a single item of documentary evidence, or of contracts with a particular corporation, or a limited number of documents, but all understandings, contracts, or correspondence between a company
As discussed above in relation to the relevance standard, almost all of the telephony metadata collected under Section 215 is unrelated to criminal activity. In Judge Reggie Walton’s words, "Ordinarily, this alone would provide sufficient grounds for a FISC judge to deny the application." The principle at work here was recognized by the Eastern District of New York: "While the standard of relevancy [as applied to subpoenas] is a liberal one, it is not so liberal as to allow a party to roam in shadow zones of relevancy and to explore matter which does not presently appear germane on the theory that it might conceivably become so." A subpoena does not itself need to be used to compel the production of records simply because at some point, in the future, they might become relevant.

In a world limited by the physical manifestation of evidence, practicality helped to cabin the scope of subpoenas. Technology may have changed what is possible in terms of the volume and nature of records that can be obtained and stored, and the level of insight that can be gleaned. But it does not invalidate the underlying principle. Subpoenas, even those issued by grand juries, may not be used to engage in fishing expeditions.

2. Specificity

Grand jury investigations are specific. That is, they represent investigations into particular individuals, or particular entities, in relation to which there is reasonable suspicion that some illegal behavior has occurred. The compelled production of records or items is thus limited by reference to the target of the investigation.


If a grand jury were, for instance, focused on the potentially criminal acts of the head of a crime family in New York, absent reasonable suspicion of some sort of connection to the syndicate, it could not issue a subpoena for the telephone records of the Parent-Teacher’s Association at Briarwood School in Santa Clara, California. In contrast, the Section 215 orders are broad and non-specific. That is, on the basis of no particular suspicion, all call records, many of which are of a purely local nature, are swept up by the NSA.

In response to this argument, the government points out that there is some precedent in the law for the government to collect records in bulk that may be relevant to an investigation and then to subject such records to subsequent analysis to determine which items are, in fact, relevant. In one case, the Eighth Circuit upheld a subpoena, even though most of the records bore no relationship to any criminal activity. This case, however, failed to support the government’s argument with regard to Section 215 and the bulk collection of metadata.

In re Grand Jury Proceedings, the government served two grand jury subpoenas duces tecum on Western Union. The first required production of monthly wire transactions at the Royal Mail Inn, Kansas City, Missouri, for a period of thirteen months. The second required production of Telegraphic Money Order Applications above $1000 from the Royal Mail Inn, Kansas City, Missouri, between January 1984 and February 1986. Western Union moved to quash the subpoenas on the ground that they amounted to an unreasonable search and seizure in violation of the Fourth Amendment. The government responded by alleging that drug dealers in Kansas City were using Western Union to transmit money.
The Eighth Circuit noted that it had previously held that Western Union customers have no privacy interest in Western Union records. The court cited the Supreme Court's holding in United States v. Miller, in which the Supreme Court determined, consistent with Smith v. Maryland, that bank customers do not enjoy a legitimate expectation of privacy in bank records subject to subpoenas.

The court in In re Grand Jury specifically noted that the request at issue—namely, the production of records from Royalleen—was not as sweeping as subpoenas that the judiciary had found to be outside the bounds of acceptability. In Federal Trade Commission v. American Tobacco Co., for instance, the Supreme Court refused to uphold the FTC's direction to two tobacco companies to produce letters and contracts. The FTC had claimed "an unlimited right of access to the respondents' papers...relevant or irrelevant, in the hope that something would turn up." The Eighth Circuit similarly declined to uphold a subpoena calling for an attorney's records over a ten-year period. The collection of all U.S. persons' telephony metadata is more properly considered in the same league as FTC v. American Tobacco Co. and Schriner v. United States, in which the courts recognized the overbroad use of government authority, as opposed to the more limited collection of information at issue in In re Grand Jury Proceedings.

3. Past Crimes

Grand jury investigations are also retrospective, searching for evidence of a past crime. The telephony metadata orders, in contrast, are both past- and forward-looking, in that they anticipate the possibility of illegal behavior in the future. Although most of the individuals in the database are suspected of no wrongdoing whatsoever, the minimization procedures allow for any information obtained from mining the data to then be used in criminal prosecution. This is an unprecedented use of subpoena information-gathering authority amounting to a permanent, ongoing grand jury investigation into all possible future criminal acts.

4. March 2009 FISC Opinion

FISC has openly recognized that the information it obtains from the metadata program could not otherwise be collected with any other legal instrument—including a subpoena duces tecum. In a secret opinion in March 2009, Judge Reggie Walton wrote:

Because the collection would result in NSA collecting call detail records pertaining to [REDACTED] of telephone communications, including call detail records pertaining to communications of United States (U.S.) persons located within the U.S. who are not the subject of any FBI investigation and whose metadata could not otherwise be legally captured in bulk, the government proposed stringent minimization procedures that strictly controlled the acquisition, accessing, dissemination, and retention of these records by the NSA and FBI.

Later in the document, he again noted that the information "otherwise could not be legally captured in bulk by the government." These assertions directly contradict the statutory requirement that the information could otherwise be obtained via subpoena duces tecum and amount to an admission, by the court, that the program violated the statute.

What makes the court's failure to stop the illegal program even more concerning, perhaps, is Judge Walton's explanation of why, even though the information could not legally be obtained in any other way, FISC allowed the government to proceed.

Nevertheless, the FISC has authorized the bulk collection of call detail records in this case based upon: (1) the government's explanation, under oath, of how the collection of and access to such data are necessary to analytical methods that are vital to the national security of the United States; and (2)

431. United States v. Cross, 416 F.2d 1201, 1235 (8th Cir. 1969); accord Newfield v. Ryan, 91 F.2d 700, 702 (5th Cir. 1937).
436. Id. at 12.
minimization procedures that carefully restrict access to the BR metadata and include specific oversight requirements.\textsuperscript{457} In other words, FISC allowed an illegal program to operate because the government (1) promised that it was vital to U.S. national security, and (2) was directed by the court to police its own house by following the minimization procedures. The former is a flimsy excuse for allowing the executive branch to break the law. The latter highlights the extent to which the court, precisely because of the size of the collection program in question, was dependent on the NSA: "In light of the scale of this bulk collection program, the Court must rely heavily on the government to monitor this program to ensure that it continues to be justified ... and that it is being implemented in a manner that protects the privacy interests of U.S. persons."\textsuperscript{456a} Recall that Congress created FISC to protect U.S. persons' privacy interests. Congress did not anticipate that FISC would simply hand over this responsibility to the NSA.

C. Escalation of Pen-Trap Provisions

All of the information obtained through the telephony metadata program is already provided for in FISA's pen register and trap and trace provisions.\textsuperscript{439} The FISC order requires that telecommunication service providers turn over all telephony metadata between the United States and abroad or wholly with-

\textsuperscript{457} Id.

\textsuperscript{439} The government secretly declassified two FISC opinions about a bulk electronic communications metadata program conducted under the Pen Register and Trap and Trace provisions of FISA. The program reportedly was ended because it failed to deliver the operational value expected. Although acknowledging the operational similarities, no discussion has been made public as to why the telephony metadata program was not conducted under section 403 of FISA, as its electronic communications bulk metadata counterpart was. See Press Release, Office of the Dir. of Intelligence, DNI Clipper Declassifies Additional Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (Nov. 18, 2013), available at http://www.dea.gov/index.php/newsroom/press-releases/19-press-releases-2013/9949-clipper-declassification-additional-intelligence-community-documents-regarding-collection-under-section-501-of-the-foreign-intelligence-surveillance-act-nov. [perma.cc/64VA-SH6A].


\textsuperscript{461} Id.

\textsuperscript{462} Id.


\textsuperscript{464} Id.

\textsuperscript{465} Id. § 1842(b)(2).

\textsuperscript{466} Id. § 1842(d)(2)

\textsuperscript{467} Id. § 1842(a)(2) (requiring "certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation is of a United States person as not conducted solely upon the basis of activities protected by the first amendment to the Constitution").
What the NSA is doing with the telephony metadata program is essentially obtaining all of this same information, without first making a particularized showing in relation to the target, obtaining an individualized court order, or ensuring the U.S. persons' data are given heightened protection. The issue is thus not whether U.S. persons' data are being collected "solely on the basis of otherwise protected First Amendment activity" — but that they are being collected without any individualized suspicion and on no basis whatsoever. In essence, the NSA has sidestepped the carefully-constructed protections of subsection three to collect all telephony metadata.

D. Potential Violation of Other Provisions of Criminal Law

There are, in addition, other statutory provisions that raise questions about the legality of the current telephony metadata program. In December 2008, FISC issued a "Supplemental Opinion" giving the court's reasons for concluding that the records to be produced pursuant to the telephony metadata orders were properly subject to production under 50 U.S.C. § 1861.444 The reason behind the order appears to be that, although such orders were previously approved, for the first time the government had identified the provisions of 18 U.S.C. §§ 2702-2703 that are relevant to the question.

Under 50 U.S.C. § 1861, Congress empowered the government to apply to FISC "for an order requiring the production of any tangible things (including books, records, papers, documents, and other items)."445 The court placed special emphasis on the use of the word "any," suggesting that it "naturally connotes an expansive meaning," extending to all members of a common set, unless Congress employed "language limiting [its] breadth."446

---


The court had apparently considered "any" to be without limit, until 18 U.S.C. §§ 2702-2703 was brought to its attention.452 This statute laid out an apparently exhaustive set of circumstances under which telephone service providers could provide customer or subscriber records to the government.453 An order under 50 U.S.C. § 1861 was not included in this list.454 At the same time that Congress had passed section 215 of the USA PATRIOT Act, moreover, it had amended sections 2702 and 2703 in ways that appeared to re-affirm that communications service providers could only divulge records to the government in particular circumstances — without specifically noting FISC orders.455

Judge Walton reconciled this tension in a most curious manner. He pointed to National Security Letters — a completely different form of subpoena (i.e., an administrative subpoena), noting that in the USA PATRIOT Act, Congress empowered the FBI, without prior judicial review, to compel a telephone service provider to produce "subscriber information and toll billing records information," on the basis of FBI certification of relevance to an authorized foreign intelligence investigation.456 Judge Walton pointed to the heightened requirements of Section 1861, i.e., that the government provide a "statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant" to a foreign intelligence investigation, and that FISC determine that the application is sufficient.457 He then noted that Section 2703(c)(2) expressly permits the government to use administrative
subpoenas to obtain certain categories of non-content information from a provider—and concluded that Congress surely could not have intended a higher standard for FISC orders.465

The problem with his reasoning is that despite the precision of 18 U.S.C. §§ 2702-2703 and the concurrent amendment of these sections with the introduction of USA PATRIOT Act section 215, Congress nowhere included in the language of 18 U.S.C. §§ 2703-2703 provision for FISC orders as an exception to the closed set. Instead, it allowed the provision of telephony metadata to the government only in two cases: first, when the governmental entity uses an administrative subpoena authorized by a federal or state statute; or, second, when a federal or state grand jury or trial subpoena issues.466 The next paragraph, moreover, ties the provision directly to the actual commission of a crime. A court order for disclosure under Section 2703(c) may only be issued by a court of competent jurisdiction where the government can provide "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation."467 The types of records the FBI sought from FISC, in contrast, extended well beyond records either relevant or material to an ongoing criminal investigation. Furthermore, under 18 U.S.C. § 2703(d), the judiciary is empowered to quash or modify such orders where the records being requested "are unusually voluminous in nature."468 It would be difficult to imagine any telephony metadata database more voluminous than one collecting all call data in the United States. As such, the statute contemplates yet further limits on the collection of information.

III. CONSTITUTIONAL CONSIDERATIONS

In its White Paper, the government argues that the telephony metadata collection program complies with the Constitution.469 In so doing, it relies on Smith v. Maryland, in which the Supreme Court held that participants in telephone calls lack a reasonable expectation of privacy (for purposes of the Fourth Amendment) in the telephone numbers dialed and received on one's phone.470 Judge Eagan similarly relies on Smith in her August 2013 memorandum opinion on the bulk collection program.471 It is the only Supreme Court Fourth Amendment case that she directly discusses, on the grounds that it is dispositive of the question of whether the NSA has the authority to collect all telephony metadata.472

The government's reliance on Smith v. Maryland is problematic. The case involved individualized, reasonable cause to believe that the target of the pen register engaged in criminal behavior and threatening and obscene conduct.473 The placement of the pen register, moreover, was obtained via consent.474 Most importantly, significant technological and societal changes mean that the intrusiveness of the technology and the resultant harm to U.S. citizens' privacy interests are fundamentally different from the situation that the Court confronted in 1979.

The cornerstone of the government's argument is Katz v. United States, a case in which the Supreme Court supplemented trespass doctrine with a reasonable expectation of privacy.475 But Katz itself was an effort by the Court to understand the Fourth Amendment in light of changing technologies. Since that time, tension has developed into what is now a split on the Court between those who consider Fourth Amendment incursions in terms of physical trespass, and those who adopt the reasoning of...

---

Kate more broadly. Thus, a series of cases involving thermal scanners, GPS devices, and highly-trained dogs have divided along these lines. Regardless of which approach one adopts, there is a strong argument that bulk collection falls within constitutional protections. The telephony metadata program amounts to a general warrant, the prohibition of which gave rise to the Fourth Amendment. The reason such warrants were rejected is because they amounted to granting the government an indefinite right of trespass, for which redress (because of their execution with legal sanction) could not be sought. Beyond the general warrant concern, the bulk telephony metadata program digitally trespasses on the private lives of U.S. citizens.

Under the reasonable expectation of privacy test, Americans do not expect that information provided to telephone service providers will be collected wholesale by the government to ascertain whom they call, who calls them, how long they talk, and where they are located when they do so. Most Americans do not even realize that they are providing this information to their telephone companies when they make a phone call. Nor do they realize the significant social network and substantive analysis that can be performed on this data to generate new insights into their private lives.

A variant of the government’s argument suggests that the only point at which an individual has a privacy interest is not at the moment of acquisition of data, but at the moment when the data is subjected to individual queries or logarithmic processing. That is, the “search” in question relies on two additional considerations: (a) whether knowledge is being extracted or further knowledge is being generated from a broader data set comprised of third party data and (b) whether a human interlocutor is involved in the exchange.

There are a number of problems with this approach. In addition to the trespass and reasonable expectation considerations discussed above, the Supreme Court has never carved out an “automation exception” to the Fourth Amendment. It is at the point that the thermal imaging device records heat signatures, that the GPS chip is attached, and that the dog steps onto the porch, that the search has occurred. That is the point at which an individual’s private information is recorded. In addition, human beings have been involved in the process all the way along—regardless of the nature of the collection device. A human being makes the decision to obtain telephony metadata and to record it. Human beings program the equipment and arrange for it to be activated and to receive the information. They decide how it will be stored, accessed, and shared in the future. Analysis of the data is simply the final step in a long series of human decisions.

A final argument offered in support of the program is that, even if privacy interests are recognized, the national security interests at stake override whatever privacy intrusion arises from the bulk collection of telephony metadata. Variants of this argument emphasize threats that the country faces and the extent to which access to information significantly strengthens the intelligence community’s hand. DOJ explained to Congress: “[T]hese . . . collection programs significantly strengthen the Intelligence Community’s early warning system for the detection of terrorists and discovery of plots against the homeland.” This claim lacks specificity. Usefulness qua usefulness is never sufficient justification for overriding statutory or constitutional constraints.

A. The Problem with Smith v. Maryland

The Fourth Amendment establishes “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” In 1967, the Supreme Court interpreted this language in a manner that protected people, not places. Justice Stewart, writing for the Court, explained, “What a person knowingly exposes to the

---

472. Id.
public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”473 As Justice Harlan noted in his concur-
rence, the question is both subjective and objective: An in-
dividual must have exhibited an actual expectation of privacy
and that expectation must “be one that society is prepared to
recognize as ‘reasonable.’”474 Resultantly, “a man’s home is, for
most purposes, a place where he expects privacy, but objects,
activities, or statements that he exposes to the ‘plain view’ of
outsiders are not ‘protected’ because no intention to keep them
to himself has been exhibited.”475

In Smith v. Maryland, the Supreme Court held that a pen reg-
ister placed on a telephone line did not constitute a search
within the meaning of the Fourth Amendment, because per-
sions making phone calls do not have a reasonable expectation
that the numbers they dial will remain private.476 The key sen-
tence from the decision centered on the customer’s relationship
with the telephone company: “A person has no legitimate ex-
pectation of privacy in information he voluntarily turns over to
to third parties.”477 It is this sentence that spawned what has come
to be known as the “third party doctrine.”478

The government relies on this opinion and the resultant third-party doctrine to argue that the telephone metadata pro-
gram is constitutional. In the DOJ’s August 2013 White Paper,
it suggests that a Section 215 order is not a search because “the
Supreme Court has expressly held participants in telephone
calls lack any reasonable expectation of privacy under the
Fourth Amendment in the telephone numbers dialed.”479 In

ACLU v. Clapper, the government again cited to the Court’s rea-

473. Id. at 331–32 (citations omitted).
475. Id.
477. Id. at 746-44.
478. See also United States v. Miller, 425 U.S. 435, 443 (1976) (extending the third
party doctrine to banking records), and United States v. Warden, 631 F.3d 286,
288 (6th Cir. 2011) (declining to extend the third party doctrine to an e-mail stored
with an Internet Service Provider on the grounds that customers have a reason-
able expectation of privacy in their content).
479. See generally White Paper, supra note 2, at 19.
480. Defendants’ Memorandum of Law in Support of Motion to Dismiss the Compliant at 32–33, ACLU v. Clapper, No. 13-cv-03949 (S.D.N.Y. Aug. 26, 2013)
(quoting Smith, 442 U.S. at 743–44).
481. Id. at 33.
482. In re Application of the Federal Bureau of Investigation for an Order Re-
quiring the Production of Tangible Things from [REDACTED], No. 13-108-sip
op. at 6. The only other case directly cited in Judge Eagan’s Fourth Amendment
discussion appears to be a decision of the P.S.A. court itself, with secondary cita-
tions. The details of the recent court opinion that the cites as precedent, however,
are redacted. Id. at 6.
483. Id. at 9.
the use of pen registers and their application to broad sectors of the population have changed as technology has advanced.687

First, consider the facts of Smith v. Maryland. On March 5, 1976, Patricia McDonough was robbed in Baltimore, Maryland.688 After giving the police a description of the robber and a 1975 Monte Carlo she had seen near the scene of the crime, she started receiving threatening and obscene phone calls from a man who identified himself as the robber.689 At one point, the caller asked her to go out in front of her house.690 When she did, Ms. McDonough saw the 1975 Monte Carlo moving slowly past her home.691 On March 16, the police observed a car of the same description in her neighborhood.692 Tracing the license plate, police discovered that the car was registered to Michael Lee Smith.693

The following day, the police asked the telephone company, without a warrant, to install a pen register to trace the numbers called from Smith’s home telephone.694 The company agreed, and that same day Smith called Ms. McDonough’s home.695 On the basis of this and other information, the police applied for and obtained a warrant to search Smith’s house.696 Upon executing the warrant, police found a telephone book with the corner turned down to Ms. McDonough’s name and number.697 In a subsequent six-man lineup, Ms. McDonough identified Smith as the person who robbed her.698

Although the police did not obtain a warrant prior to installing the pen register, at a minimum, reasonable suspicion had been established that the target of the surveillance, Michael Lee Smith, had robbed, threatened, intimidated, and harassed Patricia McDonough. The police, accordingly, installed the pen

689. Id.
690. Id.
691. Id.
692. Id.
693. Id.
694. Id.
695. Id.
696. Id.
697. Id.
698. Id.
699. Id.

The phone number is a public record and is easily available. The government, however, wants to place a pen register and trap and trace on all U.S. persons—essentially treating everyone in the United States as though they are Michael Lee Smith.

In Smith, the police wanted only to record the numbers dialed from the suspect’s telephone.699 Although it is now often forgotten, at the time the case was decided telephone companies were treated as utilities, with local telephone calls billed by the minute. What was unique about the technology involved in the pen register was that it could both identify and record the numbers dialed from a telephone—a function that the phone company itself did not have. The purpose of the pen register was therefore specific and limited.

By contrast, the bulk collection program now collects the numbers dialed, the numbers that call a particular number, trunk information, and session times. While the police in 1976 were concerned with whether Michael Lee Smith was calling one specific number, the NSA metadata program now collects all numbers dialed—in the process obtaining significant amounts of information about individuals. Calls to a rape crisis line, an abortion clinic, a suicide hotline, or a political party headquarters reveal significantly more information than what was being sought in Smith. This makes the sheer amount of information available significantly different.

Trunk information, moreover, reveals not just the target of a particular telephone call, but where the callers and receivers are located.700 At the time of Smith, the police were only able to tell when someone was located at Smith’s home. The telephone
did not follow Smith around. In contrast, mobile technologies now allow the police to ascertain where persons are located, creating a second layer of surveillance based simply on trunk identifier information. The bulk collection of records, moreover, means that the government has the ability to do that for not just one person, but for the entire country.

Further characteristics distinguish the case. In Smith v. Maryland, for instance, the police sought the information for a short period. The bulk metadata collection program, by contrast, while continued at 90-day intervals, has been operating for seven years now and the NSA argues that it should be a permanent part of the government surveillance program.

In Smith, the telephone company consented to placing the pen register on the line. There was no element of compulsion involved. This is a critical element in the analysis. The Fourth Amendment only applies to government actors. To the extent, then, that private companies are acting in their private capacities, the Fourth Amendment does not apply. In 1989, however, the Supreme Court considered a case in which a railroad company conducted drug testing on employees at the behest of the government. The Supreme Court held that when private actors act under compulsion of the sovereign authority, they must be viewed as an instrument or agent of the government.

In the case of the telephony metadata program (and in contrast to the situation in Smith v. Maryland), the government is compelling the telephone companies to produce all telephony metadata, under court order and with threat of sanction for failing to abide by the terms of the secondary order. The telecommunication service providers are thus acting directly at the behest of the government and, as such, should be considered within the reach of the Fourth Amendment.

Perhaps the most important difference between the two situations lies in the realms of technology and social construction. The extent to which we rely on electronic communications to conduct our daily lives is of a fundamentally different scale and complexity than the situation that existed at the time the Court heard arguments in Smith. Resultantly, the extent of in-

---

No. 3] Bulk Metadata Collection

formation that can be learned about not just individuals, but about neighborhoods, school boards, political parties, Girl Scout troops—indeed, about any social, political, or economic network—simply by the placement of a pen register trap and trace, is far beyond what the Court contemplated in 1979.

B. More Intrusive Technologies and Their Impact on Privacy

The government argues that even if one sets aside Smith v. Maryland and considers the collection of telephony metadata to be a search, it is nevertheless reasonable. This claim dramatically understates both the evolution of technology and the intrusiveness of the program. Millions of Americans' communications are currently being tracked. The data include intimate details about U.S. citizens' lives that can be mined for further information. Significant social analysis can also be conducted on the data. Sophisticated algorithms, for instance, can be applied to pen register information to ascertain where the important nodes are in a network. Alliances, friendships, and predilections can be uncovered by studying patterns in behavior. And unlike raw content, the type of information that can be gleaned is ordered—making it in some ways even more useful than content itself.

Consider the sheer volume of communications being monitored. Although the FISA orders that the government has released and acknowledged relate solely to one company (Verizon), officials have also acknowledged that the acquisition of telephony metadata extends to the largest telephone service providers in the United States: Verizon, AT&T, and Sprint. This means that every time the average U.S. citizen makes a telephone call, the NSA is collecting the location, the number called, the time of the call, and the length of the conversation.

The numbers are worth noting. According to the Wall Street

---


505. Id.
Journal, Verizon has 98.9 million wireless customers and 22.2 million landline customers; AT&T has 107.3 million wireless customers and 31.2 million landline customers; and Sprint has 55 million customers in total. In short, the program monitors hundreds of millions of people.

As for the type of information obtained, the FISC order requests that the telephone service providers give the government all "call detail information," a term that is defined by regulatory provision as: "Any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call, and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call." The FISC order further directs that the company provide "selection identifying information," such as originating and terminating number, International Mobile Subscriber Identity number, and the International Mobile station Equipment Identity number. As Edward Felten, a Professor of Computer Science at Princeton University, recently explained to the Senate Judiciary Committee:

These are unique numbers that identify the user or device that is making or receiving a call. Although people who want to evade surveillance can make it difficult to connect these numbers to their individual identities, for the vast ma-

506. Id.
507. 47 C.F.R. § 64.2007 (2012). Senior intelligence officials have repeatedly asserterd that although they have the authority to collect GPS data, and have in the past, they are not currently doing so under the Section 505 telephony metadata program. See, e.g., Joint Statement for the Record of Director of National Intelligence James Clapper and General Keith Alexander before the S. Comm. on the Judiciary, 113th Cong. (2013); Susanah German & Julian E. Barnes, (Revealed: NSA Downs’ CellPhone-Location Records,” WALL. ST. J., June 10, 2013, http://www.wsj.com/articles/SB10001424052748703397404578558088006134706.

509. Hearing on Continual Oversight of the Foreign Intelligence Surveillance Act Before the S. Comm. on the Judiciary, 113th Cong. 3 (2013) (written testimony of Edward W. Felten, Professor, Princeton Univ.).
510. Id.
511. Id. (citing that the numbers are in unpredictable formats, as is the time and date information, and contrasting telephony metadata to content).
512. Id. at 5.
a sexual assault hotline or a tax fraud hotline will of course not reveal the exact words that were spoken during those calls, but phone records indicating a 30-minute call to one of those numbers will still reveal information that virtually everyone would consider extremely private.513

Even if U.S. citizens wanted to opt out of having this information collected, it would be virtually impossible to do so. There have, for instance, been advances in encryption. But these technologies all revolve around content—not metadata. Although some technologies are focused on metadata, these are not sufficiently advanced to allow for real-time communication.514 The only option is therefore not to use a telephone. The cost of doing so, however, would lean towards divesting oneself of a role in the modern world—impacting one's social relationships, employment, and ability to conduct financial and personal affairs.

Notably, all of these considerations are focused on telephony metadata. But the logic of the government's argument, as applied to metadata generally, has virtually no limit. One could equally argue that all financial flows, Internet usage, and e-mail exchanges are relevant to ongoing terrorism investigations under section 215. Almost all forms of metadata could be at stake.

Americans have contractual relationships with myriad corporate entities, to whom they have entrusted parts of their lives, such as friendships, correspondence, buying patterns, and financial records. Creating a contractual relationship with Safeway, however, to gain access to reduced prices for food, is something different in kind from divulging to the U.S. government that you keep kosher, help to support your mother, and attend synagogue. Americans reasonably expect that their movements, decisions, and communications will not be recorded and analyzed by the intelligence agencies.

C. Judicial Tension: Trepass and Katz's Reasonable Expectation of Privacy

In Katz v. United States, the Court replaced the previous trespass doctrine with one based on a reasonable expectation of privacy. The Court explained, "The fact that the electronic device employed to record Katz’s conversation "did not happen to penetrate the wall of the phone booth can have no constitutional significance."

513. To quote the United States Court of Appeals for the Second Circuit, "Circuit Courts have repeatedly held that the Katz trespass test is not the only test for determining whether a statutory or constitutional warrant should be issued."

For the Court, the Constitution protected electronic violations, as much as physical intrusions, into space otherwise protected by the Fourth Amendment.

Katz itself was an effort by the Court to come to terms with new technologies. Since that time, tension has emerged and now marks a split on the Court between those who consider Fourth Amendment incursions in terms of physical trespass, and those who adopt the reasoning of Katz more broadly. Thus, a series of cases involving areas such as thermal imaging,516 GPS devices,517 and highly-trained dogs518 divide along these lines, with one Justice (Sotomayor) siding alternately with one side or the other. Regardless of which approach one adopts, however, the bulk collection of Americans’ metadata runs afoul of the Fourth Amendment.

In the realm of trespass, the program authorized under section 215 amounts to a general warrant—which was the very definition of an unreasonable search and seizure at the time of the founding. It was to prohibit general warrants, and thereby to gain the support of anti-Federalists for the fledgling Constitution, that James Madison wrote the Fourth Amendment and introduced it into Congress in 1789 as part of the Bill of Rights.519 The telephony metadata program, moreover, amounts to a digital trespass on citizens’ private lives. The application of Katz's reasonable expectation of privacy test, albeit via a different route, reaches a similar conclusion: that is, the telephony metadata collection program falls within Fourth Amendment protections.

1. The Prohibition on General Warrants

At the time of the founding, English courts rejected general warrants. A different standard, however, marked the crown’s
treatment of the American colonies. This angered the colonists, who saw themselves, first and foremost, as Englishmen—and therefore deserving of all the rights and privileges accorded to English subjects.

Perhaps the most famous case establishing the right of Englishmen to be free of a general writ dates from November 1762, when King George III's messengers broke into a man's home to execute a warrant issued by the Secretary of State. The warrant empowered the king's men "to make strict and diligent search for... the author, or one concerned in the writing of several weekly very seditious papers." The men, who searched John Entick's home for four hours without his consent and against his will, "broke open, and read over, pried into and examined all of his private papers [and] books." Upon departure, the men seized Entick's documents, charts, pamphlets, and other materials.

Chief Justice of the Common Pleas Charles Pratt, First Earl Camden, ruled that both the search and the seizure were unlawful. He explained:


509. The full warrant read:

George Montague Dunk, Earl of Halifax, Viscount Studley, and Bacon Halifax, one of the Lords of His Majesty's Honourable Privy Council, Lieutenant General of His Majesty's Forces, Lord Lieutenant General and General Governor of the Kingdom of Ireland, and principal Secretary of State, etc., these are in His Majesty's name to authorize and require you, taking a certificate of your resistance, to make strict and diligent search for John Entick, the author, or one concerned in writing of several weekly very seditious papers, entitled The Monitor, or British Freethinker, No. 357, 358, 360, 375, 376, 378, 379, and 380, London, printed for J. Wilson and J. Bell in Pater-Noster-Row; which contain gross and scandalous reflections and invective upon His Majesty's Government, and upon both Houses of Parliament, and him, having found, you are to seize and apprehend, and to bring, together with his books and papers, in safe custody before me to be examined concerning the premises, and further deal with according to law; in the due execution whereof all magistrates, sheriffs, justices of the peace, constables, and other His Majesty's officers civil and military, and all living subjects whom it may concern, are to be aiding and assisting to you in there shall be occasion; and for so doing this shall be your warrant. Given at St. James's the 6th day of November 1762, in the third year of His Majesty's reign, Duke Halifax. To Nathan Carvington, James Watrous, Thomas Andrew, and Robert Blackmore, four of His Majesty's messengers in ordinary.

510. Id. at 807.

511. Id. at 814.

512. Id. at 817-8.
played a central role in lending speed to the American Revolution. Acting under writs established by Parliamentary statute, officers of the crown had permission to search the homes, papers, and belongings of any person. As early as 1660, legislation empowered magistrates to:

"Issue a Warrant to any person or persons thereby enabling him or them with the assistance of a Sheriff, to enter into any House in the day time where such Goods are suspected to be concealed, and in case of resistance to break open such Houses, and to seize and secure the said Goods concealed, And All Officers and Ministers of Justice are hereby required to be aiding and assisting therein." 52

The writs came to be seen as the worst instrument of arbitrary power, turning colonists against the crown. Their use was part of a general crack-down engineered by British Prime Minister William Pitt, who directed the American colonial governors and royal customs officers to enforce trade and navigation laws more strictly—specifically, to "make the strictest and most diligent inquiry into the State of this dangerous and ignominious Trade." 53 He ordered every step authorized by law be taken: "to bring all such heinous Offenders to the most exemplary and condign [sic] Punishment." 54

In response to Pitt's order, the governor of Massachusetts Bay Colony began making use of the writ, prompting Boston merchants to hire James Otis to challenge its constitutionality. In what has become one of the most famous examples of early American legal oration, Otis argued that the writs were contrary to "the fundamental principles of law." 55 Scholars hail Otis's argument in the case as helping "to lay the foundation for the breach between Great Britain and her continental colonies." 56 As A.J. Langguth observed, at the Write of Assistance trial, "James Otis stood up to speak, and something profound changed in America." 57

One of our best accounts of Paxton's Case comes from John Adams, who was present at the argument and whose mentor, Jeremiah Grindley, the most distinguished member of the bar in Boston, opened the case for the crown. 58 In replying to Grindley, Otis stated that his efforts were being made "out of regard to the liberties of the subject." 59 The rights of British subjects were under assault, compelling him to oppose "all such instruments of slavery on the one hand and villany on the other as this Writ of Assistance is." 60

For Otis, the writ was "the worst instrument of arbitrary power." 61 He ignored the crown's claim of necessity—and current practice—noting that the "writ prayed for in this petition, being general, is illegal." 62 He highlighted four concerns: first, it was universal—in other words, it could be executed by anyone in possession of it; second, it was perpetual in that it indefinitely allowed the holder of the writ to conduct searches; third, no prior evidence of wrongdoing need be involved in its execution; and fourth, there was no requirement to swear to suspicion of wrongdoing or, following execution, to inquire into its exercise. "One of the most essential branches of English liberty

52 Otis, speech, supra note 32.
53 NORMAN K. RISORD, JEFFERSON'S AMERICA 1760-1813, at 75 (2d ed. 2002).
56 James M. Partlow, The Child Independence by Birth: James Otis and Writs of Assistance, in 2 A BRIEF HISTORY OF THE UNITED STATES: SIGNATORY MOMENTS IN AMERICAN PUBLIC DISCOURSE 16 (Stephen E. Lucas, ed. forthcoming); see also Paxton's Case of the Writ of Assistance, in JOSHUA QUINCY, supra note 32.
57 Otis's speech is taken from 2 Tri-Bib. PAPERS OF JOHN ADAMS 139-44 (L. Karvin, Wroth & Miller B. Zobel, eds. 1965).
58 Id. 59 Id.
is the freedom of one’s house,” Otis opined. General warrants would annihilate the privilege associated with that right.

Although the court ruled against Otis, John Adams later wrote that his arguments “breathed into this nation the breath of life.” On June 12, 1776, the Virginia Constitutional Convention adopted the Virginia Declaration of Rights—a document that deeply influenced the Declaration of Independence, as well as other states’ constitutions, and became the basis for the Bill of Rights—without which, the Constitution would never have been ratified.

The Virginia Declaration of Rights stated, inter alia, “That general warrants, whereby an officer or messenger may be commanded to search suspected places without evidence of a fact committed, or to seize any person or persons not named, or whose offense is not particularly described and supported by evidence, are grievous and oppressive and ought not to be granted.” The Massachusetts Constitution of 1780 similarly objected to the use of general warrants:

Every subject has a right to be secure from all unreasonable searches and seizures of his person, his houses, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation, and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the persons or objects of search, arrest, or seizure; and no warrant ought to be issued but in cases, and with the formalities, prescribed by the laws.

The New Hampshire Constitution of 1784 lifted the clause almost verbatim. The Virginia ratifying convention of 1788 made a point to ensure that the subsequent Constitution would include a provision affirming that “every Freeman has a right to be secure from all unreasonable searches and seizures; that his person, his house, his papers, and all other his possessions, from all unreasonable searches and seizures.” Consistent with these understanding, James Madison’s first draft of the Fourth Amendment addressed the right of the people “to be secured in their persons, houses, papers, and other property, from all unreasonable searches and seizures.”

In 1886 the Supreme Court recognized the importance of the writs and the Founders’ rejection of the same as encapsulated in the Fourth Amendment:

In order to ascertain the nature of the proceedings intended by the Fourth Amendment to the Constitution under the terms “unreasonable searches and seizures,” it is only necessary to recall the contemporary or then recent history of the controversies on the subject, both in this country and in England. The practice had obtained in the colonies of issuing writs of assistance to the revenue officers, empowering them, in their discretion, to search suspected places for smuggled goods, which James Otis pronounced “the worst instrument of arbitrary power, the most destructive of English liberty, and the fundamental principles of all law.”

538. Id.
539. 10 CHARLES FRANCIS ADAMS, THE WORKS OF JOHN ADAMS 276 (Boston, Little, Brown & Co. 1856).
540. VA. DEBT. OF BILLS 10.
541. MARK CONST. OF 1780, pt. 1, art. XIV.
542. N.H. CONST. OF 1784, art. XIII (“Every subject hath a right to be secure from all unreasonable searches and seizures of his person, his houses, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath, or affirmation; and if the order in the warrant to a civil officer, to make search in suspected places, or to seize any person or persons not named, or whose offense is not particularly described and supported by evidence, are grievous and oppressive and ought not to be granted.”)
544. 483, 484 (quoting DUNKELD, supra note 542, at 184, 191, 200-201).
545. Id. (quoting DUNKELD, supra note 543, at 207 (emphasis added)). Note that the historical antecedents suggest a broad reading of the “persons, houses, papers, and effects” language of the Fourth Amendment:
546. See Davis, supra note 539, at 559; also see H. LAVON, THE HISTORY AND DEVELOPMENT OF THE FOURTEENTH AMENDMENT TO THE UNITED STATES CONSTITUTION 101 (1927).
was found in an English law book since they placed "the liberty of every man in the hands of every petty officer." This was in February, 1761, in Boston, and the famous debate in which it occurred was perhaps the most prominent event which inaugurated the resistance of the colonies to the oppressions of the mother country. "Then and there," said John Adams, "then and there was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child of liberty was born."

The Court acknowledged the importance of Lord Camden's decision in Entick v. Carrington:

[Camden's] great judgment on that occasion is considered as one of the landmarks of English liberty. It was welcomed and applauded by the lovers of liberty in the colonies as well as in the mother country. It is regarded as one of the permanent monuments of the British Constitution, and is quoted as such by the English authorities on that subject down to the present time.

Throughout U.S. history, the Supreme Court has continued to recognize the special role played by general warrants and writs of assistance in shaping the contours of the Fourth Amendment. In 1980, the Court recognized that it was "familiar history that indiscriminate searches and seizures conducted under authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment." General warrants were presumptively unreasonable.

Consistent with this reading, Professor Akhil Amar, inquiring as to what the warrant clause means—and what the relationship is between it and the earlier reasonableness clause—suggests that "broad warrants—warrants that fail to meet the various specifications of clause two—are inherently unreasonable under clause one." Such a general warrant would immunize the officer who carried it out from a subsequent tress

pass suit. In the case of Entick v. Carrington, "Armed with sweeping warrants issued by executive officials, various government henchmen broke into Englishmen's houses, searched their papers, arrested their persons, and rummaged through their effects, in hopes of finding" wrongdoing.

Professor Thomas Davies similarly recognizes that "[t]he historical statements about search and seizure" in the Fourth Amendment "focused on condemning general warrants. In fact, the historical concerns were almost exclusively about the need to ban house searches under general warrants." Evidence suggests that "unreasonable searches and seizures" was a proxy for "the inherent illegality of any searches or seizures that might be made under general warrants." Davies posits that the reason the Framers even bothered "to adopt constitutional bars against general warrants" was "because of the genuine concern that Congress might endanger the right in the future."

The FISC Order authorizing the telephony metadata program is a general warrant. It authorizes the government to rummage through our papers and effects in the hope of finding wrongdoing. There is no previous suspicion of criminal activity. Almost none of the information obtained relates to illegal behavior.

It matters little whether one stores one's papers in a filing cabinet in one's den, or places all financial documents in the iCloud—the digital equivalent, in modern times, of a filing cabinet. Steer volume of information requires individuals to arrange for storage of everything from medical records to family photos. E-mail, in turn, holds our correspondence—papers that we place on a server with a company with whom we have a contractual relationship. Banking records may be accessible over the Internet. These are our modern day equivalents of the papers and effects held by Entick in his home.
In considering the case of Entick v. Carrington, Lord Camden wrote, "The great end for which men entered into society was to secure their property."

He continued, "By the laws of England, every invasion of private property, be it ever so minute, is a trespass." Camden added:

Papers are the owner's goods and chattels; they are his dearest property, and are so far from enduring a seizure that they will hardly bear an inspection... where private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect.\footnote{598}

Allowing the government to obtain bulk metadata is the equivalent of a digital trespass on what Justice Brandeis referred to as the "privacies of life."\footnote{599} Not only does the government gain penetrating insight into our private affairs, but it does so to a degree that even those engaged in the activity itself do not realize. That it is an electronic trespass, and not a physical one, matters naught. Brandeis explained, "It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty and private property..."\footnote{600} The digital trespass in which the NSA is engaging is not supported by probable cause. It is not supported by reasonable suspicion. No suspicion of any wrongdoing whatsoever is contemplated by the collection of records. It is the equivalent of a general warrant and, as such, is odious to the Fourth Amendment.

2. Search of Metadata and the Reasonable Expectation of Privacy

In recent Fourth Amendment cases considering new technologies, a schism has appeared in the Court between adopting an approach based on traditional concepts of trespass, and examining the facts from the vantage of the reasonable expectation of privacy—a higher bar adopted in 1967 as a way of augmenting the Court's previous reliance on physical space.

\footnote{597} (1765) 9 How. St. Tr. 1029 (C.P.) 1064.
\footnote{598} Id.
\footnote{599} Olmstead v. United States, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting).
\footnote{600} Id. at 474-75.

In \textit{United States v. Jones},\footnote{601} the Court considered a case involving 28-day surveillance.\footnote{602} The government obtained a search warrant permitting it to place a Global-Positioning System (GPS) tracking device on a car registered to the wife of a suspected drug dealer.\footnote{603} The day after the warrant expired, agents installed the device and followed the car's movements for nearly a month.\footnote{604} Information thus obtained allowed the government to indict Antoine Jones and others on drug trafficking conspiracy charges.\footnote{605} The Supreme Court held that attaching the GPS device to the car and tracing its movements amounted to a search within the meaning of the Fourth Amendment.\footnote{606}

This case is important for determining the constitutionality of the telephony metadata program in three important ways. First, it recognized that Katz's reasonable expectation of privacy test did not supplant the rights in existence at the time the Fourth Amendment was forged. Justice Scalia, writing for the Court, explained:

It is important to be clear about what occurred in this case. The government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical invasion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted.\footnote{607}

Justice Scalia cited \textit{Entick v. Carrington}, noting that the Court had described it as a "monument of English freedom - undoubtedly familiar to every American statesman" at the time the constitution was adopted, and considered to be "the true and ultimate expression of constitutional law" with regard to search and seizure.\footnote{608} For Justice Scalia, and for the Court, the reasonable expectation of privacy test was of no consequence: "At bottom, we must assure[ ] preservation of that degree of
privacy against government that existed when the Fourth Amendment was adopted."

Just as the Court eschewed Katz v. United States as being inapposite for consideration of the rights that existed when the Fourth Amendment was adopted, it would be equally inapposite to dismiss the Fourth Amendment’s rejection of general warrants. "[A]t a minimum,” Justice Scalia wrote, the “18th-century guarantee against unreasonable searches ... must provide ... the degree of protection it afforded when it was adopt-
ed." The concept of a general warrant and the Court’s conception of trespass are, as previously noted, historically con-
connected. The reason that general warrants were rejected at the time of the Founding was because they provided a carte blanche to the government to trespass at will upon one’s prop-
erty and to search through one’s papers and effects without any reasonable suspicion.

The second point to draw out of Jones is that what can be con-
sidered a shadow majority appears to recognize that changed circumstances exist, so as to augment the need for new privacy protections. At least five Justices indicated unease with the intrusiveness of modern technology in light of changed times, offer-
ing in the process different aspects of a mosaic theory of pri-
cy. Justice Alito, joined by Justice Ginsburg, Justice Breyer, and Justice Kagan, suggested that in most criminal investiga-
tions, long-term monitoring “impinges on expectations of priva-
cy.” The nature of new technologies mattered:

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 motor-
sists who choose to make use of their convenience. Many mo-
torists purchase cars that are equipped with devices that permit a central station to ascertain the car’s location at any time so that roadside assistance may be provided if needed and the car may be found if it is stolen."

569. Id. at 947.
570. Id. at 950.
571. Id. at 964 (Alito, J., concurring).
572. Id. at 963.

No. 31] Bulk Metadata Collection

Unlike in the past, the daily business of living one’s life creates a digital record with privacy implications. “Perhaps most significant,” Justice Alito added, “cell phones and other wireless devices now permit wireless carriers to track and record the location of users — and as of June 2011, it has been reported, there were more than 322 million wireless devices in use in the United States.” Before computers, practicality proved one of the greatest protectors of individual privacy. It was difficult and expensive to conduct long-term surveillance. But technol-
ogy has changed the equation. The government now is more able to engage in long-term surveillance; but though relatively short-term monitoring of individuals’ movements in public space might be consistent with the Fourth Amendment, “the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.”

Justice Sotomayor went one step further, calling into ques-
tion the entire basis for third party doctrine. Specifically, in light of the level of intrusiveness represented by modern tech-
nology, “it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in in-
formation voluntarily disclosed to third parties.” Sotomayor pointed out:

This 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. People disclose the phone numbers that they dial or text to the cellular providers; the URLs that they visit and the e-mail ad-
dresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers."

She added, “I would not assume that all information voluntarily
disclosed to some member of the public for a limited pur-
pose is, for that reason alone, disentitled to Fourth Amendment protection.”

573. Id.
574. Id. at 964.
575. Id. at 952 (Sotomayor, J., concurring).
576. Id.
577. Id.
The third point to draw from Jones reflects the growing tension between trespass and the Katz test, as applied to new and emerging technologies—and the increasingly consistent results reached by the Court, regardless of which approach is adopted. Thus, although Justice Sotomayor sided with the majority on trespass grounds, she still embraced the same result as a product of the application of Katz.

Jones was not the first manifestation of this tension in light of new and emerging technologies. In Kyllo v. United States, the Court considered whether thermal scanning conducted outside of a target’s home constituted a search within the meaning of the Fourth Amendment. Agents, having picked up a heat signature that suggested that grow lights were being used inside the target’s garage, used the information to obtain a search warrant which, when executed, revealed several marijuana plants. As in Jones, the concept of trespass figured largely in the decision.

In Kyllo, the Court held that where the government employed a device, not in general public use, to uncover details inside a home that otherwise could only be uncovered via physical intrusion, such surveillance constituted a search within the meaning of the Fourth Amendment and was thus presumptively unreasonable without a warrant. As in Jones, Justice Scalia delivered the opinion of the Court: “It would be foolish to contend,” he wrote, “that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.” The question the Court confronted was “what limits there are upon this power of technology to shrink the realm of guaranteed privacy.” In this equation, Scalia suggested, homeowners should not be left to “the mercy of advancing technology.” The Fourth Amendment, if nothing else, drew a bright line at the curtilage of the home.

577. Id. at 29.
578. Id. at 31–32.
581. Id. at 40.
582. Id. at 33–34.
583. Id.
584. Id. at 35.
585. Id. at 41 (Stevens, J., dissenting).
586. Id. at 63.
587. Id. at 68–69.
588. Id.
One who occupies a public phone booth, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communications.

Whatever role telephones played in 1967, their integration into society has only deepened in the intervening years. Electronic communications have come to play a vital role not just in social interactions, but in conducting all of one's private affairs. That we contract with private companies to ensure careful treatment of this information, that we use passwords to access our telephone, banking, and financial records online, and that we limit access to this information, is the equivalent of shutting the door of the phone booth.

The courts are beginning to recognize privacy interests in this new, electronic sphere. In 2010, for instance, in United States v. Warshak, the Sixth Circuit held that the government had violated Warshak’s Fourth Amendment rights when it obtained e-mail content from Warshak’s Internet service provider, absent a warrant based on probable cause. The court noted that Warshak had a reasonable expectation of privacy in the e-mail he had stored with an ISP.

The amount of information that computers can hold makes them different in kind. In 2011, the Ninth Circuit considered the search of a computer at the border. The dissent noted:

Computers store libraries’ worth of personal information, including substantial amounts of data that the user never intended to save and of which he is likely completely unaware (for example, browsing histories and records of deleted files in unallocated space). Computers offer “windows into [our] lives far beyond anything that could be, or would be, stuffed into a suitcase for a trip abroad.”

590 United States v. Warshak, 631 F. 3d 266 (6th Cir. 2011).
591 Id.
592 United States v. Cotterman, 637 F. 3d 1068 (9th Cir. 2011) (Fletcher, J., dissenting).
593 Id. at 1085-86 (internal citations omitted).
594 133 S. Ct. 1409 (2013).
595 Id. at 1417-18.
596 Id. at 1415-17.
597 Id. at 1416.
598 Id. at 1417-18.
599 Id. at 1417.
600 Id. at 1418 (Kagan, J., concurring).
601 Id.
ers on the Court as to the existence of mutually-reinforcing spheres protecting U.S. citizens—in the face of new technologies—from undue government interference. This is precisely the space occupied by the bulk collection of U.S. citizens’ telephony records. Under either approach, the program, and similarly situated bulk collections of U.S. citizens’ records, violates the Fourth Amendment.

D. The Proverbial Needle in the Haystack

We live in an age in which individual actors have the capability and the intent to harm U.S. national security. Such persons may be tied to state actors, the traditional target of U.S. intelligence activities, or they may not. They may be acting as part of a multi-national network, they may be acting on behalf of a domestic group, or they may simply have a grudge against the United States or its people. The potential construction, dissemination, and use of weapons of mass destruction—such as biological weapons, nuclear devices, cyber attack, or conventional force used against critical infrastructure targets—by such persons changes the equation in terms of how the state must act to protect its interests. It must try to anticipate aggression from state actors, of course, but it must also try to anticipate action from non-state actors and individuals.

With such non-traditional threats in mind, proponents of the telephony metadata program have argued that to find threats, intelligence agencies must first obtain, and then mine, all individuals’ data. The analogy that has been suggested is that intelligence agencies must first build a haystack, in order to find the proverbial needle. The assumptions underlying this model are that all individuals potentially present a threat, and that the threat from individuals can only be identified and understood in the context of all the data.

For constitutional purposes, the argument continues, it is not a search within the meaning of the Fourth Amendment to build the haystack. This only occurs once someone starts sifting through the hay to find the needle. A further nuance in this argument suggests that, to the extent that the creation of the haystack is being accomplished through technology and automation, and no human being is involved, the building of the haystack—and even the analysis of the data—is outside the confines of the Fourth Amendment.

In its 2011 report to Congress, for instance, the Department of Justice noted two NSA bulk collection programs in existence: first, the telephony metadata program under Section 215 and, second, the bulk collection of e-mail envelope information under the pen-trap provisions of FISA. DOJ noted, “Both of these programs operate on a very large scale [REDACTED TEXT] However, as described below, only a tiny fraction of such records are ever viewed by NSA intelligence analysts.”

There are a number of problems with this argument, the first being (consistent with the argument above) that it is the collection of information that brings the bulk collection of information within the meaning of a search for Fourth Amendment purposes—that is, under the reasonable expectation of privacy test, individuals reasonably assume that their movements which are recorded by cell phone towers, and their social interactions, placement in social networks, interests, and possible concerns that emerge from calling records, are not going to be recorded and transmitted to the NSA to be analyzed, queried, stored, and shared with other agencies. This is precisely what sets the NSA surveillance program apart from Smith v. Maryland, in which limited information was provided by the carrier to the police. It was on these grounds that in December 2013 Judge Richard Leon held that the NSA collection program is likely unconstitutional.

The strongest counterargument is that offered by Judge Paul O. of the Southern District of New York, who asserts that calling data on tens of millions of Americans, and the retention of this data, represented precisely what was settled in Smith. In other words, the data in question is only different in volume, not kind, from what was at stake in Smith v. Maryland. That it happens to yield more insight into individuals’ lives matters naught: the key question, instead, is whether it has been provided to a third party. The problem with this analysis is that it ignores the point of inquiring into the reasonableness of the
search. By including both an objective and a subjective standard, the Court allowed for the context and the evolution of technology to be taken into account. In Jones, as was considered above, five Justices questioned whether Smith continues to be applicable in light of the evolution of technology.

In a recent post arguing against the constitutionality of the NSA bulk metadata collection program, Professor Geoffrey R. Stone, who served on the President's Review Board of the metadata collection program, added yet another consideration. The costs traditionally associated with traditional pen registers and trap and trace equipment have, in the past, created a barrier to the government's use of the same. The use of a pen register is time-consuming, fact specific, and costly. As a practical matter, the government can use it in only a handful of situations. The knowledge that the government can use a pen register without probable cause and a warrant therefore has almost no effect on the average person's expectations of privacy or behavior.

The decision to make a telephone call (or not) thus does not turn on the "infiniscellaneous risk" that the government might have placed a pen or trap on our number. Technology, however, Stone argues, has changed the calculation. The government can now do this without any of the efficiency barriers that, in the past, would have prevented us from being placed under surveillance. This was precisely the point that Justice Alito brought out in Jones in relation to the use of GPS technologies. Technology should not continually erode our traditional expectations of privacy. Stone observes, "Without that principle, the evolution of a 'Big Brother' government could do serious damage to the liberty, privacy and dignitary interests of the individual that are essential to a free society.

607. Id.
608. Id.
609. Id.
610. Id.
611. Id.
612. Id.

No. 3] Bulk Metadata Collection

In the context of the haystack argument, it is important to note here that the previous absence of technology performed an important privacy function: it created administrative barriers to inquiring on individuals' private lives. The very question of whether or not to build a haystack is a quintessential twenty-first century question. To suggest that there is no privacy implication in building the haystack ignores the important limiting function that lack of technology and resource constraints previously played.

A second problem with the haystack approach is that the Supreme Court has not recognized any "automation exception" to the Fourth Amendment. To the contrary, it is the moment at which the thermal device picks up the heat signature, when the GPS device is placed on the car, and when the dog sniffs the marijuana inside the home that the search has occurred. In United States v. Karm, for instance, a case that turned on the use of a beeper to follow a suspected drug dealer's car, Justice Stevens explained: "The expectation of privacy should be measured from the standpoint of the citizen whose privacy is at stake, not of the government. It is compromised the moment the invasion occurs. A bathtub is a less private area when the plumber is present even if his back is turned." It is the collection of the information that thus represents an intrusion into privacy.

A variant of the haystack argument that suggests that no search occurs until a human being sees the data being collected ignores the fact that this is a government-centric approach. The Fourth Amendment, however, protects individual rights from government intrusion. It is thus from the individual's perspective that one must evaluate both the act of trespass and the objective and subjective expectations of privacy (as under Katz). And from the individual's perspective, it is at the moment the telephonic metadata is collected that the search occurs. It would thus matter little if the government mounted cameras inside every American's home, promising not to actually watch the tapes until some future point in time. The act of mounting the camera and recording the information is precisely what constitutes a
search, and thus brings such behavior within the protection of the Fourth Amendment.

A third problem with the government’s line of reasoning is that it ignores the intercession of human judgment throughout the process. It is a human being that decides to collect the information. Human beings submit applications to FISC, grant applications, and issue primary and secondary orders to collect the data. Human beings program computers to collect information and to collate it. Human beings write the algorithms, replete with inbuilt assumptions and biases, and then decide where the information goes and in what form it will be available for other human beings to see. In short, human beings are involved throughout the process. To represent it otherwise is to ignore the extent to which technology is being used at the behest of government and not in its stead.

In McCulloch v. Maryland, Chief Justice Marshall wrote, “We must never forget that it is a constitution we are expounding.” Just over a century later, Justice Brandeis recognized that in the intervening time, the Supreme Court had “repeatedly sustained the exercise of power by Congress, under various clauses of that instrument, over objects of which the Fathers could not have dreamed.”

For Brandeis, the purpose of the Fourth Amendment was to protect the privacies of life:

But “time works changes, brings into existence new conditions and purposes.” Subterfuge and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.

Justice Brandeis’ words proved prescient:

The progress of science in furnishing the government with means of espionage is not likely to stop with wire-tapping. Ways may someday be developed by which the government, without removing papers from secret drawers, can re-

617. Id. at 472.
that Congress envisioned. The bulk collection program, moreover, violates the statutory language in at least three ways: it does not comport with the requirement that the tangible goods sought "are relevant to an authorized investigation"; it violates the requirement that the information be otherwise obtainable via subpoena duces tecum; and it bypasses the statutory provisions governing pen registers and trap and trace devices. Compounding the illegality of the program are serious constitutional concerns. The FISC order governing the telephony metadata program amounts to a general warrant, which the Fourth Amendment precludes. The government's efforts to save the program on grounds of third party doctrine are unpersuasive in light of the unique context of Smith v. Maryland, new technologies, and changed circumstances. Growing tension between trespass doctrine and Katz's reasonable expectation of privacy, as applied to new technologies, suggests that under either approach, the telephony metadata program falls outside constitutional bounds.

There are a number of steps that could be taken as part of a comprehensive FISA reform, to address the shortcomings noted in this Article. First, and most importantly, to comply with constitutional demands, the administration, the courts, or Congress needs to bring the bulk collection of U.S. persons' metadata under Section 215 to an end. Second, to strengthen FISC's ability to respond to applications, a number of judicial reforms could be adopted. Foremost on this list is the introduction of adversarial counsel.

In some sense it is inevitable that FISC opinions would extend beyond the original role envisioned by the court (i.e., granting orders), to issuing memorandum opinions. Like all courts, FISC must interpret statutory language and constitutional requirements, in order to apply the law to particular circumstances. Although FISC is not exercising jurisdiction over cases and controversies, it is overseeing a judicial process and, as such, exercising judicial power.620 It is a logical extension of this function that such decisions would then become guidance for similarly situated requests from the Department of Justice and others.

620. U.S. CONST., art. III, § 1 (allocating the judicial power to federal courts, and thus requiring the courts to interpret and to apply federal law).

A high standard of due diligence is recognized and practiced by DOJ's National Security Division (NSD)—an entity particularly aware of its responsibilities in light of its role in enacting, ex parte proceedings.621 It was NSD, for instance, that recognized in January 2009 that the NSA had only been subjecting approximately ten percent of its queries to RAS inspection—and that reported this within a week to FISC.

Nevertheless, for reasons that the Founders and numerous courts in the interim have clearly recognized, the executive branch is hardly a neutral, disinterested observer when its own interests are on the line. Justice Powell explained in United States v. United States District Court that the duties and responsibilities of executive officers are "to enforce the laws, to investigate, and to prosecute... [T]hose charged with this... duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks."622 He underscored the problem: "[U]nreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy... ."623

Allowing contrary views enables the vigorous prosecution of narrow interests, in the process providing FISC with a broader and deeper understanding of the issues at stake. It has taken many scholars by surprise, for instance, that Judge Eagan's August 2013 opinion considers Smith v. Maryland as entirely dispositive of the Fourth Amendment question. United States v. Jones garners but a footnote, with the opinion omitting any sustained discussion of Fourth Amendment jurisprudence. The importance of adversarial counsel extends beyond merely a constitutional advocate to the potential use of adversarial counsel (with subpoena authorities) to represent corporate and other rights-based interests of U.S. persons. There are a number of ways in which an adversarial process could be created. This

623. Id.
is a matter for policy debate. That one is needed, from a legal and constitutional perspective, is clear.

Another alteration that would strengthen FISC’s hand would be to provide the court with the technical expertise required to allow it to ensure that the minimization and other procedures it requires are actually followed by the executive branch. As the multiple noncompliance incidents suggest, simply leaving it to the NSA to self-report creates a gap between what is legally required and what occurs in practice. Having deeper insight into the technologies is critical. There is something fundamentally disturbing about FISC simply trusting the executive branch to police its own operations. History, certainly, has taught us the danger of proceeding in this manner.

Yet, further alterations that may address some of FISC’s shortcomings relate to substantive changes to the law. Unifying the court’s hands, for instance, with regard to whether or not certain orders should be granted would help to respond to the critique that the court has such a high rate of acceptance of applications. It is Congress, at least in relation to Section 215, that imposed these limits on FISC. Removing these, and making other statutory changes, such as restoring the prior targeting requirement, heightening protections for U.S. persons, adding “and material” after “relevant,” narrowing the definition of “foreign intelligence” to exclude “foreign affairs,” and requiring the government to demonstrate past effectiveness prior to renewal orders, would further strengthen the role that FISC could play in overseeing foreign intelligence gathering.

In sum, myriad changes could be put into place to allow the government to take advantage of new technologies, to counter national security threats, and to ensure that the provisions operate in accordance with the U.S. Constitution.624 In the interim, both Congress and the courts have a role to play in insuring that the executive branch operates within statutory and constitutional constraints.

624 As a follow-on to this Article, I construct a taxonomy for potential FISA reforms in Laura K. Donohue, FISA Reform, 10 ISLP (forthcoming 2014), available at http://cyberstethos.law.georgetown.edu/gf/view/content.cgi?article=5167&content_type=epub (perma.cc/N863-LE89).
Section 702 and the Collection of International Telephone and Internet Content

Laura K. Donohue
Georgetown University Law Center, ladonohue@law.georgetown.edu

Draft date: 7/29/2014
Still undergoing revisions.

This paper can be downloaded free of charge from:
http://scholarship.law.georgetown.edu/sexpub/1355
http://ssrn.com/abstract=2436418


SECTION 702 AND THE COLLECTION
OF INTERNATIONAL TELEPHONE
AND INTERNET CONTENT

PROFESSOR LAURA K. DONOHUE

I. INTRODUCTION ...................................................... 2

II. THE EVOLUTION OF SECTION 702 .......................... 10
   A. THE PRESIDENT’S SURVEILLANCE PROGRAM........... 10
   B. RE-DEFINITION OF “FACILITY” UNDER FISA .......... 15
   C. THE PROTECT AMERICA ACT ..................................... 24
   D. THE FISA AMENDMENTS ACT ................................. 27
       1. Section 702 ...................................................... 29
       2. Sections 703 and 704 ............................................ 33
   E. EXECUTIVE ORDER 12333 ................................. 35
       1. Shifting Communications and FISA Modernization... 39
       2. Executive Order 13470 ........................................ 42

III. PROGRAMMATIC COLLECTION ................................... 47
   A. TARGETING ........................................................... 52
       1. Information To/From and About Targets .......... 55
       2. Foreig norms Determinations ............................... 61
       3. Foreign Intelligence Purpose Determination ........ 68
       4. Result of Statutory Interpretations ...................... 71

"Professor of Law, Georgetown Law. Thanks to Judge Morris Arnold, William Banks, Oren Katz, and David Kris for comments on an earlier draft of this paper. This Article is Part 2 of two-part series on NSA surveillance under the Foreign Intelligence Surveillance Act. For Part 1, see Laura K. Donohue, Bulk Metadata Collection, Statutory and Constitutional Questions, 37 Harv. J.L. & Pub. Pol’y 757-900, (2014).
was collecting large amounts of information about U.S. citizens. The National Security Agency (NSA) and Federal Bureau of Investigation (FBI) were "tapping directly into the central servers of nine leading U.S. 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."1

In conjunction with the articles, the press published a series of PowerPoint slides attributed to the NSA, describing a program called "PRISM" (also known by its SIGAD, US-9840N).2 The title slide referred to it as the most used NSA

---


2 Gellman & Poitras, supra note 1. The Privacy and Civil Liberties Oversight Board later labeled, "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." PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM CREATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, July 2, 2014, p. 7, available at http://www.pclib.gov/A7/%20Documents/Report%20PDF%20Sections%20702%20Program/CLCOS/Section%20702_Report%207/Re%20.pdf (hereinafter "7/0/80 Report").

3 PRISM%20Overview (April 2013), https://www.nsa.gov/files/n主业a/20130116/PRISM%20Overview%20Powerpoint%20Slides.pdf. A Signals Intelligence Activity Desigee (SIGAD) is an alphanumeric designation that identifies a facility used for collecting Signals Intelligence (SIGINT). The facilities may be terrestrial (e.g., connected to internet cables), seaborne (e.g., intercept ships), or satellite systems. SIGADs are used to identify SIGINT stations operated the so-called "Five Eyes" (Australia, Canada, New Zealand, the United Kingdom, and the United States). According to documents published in June 2013, as of March 2013 there were 504 active SIGADs. Glen Greenwald & Ewen MacAskill, "Speaker/Informer: the NSA's...
SIGAD. The documents explained that PRISM draws from Microsoft, Google, Yahoo, Facebook, PalTalk, YouTube, Skype, AOL, and Apple—some of the largest email, social network, and communications providers—making the type of information that could be obtained substantial: email, video and voice chat, videos, photos, stored data, VoIP, file transfers, video conferencing, notifications of target activity (e.g., login), social networking details, and special requests. The slides noted that the program started in September 2007, with just one partner (Microsoft), gradually expanding through to the most recent company (Apple, added October 2011), and that the total cost of the program was $20 million per year. As of 2011, most of the more than 250 million Internet communications obtained each year by the NSA under §702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act derived from PRISM.*

A follow-up article two days later printed another slide depicting both PRISM and "upstream" collection of communications on fiber cables and infrastructure (i.e., "[c]ollection directly from the servers of . . . U.S. Service Providers."). Upstream interception allowed the NSA to acquire Internet communications "as they transit the 'internet backbone' facilities." The NSA could collect all traffic crossing Internet cables—not just information targeted at specific Internet Protocol (IP) addresses or telephone number. The potential yield was substantial: in the first six months of 2011, the NSA acquired more than 13.25 million Internet transactions through its upstream collection. The slide urged analysts to use both PRISM and upstream collection to obtain information.

Within days of the releases, the intelligence community acknowledged the existence of the programs. In August 2013 the Director of National Intelligence, James Clapper, offered further confirmation, noting that PRISM had been in operation.


FICLOB later confirmed that as of mid-2011, approximately 94% of Internet communications obtained each year came through PRISM. FICLOB REPORT, supra note 2, at 54.
since Congress had passed the 2008 FISA Amendments Act, He declassified eight documents, and by the end of the month, he had announced that the intelligence community would release the total number of Section 702 orders issued, and targets thereby affected, on an annual basis.

Although much of the information about PRISM and upstream collection remains classified, what has been made public suggests that these programs push statutory language to its limit, even as they raise critical Fourth Amendment concerns. Accordingly, this Article proceeds in three sections:

Section 702

the evolution of Section 702, a statutory analysis of PRISM and upstream collection, and the attendant constitutional concerns.

The Article begins by considering the origins of the current programs and the relevant authorities—particularly the transfer of part of the President’s Surveillance Program, instituted just after 9/11, to the 1978 Foreign Intelligence Surveillance Act (FISA). It outlines the contours of the 2007 Protect America Act, before its replacement in 2008 by the FISA Amendments Act (FAA).

The section ends with a brief discussion of the current state of foreign intelligence collection under Executive Order 13353, outside either FISA or the FAA.

503
The Article next turns to statutory issues related to targeting, post-targeting analysis, and the retention and dissemination of information. It argues that the NSA has sidestepped FAA restrictions by adopting procedures that allow analysts to acquire information not just to or from, but also "about" targets. In its foreignness determination the agency assumes, absent evidence to the contrary, that the target is a non-U.S. person located outside domestic bounds. And weak standards mark the foreign intelligence purpose determination. Together, these elements allow for the broad collection of U.S. persons' international communications, even as they open the door to the interception of domestic communications. In regard to post-targeting analysis, the Article draws attention to the intelligence community's use of U.S. person information to query data obtained under §702, effectively bypassing protections Congress introduced to prevent reverse targeting. The Article further notes in relation to retention and dissemination that increasing consumer and industrial reliance on cryptography means that the NSA's retention of encrypted data may soon become the exception that swallows the rule.

In its constitutional analysis, the Article finds certain practices instituted under §702 to fall outside acceptable Fourth Amendment bounds. Although lower courts had begun to recognize a domestic foreign intelligence exception to the warrant clause, in 1978 Congress introduced FISA to be the sole means via which domestic foreign intelligence electronic intercepts could be undertaken. Consistent with separation of powers doctrine, this shift carried constitutional meaning. Internationally, practice and precedent prior to the FAA turned on a foreign intelligence exception. But in 2008 Congress altered the status quo, introducing individualized judicial review into the process. Like FISA, the FAA carried constitutional import.

If that were the end of the story, one could argue that the incidental collection of U.S. persons' information, as well as the interception of domestic conversations ought to be regarded in Justice Jackson's third category under Youngstown Sheet & Tube Co. v. Sawyer. Renewal in 2012, however, points in the opposite direction. The NSA's actions, for purposes of the warrant clause, appear to be constitutionally sufficient insofar as foreign intelligence gathering to or from non-U.S. persons is concerned. The tipping point comes with regard to criminal prosecution. Absent a foreign intelligence purpose, there is no exception to the warrant requirement for the query of U.S. persons' international or domestic communications.

Although a warrant is not required for foreign intelligence collection overseas, the interception of communications under §702 must still comport with the reasonableness requirements of the Fourth Amendment. A totality of the circumstances test, in which the significant governmental interest in national security is weighed against the potential intrusion into U.S. persons' privacy, applies. The incidental collection of large quantities of U.S. persons' international communications, the scanning of content for information "about" non-U.S. person targets, and the interception of non-relevant and entirely domestic communications in multi-communication transactions, as well as the query of data using U.S. person identifiers, fall outside the reasonableness component of the Fourth Amendment.

The Article concludes by calling for renewed efforts to draw a line between foreign intelligence gathering and criminal law and to create higher protections for U.S. persons, to ensure that the United States can continue to collect critical information, while remaining consistent with the right to privacy embedded in the Fourth Amendment.

*Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 397 (1952).*
LENS Conference 2014: LAWshaping in National Security

Keynote Speech: Hon. Robert S. Litt, General Counsel, Office the Director of National Intelligence
February 28, 2014

Thank you for that generous introduction. And thanks for inviting me to speak here today, even after my speech here four years ago.

About seven months ago – six weeks after the press began publishing classified documents that Edward Snowden stole – I gave a speech at the Brookings Institution. In that speech, I focused on two intelligence collection programs that had been the subject of leaks – the bulk collection of telephone metadata pursuant to Section 215 of the USA-PATRIOT Act, and the targeting of communications of non-Americans located outside the United States pursuant to Section 702 of the Foreign Intelligence Surveillance Act. I suggested that in a time of rapidly changing technology and expectations of privacy, and of a massive explosion of information, the best way to protect both national security on the one hand, and privacy, civil liberties and constitutional rights on the other hand, was through a system of strict regulation and oversight over the way the Intelligence Community collects, retains and disseminates information, and I described how that system works with reference to those programs.

No doubt you will be relieved to hear that I don’t intend to go over the ground I covered in my earlier speech. If you are interested, you can find it on the website we set up to post material relating to surveillance, www.icontherecord.tumblr.com. But much has happened since last July. The leaks have continued, becoming more and more damaging to our national security, as they focus more and more on the specific sources, methods and targets of intelligence collection, and less and less on policy issues. The President’s Review Group on Intelligence and Communications Technologies and the Privacy and Civil Liberties Oversight Board have issued reports and made recommendations. The Director of National Intelligence has declassified dozens of formerly classified documents, including a number of significant opinions of the Foreign Intelligence Surveillance Court. Numerous bills have been introduced in Congress.
Foreign governments and the EU have expressed significant concerns that have spilled over to affect bilateral and multilateral relations. The President has issued a directive instituting certain changes in how we conduct signals intelligence and has ordered that further changes be considered. But I don’t think that anything that has happened has undercut the central thesis in my speech – or demonstrated that the procedures we have in place are insufficient to protect privacy and civil liberties. In fact, it is noteworthy that in all the material that has been leaked so far, there is no evidence of any systematic abuses, of willful attempts to violate the law, or of the use of intelligence for political or other improper purposes. Nothing that has been revealed approaches the abuses of intelligence that were revealed in the 1970s, and any comparison to those abuses is reckless hyperbole.

I’d like to step back from the daily leaks – many of which have been inaccurate or sensationalized – and talk about some broader issues that the events of the last few months have raised. In particular, I’d like to consider some questions about how intelligence should operate in an era of “big data”; about the manner in which intelligence activities should be regulated and overseen; and about the importance and difficulties of transparency in an inherently and necessarily secret enterprise.

I. The Promise and Problem of Big Data

I want to begin by talking about the promise, and the problem, of big data. I should begin by cautioning that I’m not an engineer, or an analyst – I’m just a lawyer. For a layman like me, it’s not easy to define what big data is. A post at the MIT Review of Technology last October listed half a dozen or more different definitions. It is surely a coincidence unrelated to commercial interests that Microsoft’s proposed definition talked about the use of “serious computing power” while Oracle’s talked about relational databases.1

For today, I think that the most useful approach focuses on what can be done with data. Big data doesn’t just mean a lot of data. It’s large quantities of data, often from different sources, often unstructured or structured and formatted in different ways, but that can be analyzed and evaluated using sophisticated tools to reveal interesting and provocative

information or correlations that would otherwise be invisible or obscured. And in the context of intelligence collection and analysis, it means in particular data that may contain large amounts of non-pertinent information along with information that is of legitimate foreign intelligence value.

The amount and variety of information that exists today is staggering. According to one study conducted in 2012, every day 2.5 exabytes of data – I think that’s 2.5 billion billion bytes – are created. That’s equivalent to filling up almost sixty billion iPads, every day. By another estimate, 90 percent of the digital data existing today was created in just the last two years. Where is all this data? Well, just to give a few examples, data is available from commercial brokers; from publicly available sources such as social media; from private or public surveillance cameras; from communications and communications metadata; or is already in the government’s possession because it is lawfully collected.

Private companies have been using big data for some time to answer questions that were previously too difficult for them to answer with traditional data science. Retailers use it to figure out how prices, demographics, economic indicators, Internet use, and even the weather all come together to impact sales. Financial firms use it to identify potentially fraudulent activity. Social media companies use it to target ads on their sites so that you’re more likely to click on them.

But if big data is useful to private companies, you can imagine its appeal for intelligence professionals, whose job it is to uncover hidden information. Within the huge mass of information that is generated every day is information that we can use to disrupt terror plots, find foreign spies, detect illicit transfers of nuclear weapons and stop cyber attacks. Big data solutions could help us sort through this information and deal with these challenges – challenges which, for the sake of our nation and our allies, we need to meet head on.

Let me give you a couple of examples. In recent months we have all become familiar with the concept of communications metadata. This is information about communications, such as the number dialed and the length of the call – not the substance of the communications and not the identity of the persons who are communicating – but it can nonetheless be very valuable to intelligence analysts. When collected and analyzed in bulk, this can be a kind of “big data.” For example, if we collected large amounts of metadata about foreign telephone calls, we could make


\[3\] Id.
targeted queries based on information about persons we have already identified as potential threats. But another way we could use metadata about foreign calls is to compare it with other databases of lawfully collected information and employ big data tools to see if new insights emerge. Sophisticated analysis of metadata could help us identify terrorists or other persons of interest as a basis for further inquiry – and thus help appropriately and narrowly focus how we use other forms of intelligence collection.

Another potentially fruitful use of big data comes from the explosion of open source information publicly available on social media. In the aftermath of the Arab Spring, numerous commentators pointed out the important role that social media played in that region-wide social upheaval. Analysis of this information can help give policy makers early warning and deeper understanding of trends around the world. For example, just two weeks ago IARPA – the Intelligence Advanced Research Projects Activity, which is basically the intelligence version of the better-known DARPA – reported that by monitoring publicly available information, it was able to identify outbreaks of disease as much as two weeks before they were reported in local media or by health agencies.4

At the same time, there are obvious and legitimate concerns about permitting our intelligence services to collect and analyze large datasets that by definition will include a great deal of information about persons who are not foreign intelligence targets. The same capabilities that allow intelligence analysts to extract important information about terrorists, spies or cyber threats from large quantities of data could be abused to extract information about ordinary people. Looked at in this light, “big data” can start to sound like “big brother.” That’s not necessarily the case – in fact, because big data is all about looking at large amounts of data, it doesn’t necessarily require tying information to identifiable individuals. Patterns can emerge without the need to examine, or investigate, the individual dots that make up the pattern. But there’s no doubt that the collection and analysis of big data by the Intelligence Community poses concerns that are different than those posed by more traditional targeted collection and analysis. That’s one reason that the government has moved more slowly than the private sector in this area.

---

The question, then, is what do we want our Intelligence Community to do with big data? On the one hand, we could conclude, as some advocate, that the collection and analysis of large amounts of data is inherently so dangerous and susceptible of abuse that we should bar the Intelligence Community from using it at all. The other approach is to recognize the promise as well as the problem of big data, and to allow its use subject to regulation and oversight. I expect that my framing of the problem suggests how I would answer it, but I want to explore the issue in a bit more depth.

The first approach essentially asks our nation to forgo the possible benefits of big data for intelligence purposes because of the risks to privacy and civil liberties. There is, of course, a real risk that any intelligence tool can be abused or misused in the future, and I do not want to downplay that risk. But the risk of misuse exists with any tool, with any authority, and with any person using that tool or authority. That’s why over the last few decades we have erected elaborate and multi-layered oversight of the Intelligence Community. And this oversight works: the Intelligence Community’s record of compliance in recent years, while not spotless, does not reflect any systematic abuses.

There are, of course, legal limits, imposed by the Constitution and statutory law, on what we can do with big data. To pick one relatively easy example, the Fourth Amendment would prevent the government from collecting the content of all communications taking place within the United States, no matter how useful that might be for law enforcement or intelligence purposes. So as I discuss this issue, I’m going to assume that we are talking about using big data in a manner that is consistent with the law.

In my view, telling the Intelligence Community that it cannot collect and analyze big data because of the risks of misuse is a bit like someone going to Kitty Hawk in December 1903, watching Orville and Wilbur Wright fly a flimsy wood and fabric contraption ten feet off the ground for a hundred feet, and deciding that this “aeroplane” is way too dangerous, and its potential benefits far too speculative. That’s about the stage we are at in our understanding of what can be done with big data – and how our use of that data can be made safer. Moreover, as with airplanes in 1903, the United States is not the only nation seeking to make use of big data in furtherance of its national interests. As Senator Sheldon Whitehouse said in December, at a Judiciary Committee hearing where I testified, “[i]f we were to pass a law that prevented our
intelligence and defense establishment from operating in [the] big data atmosphere, we would be essentially unilaterally disarming in an arena where other governments are very active.\textsuperscript{5}

Consideration of the appropriate role of big data in our democratic society reflects the changing nature of privacy in the information age. Today we share an enormous amount of personal and sensitive data with private companies and often with the entire Internet-connected world, yet many of us want this information to be treated as "private" for many purposes. In particular, as I said at Brookings, we feel very differently about sharing large amounts of information with private companies, and sharing the same information with the government, not because of the nature of the information itself but because of what the government could do with the information.

I don't think it's going to be very productive for us to pretend that big data doesn't exist, or to try to wish it away. The Luddites did not win; mechanized textile manufacturing carried the day. The more prudent, if less simple, approach is to deal with the problem where it exists. If we are concerned about how the government can use information, let us craft sensible limits on the way that information is used, for what purposes, and by whom, so that we can all be more confident that we are protecting both national security and privacy.

At the end of the day we need to determine whether there is a system of controls and oversight that gives us comfort that our intelligence services are using big data appropriately. I believe that there could be such a system. We could impose strict limits on the purpose for which big data may be used, the types of analysis that can be done against it, and how it could be disseminated to others. Approval and review processes could be designed to ensure that big data was used only in conformity with the limits we establish. We could use technological tools to restrict and monitor access to the data to enforce those restrictions. We could place limits on how long data can be stored in our databases. And we could use our existing compliance and oversight framework to proactively discover mistakes and quickly fix them.

If this approach sounds familiar, it's because this is what the Intelligence Community already does. In fact, it's precisely the approach that we took in the bulk telephony metadata program, as I laid out at Brookings. This regulatory framework goes well beyond the controls

that most, if not all, of the private sector has with respect to its use of information. While NSA has had well-publicized technical challenges in implementing the bulk telephone metadata program, these problems were self-identified, self-reported and self-remedied, thanks to its robust compliance and oversight system. And while the telephone metadata program has been criticized, and the President has determined that it will be ended in its current form, no one who has looked at it – not the Review Group, not the Privacy and Civil Liberties Oversight Board, not the President – has suggested that it was in any way abused. I think that this model is the right way to approach the problem and the promise of big data.

II. The Challenge of Oversight and Transparency

You may have noticed that a few minutes ago I talked about decisions “we” might make about how to regulate and oversee the Intelligence Community’s use of big data. This of course begs the question: who is “we” in this context? The problem is a familiar one. Intelligence must by its very nature be conducted in secret in order to be effective. We simply cannot advertise what we are collecting, who we are collecting from and how we collect it without compromising our ability to protect the nation. At the same time, the nature of the intelligence business, and the potential (and actual history) of abuse, requires strong and credible oversight to provide assurance to the public.

Since the 1970s, when the Church and Pike Committees exposed genuine abuses by the Intelligence Community, that oversight has been accomplished through the select committees on intelligence of the House and Senate. By law, we are required to keep these committees fully and currently informed of intelligence activities, and we do. We provide them hundreds of finished intelligence products, dozens of written notifications each month, and dozens more briefings, covering the full range of activities from covert actions, to satellite construction, to personnel matters, to the most recent information about the state of affairs in Ukraine or Syria, and including our intelligence collection programs. The Intelligence Committees also exercise oversight through annual authorization bills and the classified annexes to those bills, which often provide very detailed prescriptions, directives and reporting requirements. Much of this takes place in a classified format, and a small portion of the most sensitive material is briefed only to Committee leadership, but the Intelligence Community takes its obligations to the committees extremely seriously. In effect, the Intelligence Committees act as the people’s authorized agents
and representatives in overseeing intelligence. But their oversight, just like the activities they oversee, must largely be conducted in secret.

In addition to Congressional oversight, there is oversight within the Executive Branch and from the judiciary. Within the Executive Branch, oversight of intelligence activities is conducted by Inspectors General, General Counsels, Privacy and Civil Liberties Officers, and the Department of Justice – and a culture of compliance is instilled in every intelligence officer. And as the recently declassified opinions make clear, the FISA Court’s oversight of activities within its jurisdiction is real and searching. Indeed, at the President’s direction and with the Court’s consent, its role in oversight of the bulk telephone metadata program has recently been enhanced; the Court must now review any proposed query of that data to determine that it is appropriately based on a reasonable, articulable suspicion of a link to terrorism. All in all, I believe that the oversight of America’s intelligence activities that exists today, involving all three branches of government, is far more extensive and effective than any other in the world.

In the wake of Snowden’s leaks, each of the pillars of this oversight structure has been called into question. The FISA Court has been called a rubber stamp. The Executive Branch has been accused of whitewashing problems. Some Members of Congress have claimed that they were uninformed of important matters and have criticized the oversight by the Intelligence Committees. And the media and advocacy groups have called for much greater disclosure of information about collection programs than has been the norm in the past. In short, the entire question of how intelligence activities should be overseen has been reopened.

This discussion is going to play out over the coming months, but I want to offer some observations on each of these issues. I want to emphasize that these are my own thoughts and don’t necessarily represent the view of the ODNI, the Intelligence Community or the Administration, but I hope that they’ll provoke some thought.

Let me start with the FISA Court. There have been a number of proposals for reform of how the court operates, including changing the process by which judges are selected for the Court, allowing the participation of independent advocates in some cases, and requiring greater disclosure of Court opinions. I believe that these proposals should be considered with a few general principles in mind.
First, it's important to remember that the FISA Court is a unique institution. Historically, the conduct of foreign intelligence has been viewed as a core responsibility of the President, and I know of no other country that has the same degree of judicial involvement in the authorization and oversight of foreign intelligence.

Second, because of this unique role, and the classified nature of the activities it oversees, the FISA Court is not like other courts. When thinking about how to change it, we should not take as our lodestar a traditional, Perry Mason-like adversary proceeding. Even in other courts, proceedings relating to the gathering of evidence — such as the issuance of search warrants or electronic surveillance orders — are typically conducted ex parte and in secret, even when they may involve important legal or constitutional issues.

Third, we have made significant strides in providing public insight into the workings of the Court, by declassifying and releasing many of its significant opinions and orders. The FISA Court itself has also published detailed descriptions of how it does its business. The process of releasing opinions was under way even before the leaks began, and appropriately so. But reviewing a document to determine what can be released consistent with national security is a complicated task, and I must admit that in this instance, the illegal disclosure of these programs affected the balance between transparency and national security. Even apart from the impact of these leaks, we are continuing to review additional documents for release, in the interest of providing as much information as we can consistent with national security.

Finally, and I want to emphasize this point, the FISA Court has operated effectively, independently, and appropriately. The opinions that have been released show that the criticisms of the Court as a "rubber stamp" are plainly and simply wrong. While it's true that the Court makes its decisions ex parte and in secret, it's also true that it has outstanding, experienced judges, and a capable professional staff that provides searching review of the government's submissions. These are the same judges, after all, who have written opinions bluntly criticizing the way that we have handled certain compliance incidents.

Having said that, I recognize that — in part because of uninformed criticism — we need to take steps to restore public confidence in the Court. For this reason, the Administration supports proposals to provide for a panel of cleared lawyers that the Court could call upon to provide
independent advocacy in cases involving significant issues. Hopefully, this will ensure that the public’s perception of the Court’s independence and integrity matches the reality.

Similarly, regaining the public’s trust may require that we establish more oversight of intelligence activities within the Executive Branch. The more people who are watching over intelligence activities, the harder it is for anyone to abuse their authorities. The President has already directed that some changes be made to strengthen Executive Branch oversight of intelligence activities, including annual reviews of intelligence priorities and sensitive targets, and to ensure that we take into account the risks as well as the benefits of signals intelligence activities.

But increased oversight comes with costs. Intelligence is already, as my colleague Stephen Preston has said, essentially a regulated business, and just as with any other business, more regulation produces more complexity. We should not impose so much regulation and oversight on our intelligence officers that it stifles their ability and willingness to be creative and aggressive, within the law, in defense of our nation. I’m reminded of a comment about Bobby Knight – if I can mention that name in this town. Supposedly, he was so overbearing that his players ran up court on the fast break looking back for instructions. We shouldn’t want our intelligence officers to work that way. And we should also bear in mind that the more rules and processes we create, the more opportunities we create for violations of those rules. Intelligence officers aren’t lawyers; they need to understand clearly what they can and cannot do. So we need to find the sweet spot of appropriate regulation and oversight that does not bog down a necessary element of our national security.

Let me turn now to the issue of Congressional oversight. As I said earlier, the accommodation that we have made as a nation between the need for oversight and the need for secrecy has been to empower the Congressional intelligence committees to serve as the representatives of the public. I think that this is a wise approach. Intelligence is a complicated business and one that must be kept isolated from partisan political pressure. The Intelligence Committees, with their tradition of nonpartisanship and their experienced and knowledgeable staff, have been pretty good at that. But the historic accommodation is now under great stress, in

---

part from some Members of Congress who have said that they were not adequately informed of intelligence operations, and in part from critics who believe that the intelligence committees are not sufficiently vigorous in their oversight.

Let’s be clear about a couple of things. We informed the Intelligence Committees – as well as the Judiciary Committees – about the bulk telephone metadata collection and the 702 collection, as we were required to do. And while some members of the committees raised questions about these programs, the great majority of the committee members supported them after the concerns were fully debated. The real complaint of many critics is not that oversight was inadequate, but that they disagree with the result that the authorized oversight process reached. That’s an issue of policy, not oversight.

Second, the charge that Congress was not informed about these collection programs is entirely, and in some instances hypocritically, misplaced. As I have said before, we did make information about these programs available to every Member of Congress at the time the relevant statutes were reauthorized, and there are even statements in the Congressional Record urging Members to go review that information. Any change in the way in which Congress oversees intelligence activities should take into account whether those who would conduct the oversight are willing to take the time to understand the activities that they would be overseeing.

Finally, I want to talk about transparency. The value of transparency is more than a little counterintuitive to agencies whose operations are dependent on secrecy, but I think that the events of the last few months have taught the Intelligence Community that we need to lean as far forward as we can in disclosing information about what we do. As a result, we have been more open than ever before. We’ve declassified thousands of pages of documents, we’ve testified at open hearings, and we have allowed providers to make significant disclosures as well. The President has made clear that he wants this openness to continue and it will. Greater public disclosure is necessary to restore the American people’s trust that intelligence activities are not only lawful and important to protecting our national security, but that they are appropriate and proportional in light of the privacy interests at stake. In the long run, our ability to protect the public requires that we have the public’s support.

But lines must be drawn. First and foremost, we cannot allow transparency to compromise our sources and methods. We must continue to protect information about the
specific targets of our intelligence collection, the specific methods by which we accomplish that collection, and the specifics of the intelligence we collect. Were we to announce to the world that we have the ability, for example, to intercept emails sent using particular email services, we would enable terrorists, cyber criminals, foreign intelligence officers and other foreign intelligence targets to migrate to other email services so that they could communicate without fear of detection. We may never know what we are missing until it is too late. We can be, and we will be, more transparent about how we interpret certain laws to support our activities, about the procedures and oversight we have in place to ensure that our intelligence activities are lawful and appropriate, and about the degree to which we have followed the law and our policies, but if intelligence is too transparent it is useless or worse.

I think that greater transparency about our processes could help us cope with one of the principal failings I see in the current discussion of intelligence activities, which is the failure to distinguish among what the Intelligence Community can do technically, what it can do legally and what it actually does. Too much of the recent discussion has focused on technical capabilities — which are often fascinating — while leaving a misleading impression of actual activities.

For example, there have been press reports that NSA has engaged in a concerted effort to break encryption codes. Without commenting on the truth of these stories . . . isn’t that exactly what intelligence agencies have historically done, and what they are supposed to do? We know that our enemies use encryption and other techniques precisely to avoid surveillance; NSA’s job is to figure out how to break those techniques, and its capabilities are unmatched. But saying that NSA can break encryption is different from saying that they routinely spy on encrypted conversations of ordinary Americans or foreigners. They don’t; all of NSA’s technical expertise is brought to bear in furtherance of its authorized foreign intelligence mission and within the law. But it is difficult to push back against these mischaracterizations if the basic procedural framework that makes clear what the limits are and how those limits are enforced is being wholly shielded from public view.

And this leads to the other question I want to raise about transparency, which is who is responsible for deciding what should be secret and what should be public. Decisions about what can be disclosed consistent with the national interest require an appreciation of both sides of the
equation: both the value of transparency and the value of secrecy. In my opinion, we cannot survive as a nation if we let those decisions be made by individuals who cannot fully comprehend the implications of their actions. The loss of certain intelligence capabilities can result in the waste of millions of dollars, in an inability to give our policymakers the warning that they need to deal appropriately with threats, or, in the worst case, in the loss of lives. That’s why we go through a careful, thorough, deliberative process before we disclose classified information, to ensure that we do not endanger capabilities or lives.

But leakers disrupt this process by taking it upon themselves to decide what should and should not be withheld from public view. They do this without understanding the context for the information that they release, and in willful disregard for the sensitive sources and methods that they are placing in harm’s way. In short, leakers believe that they know more than everyone else, including the legislative and judicial branches of government that have continually endorsed the principle of classification for national security reasons.

Individuals in the Intelligence Community who want to blow the whistle on genuine waste, fraud, and abuse or illegality should do so. We expect and require our people to report cases where they believe the law wasn’t being followed, or where people were acting in ways that violated our internal procedures and guidelines. We have established procedures to allow members of the Intelligence Community to raise their concerns with the appropriate authorities, including Congress, without risking harm to our national security, and without facing reprisals for their disclosures.

But what’s most striking to me about the leaks that have taken place over the past few months is that they’ve really not been about whistleblowing at all. None of the leaks have shown that the government was engaged in any willful violation of law; even those who disagree with some of the legal analysis supporting our activities must acknowledge that they were deemed lawful by the FISA Court, the Department of Justice and the lawyers in the Intelligence Community. None of the leaks have shown that the Intelligence Community was doing things that were hidden from the Congress or the courts. Instead, the leakers’ argument appears to be that the Intelligence Community was engaging in behavior that they disagree with as a matter of policy. That’s hardly a justification for the risks to national security that these leaks have caused.

So let me summarize my main themes today.
Regardless of what critics charge, the Intelligence Community operates within a framework of law and oversight. As we contemplate the challenge of big data, we should look to apply that same framework, to ensure that we can make appropriate use of the multi-faceted information now available to us – and that we don’t make inappropriate use of it. And as we contemplate changes in how the Intelligence Community is overseen, we should bear in mind how that oversight has operated in the past, and the dangers of imposing so many rules and bureaucratic procedures that the intelligence enterprise becomes ineffective. We need clear and workable rules, rather than simply more rules.

Finally, we recognize that to a degree far beyond what we ever considered before, we must give the public a better and more complete understanding of the processes and procedures we use to guide and regulate our intelligence activities. Public confidence in the way that we conduct our necessarily secret activities is essential if we are to continue to quickly respond to the many, varied, and changing threats our nation faces. Some of our activities must and will remain secret, or we will undermine the security not only of Americans but also the citizens of other countries upon whose support we rely for many of our intelligence activities. But the rigorous oversight that we face from all three branches of Government – together with our commitment to greater transparency – should give some comfort that the Intelligence Community continues to perform its difficult job with full respect for the law and for individuals’ privacy and civil rights.

Thank you.
Privacy, Technology & National Security
An Overview of Intelligence Collection — Robert S. Litt, ODNI General Counsel
July 18, 2013

Remarks as prepared for delivery to the Brookings Institution, Washington, DC.

I. Introduction

I wish that I was here in happier times for the Intelligence Community. The last several weeks have seen a series of reckless disclosures of classified information about intelligence activities. These disclosures threaten to cause long-lasting and irreversible harm to our ability to identify and respond to the many threats facing our Nation. And because the disclosures were made by people who did not fully understand what they were talking about, they were sensationalized and led to mistaken and misleading impressions. I hope to be able to correct some of these misimpressions today.

My speech today is prompted by disclosures about two programs that collect valuable foreign intelligence that has protected our Nation and its allies: the bulk collection of telephony metadata, and the so-called “PRISM” program. Some people claim that these disclosures were a form of “whistleblowing.” But let’s be clear. These programs are not illegal. They are authorized by Congress and are carefully overseen by the Congressional intelligence and judiciary committees. They are conducted with the approval of the Foreign Intelligence Surveillance Court and under its supervision. And they are subject to extensive, court-ordered oversight by the Executive Branch. In short, all three branches of Government knew about these programs, approved them, and helped to ensure that they complied with the law. Only time will tell the full extent of the damage caused by the unlawful disclosures of these lawful programs.

Nevertheless, I fully appreciate that it’s not enough for us simply to assert that our activities are consistent with the letter of the law. Our Government’s activities must always reflect and reinforce our core democratic values. Those of us who work in the intelligence profession share these values, including the importance of privacy. But security and privacy are not zero-sum. We have an obligation to give full meaning to both: to protect security while at the same time protecting privacy and other constitutional rights. But although our values are enduring, the manner in which our activities reflect those values must necessarily adapt to changing societal expectations and norms. Thus, the Intelligence Community continually evaluates and improves the safeguards we have in place to protect privacy, while at the same time ensuring that we can carry out our mission of protecting national security.

So I’d like to do three things today. First, I’d like to discuss very briefly the laws that govern intelligence collection activities. Second, I want to talk about the effect of
changing technology, and the corresponding need to adapt how we protect privacy, on those collection activities. And third, I want to bring these two strands together, to talk about how some of these laws play out in practice—how we structure the Intelligence Community’s collection activities under FISA to respond to these changes in a way that remains faithful to our democratic values.

II. Legal Framework

Let me begin by discussing in general terms the legal framework that governs intelligence collection activities. And it is a bedrock concept that those activities are bound by the rule of law. This is a topic that has been well addressed by others, including the general counsels of the CIA and NSA, so I will make this brief. We begin, of course, with the Constitution. Article II makes the President the Commander in Chief and gives him extensive responsibility for the conduct of foreign affairs. The ability to collect foreign intelligence derives from that constitutional source. The First Amendment protects freedom of speech. And the Fourth Amendment prohibits unreasonable searches and seizures.

I want to make a few points about the Fourth Amendment. First, under established Supreme Court rulings a person has no legally recognized expectation of privacy in information that he or she gives to a third party. So obtaining those records from the third party is not a search as to that person. I’ll return to this point in a moment. Second, the Fourth Amendment doesn’t apply to foreigners outside of the United States. Third, the Supreme Court has said that the “reasonableness” of a warrantless search depends on balancing the “intrusion on the individual’s Fourth Amendment interests against” the search’s “promotion of legitimate Governmental interests.” (1)

In addition to the Constitution, a variety of statutes govern our collection activities. First, the National Security Act and a number of laws relating to specific agencies, such as the CIA Act and the NSA Act, limit what agencies can do, so that, for example, the CIA cannot engage in domestic law enforcement. We are also governed by laws such as the Electronic Communications Privacy Act, the Privacy Act and, in particular, the Foreign Intelligence Surveillance Act, or FISA. FISA was passed by Congress in 1978 and significantly amended in 2001 and 2008. It regulates electronic surveillance and certain other activities carried out for foreign intelligence purposes. I’ll have much more to say about FISA later.

A final important source of legal restrictions is Executive Order 12333. This order provides additional limits on what intelligence agencies can do, defining each agency’s authorities and responsibilities. In particular, Section 2.3 of EO 12333 provides that elements of the Intelligence Community “are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures … approved by the Attorney General … after consultation with” the Director of National Intelligence. These procedures must be consistent with the agencies’ authorities. They must also establish strict limits on collecting, retaining or disseminating information
about U.S. persons, unless that information is actually of foreign intelligence value, or in certain other limited circumstances spelled out in the order, such as to protect against a threat to life. These so-called “U.S. person rules” are basic to the operation of the Intelligence Community. They are among the first things that our employees are trained in, and they are at the core of our institutional culture.

It’s not surprising that our legal regime provides special rules for activities directed at U.S. persons. So far as I know, every nation recognizes legal distinctions between citizens and non-citizens. But as I hope to make clear, our intelligence collection procedures also provide protection for the privacy rights of non-citizens.

III. Impact of Changing Societal Norms

Let me turn now to the impact of changing technology on privacy. Prior to the end of the nineteenth century there was little discussion about a “right to privacy.” In the absence of mass media, photography and other technologies of the industrial age, the most serious invasions of privacy were the result of gossip or Peeping Toms. Indeed, in the 1890 article that first articulated the idea of a legal right to privacy, Louis Brandeis and Samuel Warren explicitly grounded that idea on changing technologies: Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right “to be let alone.” Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that “what is whispered in the closet shall be proclaimed from the house-top.” (2)

Today, as a result of the way digital technology has developed, each of us shares massive amounts of information about ourselves with third parties. Sometimes this is obvious, as when we post pictures on social media or transmit our credit card numbers to buy products online. Other times it is less obvious, as when telephone companies store records listing every call we make. All in all, there’s little doubt that the amount of data that each of us provides to strangers every day would astonish Brandeis and Warren—let alone Jefferson and Madison.

And this leads me to what I consider to be the key question. Why is it that people are willing to expose large quantities of information to private parties but don’t want the Government to have the same information? Why, for example, don’t we care if the telephone company keeps records of all of our phone calls on its servers, but we feel very differently about the prospect of the same information being on NSA servers? This does not seem to me to be a difficult question: we care because of what the Government could do with the information.

Unlike a phone company, the Government has the power to audit our tax returns, to prosecute and imprison us, to grant or deny licenses to do business, and many other things. And there is an entirely understandable concern that the Government may abuse
this power. I don’t mean to say that private companies don’t have a lot of power over us. Indeed, the growth of corporate privacy policies, and the strong public reaction to the inadvertent release or commercial use of personal information, reinforces my belief that our primary privacy concern today is less with who has information than with what they do with it. But there is no question that the Government, because of its powers, is properly viewed in a different light.

On the other hand, just as consumers around the world make extensive use of modern technology, so too do potentially hostile foreign governments and foreign terrorist organizations. Indeed, we know that terrorists and weapons proliferators are using global information networks to conduct research, to communicate and to plan attacks. Information that can help us identify and prevent terrorist attacks or other threats to our security is often hiding in plain sight among the vast amounts of information flowing around the globe. New technology means that the Intelligence Community must continue to find new ways to locate and analyze foreign intelligence. We need to be able to do more than connect the dots when we happen to find them; we need to be able to find the right dots in the first place.

One approach to protecting privacy would be to limit the Intelligence Community to a targeted, focused query looking for specific information about an identified individual based on probable cause. But from the national security perspective, that would not be sufficient. The business of foreign intelligence has always been fundamentally different from the business of criminal investigation. Rather than attempting to solve crimes that have happened already, we are trying to find out what is going to happen before it happens. We may have only fragmentary information about someone who is plotting a terrorist attack, and need to find him and stop him. We may get information that is useless to us without a store of data to match it against, such as when we get the telephone number of a terrorist and want to find out who he has been in touch with. Or we may learn about a plot that we were previously unaware of, causing us to revisit old information and find connections that we didn’t notice before—and that we would never know about if we hadn’t collected the information and kept it for some period of time. We worry all the time about what we are missing in our daily effort to protect the Nation and our allies.

So on the one hand there are vast amounts of data that contains intelligence needed to protect us not only from terrorism, but from cyber attacks, weapons of mass destruction, and good old-fashioned espionage. And on the other hand, giving the Intelligence Community access to this data has obvious privacy implications. We achieve both security and privacy protection in this context in large part by a framework that establishes appropriate controls on what the Government can do with the information it lawfully collects, and appropriate oversight to ensure that it respects those controls. The protections depend on such factors as the type of information we collect, where we collect it, the scope of the collection, and the use the Government intends to make of the information. In this way we can allow the Intelligence Community to acquire necessary foreign intelligence, while providing privacy protections that take account of modern technology.
IV. FISA Collection

In showing that this approach is in fact the way our system deals with intelligence collection, I’ll use FISA as an example for a couple of reasons. First, because FISA is an important mechanism through which Congress has legislated in the area of foreign intelligence collection. Second, because it covers a wide range of activities, and involves all three sources of law I mentioned earlier: constitutional, statutory and executive. And third, because several previously classified examples of what we do under FISA have recently been declassified, and I know people want to hear more about them.

I don’t mean to suggest that FISA is the only way we collect foreign intelligence. But it’s important to know that, by virtue of Executive Order 12333, all of the collection activities of our intelligence agencies have to be directed at the acquisition of foreign intelligence or counterintelligence. Our intelligence priorities are set annually through an interagency process. The leaders of our Nation tell the Intelligence Community what information they need in the service of the Nation, its citizens and its interests, and we collect information in support of those priorities.

I want to emphasize that the United States, as a democratic nation, takes seriously this requirement that collection activities have a valid foreign intelligence purpose. We do not use our foreign intelligence collection capabilities to steal the trade secrets of foreign companies in order to give American companies a competitive advantage. We do not indiscriminately sweep up and store the contents of the communications of Americans, or of the citizenry of any country.

We do not use our intelligence collection for the purpose of repressing the citizens of any country because of their political, religious or other beliefs. We collect metadata—information about communications—more broadly than we collect the actual content of communications, because it is less intrusive than collecting content and in fact can provide us information that helps us more narrowly focus our collection of content on appropriate targets. But it simply is not true that the United States Government is listening to everything said by every citizen of any country.

Let me turn now to FISA. I’m going to talk about three provisions of that law: traditional FISA orders, the FISA business records provision, and Section 702. These provisions impose limits on what kind of information can be collected and how it can be collected, require procedures restricting what we can do with the information we collect and how long we can keep it, and impose oversight to ensure that the rules are followed. This sets up a coherent regime in which protections are afforded at the front end, when information is collected; in the middle, when information is reviewed and used; and at the back end, through oversight, all working together to protect both national security and privacy. The rules vary depending on factors such as the type of information being collected (and in particular whether or not we are collecting the content of communications), the nature of the person or persons being targeted, and how narrowly or broadly focused the collection is. They aren’t identical in every respect to the rule that apply to criminal investigations,
but I hope to persuade you that they are reasonable and appropriate in the very different context of foreign intelligence.

So let’s begin by talking about traditional FISA collection. Prior to the passage of FISA in 1978, the collection of foreign intelligence was essentially unregulated by statutory law. It was viewed as a core function of the Executive Branch. In fact, when the criminal wiretap provisions were originally enacted, Congress expressly provided that they did not “limit the constitutional power of the President ... to obtain foreign intelligence information ... deemed essential to the national security of the United States.” (3) However, ten years later, as a result of abuses revealed by the Church and Pike Committees, Congress imposed a judicial check on some aspects of electronic surveillance for foreign intelligence purposes. This is what is now codified in Title I of FISA, sometimes referred to as “traditional FISA.”

FISA established a special court, the Foreign Intelligence Surveillance Court, to hear applications by the Government to conduct electronic surveillance for foreign intelligence purposes. Because traditional FISA surveillance involves acquiring the content of communications, it is intrusive, implicating recognized privacy interests; and because it can be directed at individuals inside the United States, including American citizens, it implicates the Fourth Amendment. In FISA, Congress required that to get a “traditional” FISA electronic surveillance order, the Government must establish probable cause to believe that the target of surveillance is a foreign power or an agent of a foreign power, a probable cause standard derived from the standard used for wiretaps in criminal cases. And if the target is a U.S. person, he or she cannot be deemed an agent of a foreign power based solely on activity protected by the First Amendment—you cannot be the subject of surveillance merely because of what you believe or think.

Moreover, by law the use of information collected under traditional FISA must be subject to minimization procedures, a concept that is key throughout FISA. Minimization procedures are procedures, approved by the FISA Court, that must be “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.” (4) For example, they generally prohibit disseminating the identity of a U.S. person unless the identity itself is necessary to understand the foreign intelligence or is evidence of a crime. The reference to the purpose and technique of the particular surveillance is important. Minimization procedures can and do differ depending on the purpose of the surveillance and the technique used to implement it. These tailored minimization procedures are an important way in which we provide appropriate protections for privacy.

So let me explain in general terms how traditional FISA surveillance works in practice. Let’s say that the FBI suspects someone inside the United States of being a spy, or a terrorist, and they want to conduct electronic surveillance. While there are some exceptions spelled out in the law, such as in the case of an emergency, as a general rule
they have to present an application to the FISA Court establishing probable cause to believe that the person is an agent of a foreign power, according to the statutory definition. That application, by the way, is reviewed at several levels within both the FBI and Department of Justice before it is submitted to the Court. Now, the target may have a conversation with a U.S. person that has nothing to do with the foreign intelligence purpose of the surveillance, such as talking to a neighbor about a dinner party.

Under the minimization procedures, an analyst who listens to a conversation involving a U.S. person that has no foreign intelligence value cannot generally share it or disseminate it unless it is evidence of a crime. Even if a conversation has foreign intelligence value—let’s say a terrorist is talking to a confederate—that information may only be disseminated to someone with an appropriate need to know the information pursuant to his or her mission.

In other words, electronic surveillance under FISA’s Title I implicates the well-recognized privacy interest in the contents of communications, and is subject to corresponding protections for that privacy interest—in terms of the requirements that it be narrowly targeted and that it have a substantial factual basis approved by the Court, and in terms of the limitations imposed on use of the information.

Now let me turn to the second activity, the collection of business records. After FISA was passed, it became apparent that it left some significant gaps in our intelligence collection authority. In particular, while the Government had the power in a criminal investigation to compel the production of records with a grand jury subpoena, it lacked similar authority in a foreign intelligence investigation. So a provision was added in 1998 to provide such authority, and was amended by Section 215 of the USA-PATRIOT Act passed shortly after 9/11. This provision, which is generally referred to as “Section 215,” allows us to apply to the FISA Court for an order requiring production of documents or other tangible things when they are relevant to an authorized national security investigation. Records can be produced only if they are the type of records that could be obtained pursuant to a grand jury subpoena or other court process—in other words, where there is no statutory or other protection that would prevent use of a grand jury subpoena. In some respects this process is more restrictive than a grand jury subpoena. A grand jury subpoena is issued by a prosecutor without any prior judicial review, whereas under the FISA business records provision we have to get court approval. Moreover, as with traditional FISA, records obtained pursuant to the FISA business records provision are subject to court-approved minimization procedures that limit the retention and dissemination of information about U.S. persons—another requirement that does not apply to grand jury subpoenas.

Now, of course, the FISA business records provision has been in the news because of one particular use of that provision. The FISA Court has repeatedly approved orders directing several telecommunications companies to produce certain categories of telephone metadata, such as the number calling, the number being called, and the date, time and duration of the call. It’s important to emphasize that under this program we do not get the
content of any conversation; we do not get the identity of any party to the conversation; and we do not get any cell site or GPS locational information.

The limited scope of what we collect has important legal consequences. As I mentioned earlier, the Supreme Court has held that if you have voluntarily provided this kind of information to third parties, you have no reasonable expectation of privacy in that information. All of the metadata we get under this program is information that the telecommunications companies obtain and keep for their own business purposes. As a result, the Government can get this information without a warrant, consistent with the Fourth Amendment.

Nonetheless, I recognize that there is a difference between getting metadata about one telephone number and getting it in bulk. From a legal point of view, Section 215 only allows us to get records if they are “relevant” to a national security investigation, and from a privacy perspective people worry that, for example, the government could apply data mining techniques to a bulk data set and learn new personal facts about them—even though the underlying set of records is not subject to a reasonable expectation of privacy for Fourth Amendment purposes.

On the other hand, this information is clearly useful from an intelligence perspective: It can help identify links between terrorists overseas and their potential confederates in the United States. It’s important to understand the problem this program was intended to solve. Many will recall that one of the criticisms made by the 9/11 Commission was that we were unable to find the connection between a hijacker who was in California and an al-Qaida safe house in Yemen. Although NSA had collected the conversations from the Yemen safe house, they had no way to determine that the person at the other end of the conversation was in the United States, and hence to identify the homeland connection. This collection program is designed to help us find those connections.

In order to do so, however, we need to be able to access the records of telephone calls, possibly going back many years. However, telephone companies have no legal obligation to keep this kind of information, and they generally destroy it after a period of time determined solely by their own business purposes. And the different telephone companies have separate datasets in different formats, which makes analysis of possible terrorist calls involving several providers considerably slower and more cumbersome. That could be a significant problem in a fast-moving investigation where speed and agility are critical, such as the plot to bomb the New York City subways in 2009.

The way we fill this intelligence gap while protecting privacy illustrates the analytical approach I outlined earlier. From a subscriber’s point of view, as I said before, the difference between a telephone company keeping records of his phone calls and the Intelligence Community keeping the same information is what the Government could do with the records. That’s an entirely legitimate concern. We deal with it by limiting what the Intelligence Community is allowed do with the information we get under this program—limitations that are approved by the FISA Court:
First, we put this information in secure databases. Second, the only intelligence purpose for which this information can be used is counterterrorism.

Third, we allow only a limited number of specially trained analysts to search these databases.

Fourth, even those trained analysts are allowed to search the database only when they have a reasonable and articulable suspicion that a particular telephone number is associated with particular foreign terrorist organizations that have been identified to the Court. The basis for that suspicion has to be documented in writing and approved by a supervisor.

Fifth, they’re allowed to use this information only in a limited way, to map a network of telephone numbers calling other telephone numbers.

Sixth, because the database contains only metadata, even if the analyst finds a previously unknown telephone number that warrants further investigation, all she can do is disseminate the telephone number. She doesn’t even know whose number it is. Any further investigation of that number has to be done pursuant to other lawful means, and in particular, any collection of the contents of communications would have to be done using another valid legal authority, such as a traditional FISA.

Finally, the information is destroyed after five years.

The net result is that although we collect large volumes of metadata under this program, we only look at a tiny fraction of it, and only for a carefully circumscribed purpose—to help us find links between foreign terrorists and people in the United States. The collection has to be broad to be operationally effective, but it is limited to non-content data that has a low privacy value and is not protected by the Fourth Amendment. It doesn’t even identify any individual. Only the narrowest, most important use of this data is permitted; other uses are prohibited. In this way, we protect both privacy and national security.

Some have questioned how collection of a large volume of telephone metadata could comply with the statutory requirement that business records obtained pursuant to Section 215 be “relevant to an authorized investigation.” While the Government is working to determine what additional information about the program can be declassified and disclosed, including the actual court papers, I can give a broad summary of the legal basis. First, remember that the “authorized investigation” is an intelligence investigation, not a criminal one. The statute requires that an authorized investigation be conducted in accordance with guidelines approved by the Attorney General, and those guidelines allow the FBI to conduct an investigation into a foreign terrorist entity if there is an “articulable factual basis … that reasonably indicates that the [entity] may have engaged in … international terrorism or other threat to the national security,” or may be planning or supporting such conduct. (5) In other words, we can investigate an organization, not
merely an individual or a particular act, if there is a factual basis to believe the organization is involved in terrorism. And in this case, the Government’s applications to collect the telephony metadata have identified the particular terrorist entities that are the subject of the investigations.

Second, the standard of “relevance” required by this statute is not the standard that we think of in a civil or criminal trial under the rules of evidence. The courts have recognized in other contexts that “relevance” can be an extremely broad standard. For example, in the grand jury context, the Supreme Court has held that a grand jury subpoena is proper unless “there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury’s investigation.” (6) And in civil discovery, relevance is “construed broadly to encompass any matter that bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be in the case.” (7)

In each of these contexts, the meaning of “relevance” is sufficiently broad to allow for subpoenas or requests that encompass large volumes of records in order to locate within them a smaller subset of material that will be directly pertinent to or actually be used in furtherance of the investigation or proceedings. In other words, the requester is not limited to obtaining only those records that actually are potentially incriminating or pertinent to establishing liability, because to identify such records, it is often necessary to collect a much broader set of the records that might potentially bear fruit by leading to specific material that could bear on the issue.

When it passed the business records provision, Congress made clear that it had in mind such broad concepts of relevance. The telephony metadata collection program meets this relevance standard because, as I explained earlier, the effectiveness of the queries allowed under the strict limitations imposed by the court—the queries based on “reasonable and articulable suspicion”—depends on collecting and maintaining the data from which the narrowly focused queries can be made. As in the grand jury and civil discovery contexts, the concept of “relevance” is broad enough to allow for the collection of information beyond that which ultimately turns out to be important to a terrorism-related investigation. While the scope of the collection at issue here is broader than typically might be acquired through a grand jury subpoena or civil discovery request, the basic principle is similar: the information is relevant because you need to have the broader set of records in order to identify within them the information that is actually important to a terrorism investigation. And the reasonableness of this method of collection is reinforced by the all of the stringent limitations imposed by the Court to ensure that the data is used only for the approved purpose.

I want to repeat that the conclusion that the bulk metadata collection is authorized under Section 215 is not that of the Intelligence Community alone. Applications to obtain this data have been repeatedly approved by numerous judges of the FISA Court, each of whom has determined that the application complies with all legal requirements. And Congress reauthorized Section 215 in 2011, after the Intelligence and Judiciary Committees of both Houses had been briefed on the program, and after information
describing the program had been made available to all Members. In short, all three branches of Government have determined that this collection is lawful and reasonable—in large part because of the substantial protections we provide for the privacy of every person whose telephone number is collected.

The third program I want to talk about is Section 702, part of the FISA Amendments Act of 2008. Again, a little history is in order. Generally speaking, as I said before, Title I of FISA, or traditional FISA, governs electronic surveillance conducted within the United States for foreign intelligence purposes. When FISA was first passed in 1978, Congress did not intend it to regulate the targeting of foreigners outside of the United States for foreign intelligence purposes.

This kind of surveillance was generally carved out of coverage under FISA by the way Congress defined “electronic surveillance.” Most international communications in 1978 took place via satellite, so Congress excluded international radio communications from the definition of electronic surveillance covered by FISA, even when the radio waves were intercepted in the United States, unless the target of the collection was a U.S. person in the United States.

Over time, that technology-based differentiation fell apart. By the early twenty-first century, most international communications travelled over fiber optic cables and thus were no longer “radio communications” outside of FISA’s reach. At the same time there was a dramatic increase in the use of the Internet for communications purposes, including by terrorists. As a result, Congress’s original intention was frustrated; we were increasingly forced to go to the FISA Court to get individual warrants to conduct electronic surveillance of foreigners overseas for foreign intelligence purposes.

After 9/11, this burden began to degrade our ability to collect the communications of foreign terrorists. Section 702 created a new, more streamlined procedure to accomplish this surveillance. So Section 702 was not, as some have called it, a “defanging” of the FISA Court’s traditional authority. Rather, it extended the FISA Court’s oversight to a kind of surveillance that Congress had originally placed outside of that oversight: the surveillance, for foreign intelligence purposes, of foreigners overseas. This American regime imposing judicial supervision of a kind of foreign intelligence collection directed at citizens of other countries is a unique limitation that, so far as I am aware, goes beyond what other countries require of their intelligence services when they collect against persons who are not their own citizens.

The privacy and constitutional interests implicated by this program fall between traditional FISA and metadata collection. On the one hand we are collecting the full content of communications; on the other hand we are not collecting information in bulk and we are only targeting non-U.S. persons for valid foreign intelligence purposes. And the information involved is unquestionably of great importance for national security: collection under Section 702 is one of the most valuable sources of foreign intelligence we have. Again, the statutory scheme, and the means by which we implement it, are designed to allow us to collect this intelligence, while providing appropriate protections
for privacy. Collection under Section 702 does not require individual judicial orders authorizing collection against each target. Instead, the FISA Court approves annual certifications submitted by the Attorney General and the Director of National Intelligence that identify categories of foreign intelligence that may be collected, subject to Court-approved “targeting” procedures and “minimization” procedures.

The targeting procedures are designed to ensure that we target someone only if we have a valid foreign intelligence purpose; that we target only non-U.S. persons reasonably believed to be outside of the United States; that we do not intercept wholly domestic communications; and that we do not target any person outside the United States as a “back door” means of targeting someone inside the United States. The procedures must be reviewed by the Court to ensure that they are consistent with the statute and the Fourth Amendment. In other words, the targeting procedures are a way of minimizing the privacy impact of this collection both as to Americans and as to non-Americans by limiting the collection to its intended purpose.

The concept of minimization procedures should be familiar to you by now: they are the procedures that limit the retention and dissemination of information about U.S. persons. We may incidentally acquire the communications of Americans even though we are not targeting them, for example if they talk to non-U.S. persons outside of the United States who are properly targeted for foreign intelligence collection. Some of these communications may be pertinent; some may not be. But the incidental acquisition of non-pertinent information is not unique to Section 702. It is common whenever you lawfully collect information, whether it’s by a criminal wiretap (where the target’s conversations with his friends or family may be intercepted) or when we seize a terrorist’s computer or address book, either of which is likely to contain non-pertinent information. In passing Section 702, Congress recognized this reality and required us to establish procedures to minimize the impact of this incidental collection on privacy.

How does Section 702 work in practice? As of today, there are certifications for several different categories of foreign intelligence information. Let’s say that the Intelligence Community gets information that a terrorist is using a particular email address. NSA analysts look at available data to assess whether that email address would be a valid target under the statute—whether the email address belongs to someone who is not a U.S. person, whether the person with the email address is outside the United States, and whether targeting that email address is likely to lead to the collection of foreign intelligence relevant to one of the certifications. Only if all three requirements of the statute are met, and validated by supervisors, will the email address be approved for targeting. We don’t randomly target email addresses or collect all foreign individuals’ emails under Section 702; we target specific accounts because we are looking for foreign intelligence information. And even after a target is approved, the court approved procedures require NSA to continue to verify that its targeting decision is valid based on any new information.

Any communications that we collect under Section 702 are placed in secure databases, again with limited access. Trained analysts are allowed to use this data for legitimate
foreign intelligence purposes, but the minimization procedures require that if they review a communication that they determine involves a U.S. person or information about a U.S. person, and they further determine that it has no intelligence value and is not evidence of a crime, it must be destroyed. In any case, conversations that are not relevant are destroyed after a maximum of five years. So under Section 702, we have a regime that involves judicial approval of procedures that are designed to narrow the focus of the surveillance and limit its impact on privacy. I’ve outlined three different collection programs, under different provisions of FISA, which all reflect the framework I described. In each case, we protect privacy by a multi-layered system of controls on what we collect and how we use what we collect, controls that are based on the nature and intrusiveness of the collection, but that take into account the ways in which that collection can be useful to protect national security. But we don’t simply set out a bunch of rules and trust people to follow them. There are substantial safeguards in place that help ensure that the rules are followed.

These safeguards operate at several levels. The first is technological. The same technological revolution that has enabled this kind of intelligence collection and made it so valuable also allows us to place relatively stringent controls on it. For one thing, intelligence agencies can work with providers so that they provide the information we are allowed to acquire under the relevant order, and not additional information. Second, we have secure databases to hold this data, to which only trained personnel have access. Finally, modern information security techniques allow us to create an audit trail tracking who uses these databases and how, so that we have a record that can enable us to identify any possible misuse. And I want to emphasize that there’s no indication so far that anyone has defeated those technological controls and improperly gained access to the databases containing people’s communications. Documents such as the leaked secondary order are kept on other NSA databases that do not contain this kind of information, to which many more NSA personnel have access.

We don’t rely solely on technology. NSA has an internal compliance officer, whose job includes developing processes that all NSA personnel must follow to ensure that NSA is complying with the law. In addition, decisions about what telephone numbers we use as a basis for searching the telephone metadata are reviewed first within NSA, and then by the Department of Justice. Decisions about targeting under Section 702 are reviewed first within NSA, and then by the Department of Justice and by my agency, the Office of the Director of National Intelligence, which has a dedicated Civil Liberties Protection Officer who actively oversees these programs. For Title I collection, the Department of Justice regularly conducts reviews to ensure that information collected is used and disseminated in accordance with the court-approved minimization procedures. Finally, independent Inspectors General also review the operation of these programs. The point is not that these individuals are perfect; it’s that as you have more and more people from more and more organizations overseeing the operation of the programs, it becomes less and less likely that unintentional errors will go unnoticed or that anyone will be able to misuse the information.

But wait, there’s more. In addition to this oversight by the Executive Branch, there is
considerable oversight by both the FISA Court and the Congress. As I’ve said, the FISA Court has to review and approve the procedures by which we collect intelligence under FISA, to ensure that those procedures comply with the statute and the Fourth Amendment. In addition, any compliance matter, large or small, has to be reported to the Court. Improperly collected information generally must be deleted, subject only to some exceptions set out in the Court’s orders, and corrective measures are taken and reported to the Court until it is satisfied.

And I want to correct the erroneous claim that the FISA Court is a rubber stamp. Some people assume that because the FISA Court approves almost every application, it does not give these applications careful scrutiny. In fact the exact opposite is true. The judges and their professional staff review every application carefully, and often ask extensive and probing questions, seek additional information, or request changes, before the application is ultimately approved. Yes, the Court approves the great majority of applications at the end of this process, but before it does so, its questions and comments ensure that the application complies with the law.

Finally, there is the Congress. By law, we are required to keep the Intelligence and Judiciary Committees informed about these programs, including detailed reports about their operation and compliance matters. We regularly engage with them and discuss these authorities, as we did this week, to provide them information to further their oversight responsibilities. For example, when Congress reauthorized Section 215 in 2009 and 2011 and Section 702 in 2012, information was made available to every member of Congress, by briefings and written material, describing these programs in detail.

***

In short, the procedures by which we implement collection under FISA are a sensible means of accounting for the changing nature of privacy in the information age. They allow the Intelligence Community to collect information that is important to protect our Nation and its allies, while protecting privacy by imposing appropriate limits on the use of that information. Much is collected, but access, analysis and dissemination are subject to stringent controls and oversight. This same approach—making the extent and nature of controls over the use of information vary depending on the nature and sensitivity of the collection—is applied throughout our intelligence collection.

And make no mistake, our intelligence collection has helped to protect our Nation from a variety of threats—and not only our Nation, but the rest of the world. We have robust intelligence relationships with many other countries. These relationships go in both directions, but it is important to understand that we cannot use foreign intelligence to get around the limitations in our laws, and we assume that our other countries similarly expect their intelligence services to operate in compliance with their own laws. By working closely with other countries, we have helped ensure our common security. For example, while many of the details remain classified, we have provided the Congress a list of 54 cases in which the bulk metadata and Section 702 authorities have given us information that helped us understand potential terrorist activity and even disrupt it, from
potential bomb attacks to material support for foreign terrorist organizations. Forty-one of these cases involved threats in other countries, including 25 in Europe. We were able to alert officials in these countries to these events, and help them fulfill their mission of protecting their nations, because of these capabilities.

I believe that our approach to achieving both security and privacy is effective and appropriate. It has been reviewed and approved by all three branches of Government as consistent with the law and the Constitution. It is not the only way we could regulate intelligence collection, however. Even before the recent disclosures, the President said that we welcomed a discussion about privacy and national security, and we are working to declassify more information about our activities to inform that discussion. In addition, the Privacy and Civil Liberties Oversight Board—an independent body charged by law with overseeing our counterterrorism activities—has announced that it intends to provide the President and Congress a public report on the Section 215 and 702 programs, including the collection of bulk metadata. The Board met recently with the President, who welcomed their review and committed to providing them access to all materials they will need to fulfill their oversight and advisory functions. We look forward to working with the Board on this important project.

This discussion can, and should, have taken place without the recent disclosures, which have brought into public view the details of sensitive operations that were previously discussed on a classified basis with the Congress and in particular with the committees that were set up precisely to oversee intelligence operations. The level of detail in the current public debate certainly reflects a departure from the historic understanding that the sensitive nature of intelligence operations demanded a more limited discussion. Whether or not the value of the exposure of these details outweighs the cost to national security is now a moot point. As the debate about our surveillance programs goes forward, I hope that my remarks today have helped provide an appreciation of the efforts that have been made—and will continue to be made—to ensure that our intelligence activities comply with our laws and reflect our values.

Thank you.


(2) Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193, 195 (1890)

(3) 82 Stat. 214, formerly codified at 18 U.S.C. § 2511(3)

(4) See, e.g., 50 U.S.C. §§ 1801(h)(1) & 1821(4)(A)

(5) Attorney General’s Guidelines for Domestic FBI Operations (2008), at 23

Thoughts on a Blue-Sky Overhaul of Surveillance Laws: Introduction

By David Kris

Saturday, May 18, 2013 at 11:00 AM

[Editor's Note: This is the first in a series of four posts, in which David S. Kris discusses the possibility of wide-ranging reform to U.S. surveillance law.]

A paper I wrote for Ben Wittes a few years ago discussed the “modernization” of our foreign intelligence surveillance laws after September 11, 2001, culminating in the FISA Amendments Act (FISA) of 2008.[1] The FISA, which was recently renewed by Congress,[2] resolved two difficult issues, at least for the short run. First, the new law addressed the growing indeterminacy of location in the world of communications by regulating some types of electronic surveillance based on a “reasonable belief,” rather than actual knowledge, of the location of the surveillance target, regardless of the location of his interlocutors.[3] For this class of surveillance, involving foreign targets reasonably believed to be located abroad, the FISA expanded the government’s authority, requiring less advance judicial review than prior law.[4] Second, the FISA was politically viable in part because it also contracted the government’s authority in one respect, requiring more advance judicial review than prior law demanded in the surveillance of Americans (rather than foreigners) reasonably believed to be located abroad.[5]

FISA modernization unquestionably solved some problems, but also increased the law’s complexity. By defining certain new classes of surveillance, and establishing new rules to govern them, the FISA established a more intricate legal regime for the nation’s eavesdroppers. The FBI and the National Security Agency, for example, now face at least nine legally distinct categories of foreign intelligence collection (ignoring, for the moment, the FBI’s law enforcement collection authorities), each with separate but sometimes related requirements: (1) electronic surveillance under the 1978 elements of FISA;[6] (2) FISA physical searches;[7] (3) FISA surveillance for certain foreign embassies and other establishments;[8] (4) FISA searches of such establishments;[9] (5) FISA surveillance of non-U.S. persons reasonably believed to be located abroad;[10] (6) FISA surveillance of U.S. persons reasonably believed to be located abroad;[11] (7) collection of certain metadata under FISA’s pen-register provisions;[12] (8) collection of business records and other tangible things under another FISA provision;[13] and (9) other collection not regulated by FISA or the FAA.[14] Complexity at the legal level, moreover, compounds significantly at the operational level, where surveillance targets may fall under different categories as they travel or switch communications methods, and particularly where laws have to be applied in an environment of rapid technological change, like the Internet (although I cannot say much here about operational challenges). There has long been a demand for technology-neutral approaches to regulation of surveillance (a generally sound approach), but sometimes new technology creates new opportunities and challenges that outstrip even the most agnostic regulatory scheme, or the government’s ability to implement it.

1 Available at http://www.lawfareblog.com/2013/05/thoughts-on-a-blue-sky-overhaul-of-surveillance-laws-introduction/.
Combined legal and operational complexity threatens both national security and civil liberties. It threatens security where risk-averse officials abstain from surveillance in the face of uncertainty to avoid possible transgressions and associated liability. Where that occurs, in a specific case or a class of cases, officials may be collecting less intelligence than they should (according to the law as it actually is). The opposite problem exists where complexity masks a legal prohibition and officials proceed without realizing that they should not. In short, where the line is hard to discern, government officials will more likely stop short and overstep, committing what statisticians call Type I and Type II errors. Meaningful public debate about surveillance rules, already difficult in a classified environment, also suffers with increased complexity.

For these reasons, I wrote in 2008, although the FAA represented a reasonable approach, we might some day want—or need—to consider a more radical overhaul of our surveillance laws.[15] As Judge Royce Lamberth, the former Presiding Judge of the FISA Court, explained in 2007, “The years since September 11, 2001, have witnessed a remarkable transformation in the law and practice of national security . . . . The transformation, however, has not been systematic. Rather . . . it has been incremental, and at times even chaotic.”[16] One possible response to this would be a blue-sky review and possible overhaul of our surveillance (and information-collection) laws as a whole, with everything but the Constitution in play. That is the subject of this series of Lawfare posts.


[3] See 50 U.S.C. § 1881a(a). As explained in NSIP, “With the advent of web-based communication and other developments, the government cannot always determine—consistently, reliably, and in real time—the location of parties to an e-mail message.” 1 NSIP § 16:3 at 532.


[14] See Executive Order 12333; USSID-18; 1 NSIP Chapter 16. The nine categories listed here are only the major ones, and many of them would admit of sub-categories.


[16] 1 NSIP Preface at v.
Thoughts on a Blue-Sky Overhaul of Surveillance Laws: Challenges

By David Kris

Sunday, May 19, 2013 at 11:00 AM

[Editor’s Note: this is the second in a series of four posts by David Kris, on large-scale surveillance reform. The first, an introduction, can be found here. Below, David discusses the challenges facing any “blue-sky” overhaul.]

A blue-sky overhaul, while easy to imagine, would be extraordinarily difficult to execute, fraught with risk, and likely to fail in practice. Savvy officials in government know this, which is one of the main reasons that comprehensive reform does not occur. Looking back, for example, it appears that some of the issues addressed by the FAA may have been recognized as early as 1987, at least to some degree, but deferred for 20 years precisely because of the challenges inherent in seeking their resolution.[1] As I have explained elsewhere:

In 1990, DOJ’s Office of Intelligence Policy and Review (OIPR) wrote a memo to the Office of the Deputy Attorney General explaining that it had been “working with the National Security Agency for the past three years to develop possible amendments to the Foreign Intelligence Surveillance Act to meet a need created by technological advances.” In particular, these technological advances appear to have affected “NSA’s collection of international and foreign communications,” creating a “practical imperative” for legislation. The 1990 memo cited draft legislation on which DOJ and the NSA were “close to agreement,” and which would have “provide[d] for Attorney General certification, rather than court order” for the surveillance. However, the 1990 memo also identified several “policy and tactical issues” counseling against seeking new legislation. These policy and tactical issues appear to have overcome the practical imperative in 1990, resulting in no amendments to FISA.[2]

These “policy and tactical” issues, the government’s 1990 memo explained, included the following:
• the fact that “committee jurisdiction in both the House and Senate is concurrent between the Intelligence and Judiciary Committees,” and while the “problems giving rise to the possible amendments have all been discussed with the Intelligence Committees,” they had not been discussed “with the Judiciary Committees”;
• concerns about separation of powers, and the question whether “putting the proposed new collection under the statute, albeit on the basis of Attorney General certification, pose[s] greater separation of powers problems than attempting to exclude the collection from the statute?”
• “the risk of added congressional restrictions if the statute is opened up to amendment”; and
• the fact that “the proposed amendment to FISA to resolve the NSA problem . . . is certain to be written in such enigmatic terms that only those who have been briefed in executive session will understand them,” thus risking “speculation in the media about

---

2 Available at http://www.lawfareblog.com/2013/05/thoughts-on-a-blue-sky-overhaul-of-surveillance-laws-challenges/.
what is really intended and probably deep suspicion that something sinister is going on.” [3]

All of these concerns, and others, could apply even more strongly to a blue-sky overhaul of surveillance laws in general. The official commencement of such an effort, if disclosed, could produce ripple effects of the sort outlined above – e.g., “deep suspicion that something sinister is going on.” Moreover, even if there were a policy decision within the executive branch to develop an overhaul package, and even if it were conducted in a protected, sandbox environment with no ripple effects, the government officials best suited to perform it will be most needed for daily operations. This is something outsiders may not appreciate: even within the vast U.S. Intelligence Community, relatively few officials have the truly deep knowledge and skills to properly perform a blue-sky review of our surveillance laws. Some of that scarcity results from legal complexity, some from technical and operational complexity, and some from the perfect storm where they converge. Most of the officials who have the legal and technical knowledge and skills cannot retreat from day-to-day operational responsibilities – in fact, the work of meeting those responsibilities is part of what qualifies them to conduct an overhaul. Outsiders, who may have more free time than their government counterparts, have less operational and other knowledge, and a blue-sky endeavor uninformed by ground-truth will almost surely fail.

Nonetheless, if complexity pains escalate sufficiently, or if there is a crisis of some sort, an overhaul may become possible or required despite the risks and costs. More importantly, even if it would not yield a viable legislative product, the process and results of an overhaul might, by identifying a preferred end state, serve as a polestar for more realistic incremental change over time. It might also help triage efforts to address anomalies in current law, allowing officials to focus on those most in need of correction. This is probably its chief value.

As a former government official with at least a lingering sense of the legal and operational challenges, I have given some thought to how we might conduct a blue-sky overhaul if we wanted or needed to do so. Without suggesting that it is in fact a good idea, what follows beginning in tomorrow’s post is a sketch of one way we might proceed.[4]

[1] See 1 NSIP § 16:5 at 557.
[4] Such an overhaul would be a good example of what social scientists refer to as a “wicked” problem, in which the resolution of each aspect of the problem requires resolution of all. See Horst Rittel and Melvin Webber, Dilemmas in a General Theory of Planning, Policy Sciences Vol. 4 at 155-169 (1973). For that reason, the sketch that follows may be deceptively linear. It is nearly certain that the process I describe would need to loop and iterate.
Thoughts on a Blue-Sky Overhaul of Surveillance Laws: Approach\(^3\)

By David Kris

Monday, May 20, 2013 at 9:00 AM

[Editor’s Note: below you’ll find the third in a series of posts by David Kris on surveillance reform. In the first two installments, David introduced his subject, and then overviewed the challenges facing an attempt to overhaul the legal rules for surveillance. Below he sketches a possible approach to a "blue-sky" reform effort.]

The first task in any overhaul effort would probably be to define the conduct to be regulated. In part for convenience, I have referred here to an overhaul of “surveillance” laws, but the project would need to consider more than just electronic surveillance. It could include physical searches, and other methods of collecting information. Current law governing intelligence collection offers a starting point for defining the scope of the project, but perhaps we would want to regulate more, or less, than we currently do. The Fourth Amendment provides another starting point, but it may be too narrow because many current statutes (e.g., those governing pen-trap surveillance) regulate conduct that is not a Fourth Amendment search or seizure.[1] Extant foreign intelligence collection activity (as opposed to regulation) might also serve as a guide, but that too is subject to change, and not all current foreign intelligence activity is equally regulated. Moreover, a focus on intelligence leaves the question whether to address law enforcement collection, because differences between the two regimes may themselves create severe anomalies – particularly for the FBI[2] – where the same information can be obtained under each.

A related question concerns the nature of the overhaul. For example, if limited to legislative change, we may want to ignore some collection activity altogether, and leave it to internal executive branch regulation, as Congress did when it enacted FISA in 1978.[3] Today, a good deal of foreign intelligence collection is regulated by the Fourth Amendment and Executive Order 12333 and its subordinate procedures, but not in any meaningful way by statute; bringing all of that activity under statutory control would be a radical step. In short, defining the conduct to be regulated is not as straightforward as it might sound, but will fundamentally affect the basic scope of the project.

The next step, and in some ways the hardest and most important one, would be to divide the universe of relevant conduct into meaningful pieces, which can be regulated in different ways, at different levels of intensity. This process of division probably should begin with our values. For example, where do we most and least value privacy?[4]

Where do we want or need broad governmental power, and the famous “speed and agility” that apparently motivated the Terrorist Surveillance Program?[5] Whatever proposals emerge from the overhaul, they would likely need to distinguish in some way between different forms of collection – e.g., between non-consensual surveillance of the words spoken in a telephone call between two American citizens in the United States, and the consensual monitoring of the telephone numbers dialed (but not the words spoken) in a call between two citizens of Afghanistan located in that country, or the mere physical

\(^{3}\) Available at http://www.lawfareblog.com/2013/05/thoughts-on-a-blue-sky-overhaul-of-surveillance-laws-approach/.
surveillance of the Afghans when they visit a public market in Kabul. What are the values that inform this distinction?

Rather than beginning with a clean slate, and an attempt to discern our values from scratch, it may help to note the distinctions that have in fact been used in prior and current statutes and rules, which reflect values we have adopted, or at least enacted into law, from time to time. A blue-sky project would critically review these distinctions and consider whether to adopt, reject, modify, or supplement them. Here is a list of some (not all) of those distinctions:

A. Distinctions Concerning the Target of Surveillance and/or His Interlocutors

1. **Location.** An overhauled legal regime might distinguish between targets who are known or reasonably believed to be in the United States, those who are known or reasonably believed to be abroad, and those whose location is uncertain. As explained above, the FAA was designed in part to address the growing uncertainty of location in electronic communications, particularly web-based communications. Distinctions are possible based on the location of the target alone, or the target and his interlocutors. Alternatively, a new regime might abandon location as a distinguishing feature, on the theory that it is becoming ever more indeterminate.

2. **Nationality and Citizenship.** We would need to consider whether to distinguish between targets who are known or reasonably believed to be U.S. persons, those who are known or reasonably believed not to be U.S. persons, and those whose status is uncertain. In today’s world, nationality is often difficult to discern; even in 1978, FISA required assumptions about nationality that were largely based on location. As location becomes more indeterminate, nationality may as well. Again, distinctions are possible based on the nationality or citizenship of the target alone, or of the target and her interlocutors.

3. **Other Nationality-Related Issues.** Under FISA, there are distinctions between entities that are controlled by a foreign government, and those openly acknowledged to be controlled by a foreign government. The theory is that errors are less likely with respect to the latter (justifying some expanded collection authority), but there is some question whether there is much of a practical difference and whether, if there is, it justifies the added complexity in the overall regime resulting from the distinction.

4. **International versus Domestic Terrorism.** In keeping with a distinction recognized by the Supreme Court, FISA applies only to international terrorism, not domestic terrorism, but surveillance of domestic terrorism need not proceed solely under ordinary law enforcement standards. The Supreme Court invited Congress to enact a special domestic security surveillance statute with standards different than those governing surveillance of ordinary crime, and Congress could always accept the invitation. Again, however, creating a new class of surveillance for domestic security threats, which would be regulated somewhere on the continuum between FISA (which applies to foreign security threats) and the federal wiretap statute known as Title III (which applies to ordinary crime) would generate still more complexity in the law.

5. **Reasonable Expectation of Privacy.** The regulatory role of a reasonable expectation of privacy could also be considered as part of a blue-sky overhaul. This concept, rooted in the Fourth Amendment, is obviously central, but FISA has used it more broadly than the Constitution may require – e.g., in drawing distinctions based on
whether "a person" (meaning a U.S. person) has a reasonable expectation of privacy, even when the particular person being targeted (e.g., certain non-U.S. persons) may not have such an expectation.\cite{14}

6. Consent. A blue-sky overhaul could consider whether and how to distinguish surveillance based on the consent of one or all parties to a communication or other form of collected information.\cite{15}

B. Distinctions Based on How the Government Conducts the Surveillance

7. Investigative Agency Limits. An important question in an overhaul would be whether to limit collection techniques to certain types of investigations conducted by certain types of agencies in certain circumstances.\cite{16} For example, there may be reasons that the FBI should enjoy more investigative authority than the CIA in certain domestic settings, and perhaps reasons for the opposite outcome abroad. But one possible price of this agency-specific tailoring is more complexity and perhaps uncertainty.

8. Targeting. There is a question whether to distinguish in our law between surveillance targeting a specific person and surveillance that does not target any specific person.\cite{17} This was an enormously important distinction when FISA was enacted in 1978, with the statute designed to focus on any targeting of a particular, known U.S. person inside the United States.\cite{18} Collection targeting a specific person may be more intrusive than generic surveillance that happens to collect communications of many persons, but advances in technology since 1978 may put the distinction in a slightly different light (there are limits on what I can say publicly in this area).\cite{19}

9. Location of Collection. An overhaul could consider whether to distinguish classes of surveillance based on the location in which the surveillance (or other collection) occurs. Again, in the past we have distinguished between collection in the United States and abroad,\cite{20} but location seems to be harder and harder to determine in real time. The uncertainty here is obviously less severe than with respect to the location of targets, since the government's own collection conduct is at issue, but there may be complexities that arise with advancing technology.

10. Surveillance Solely Directed at Foreign Powers. Today, FISA distinguishes according to whether the surveillance or other collection is directed solely at foreign powers and/or has a reasonable likelihood of collecting U.S. person communications.\cite{21} We could maintain, change, or eliminate this distinction as part of a blue-sky overhaul.

11. Use of a Collection Device. We could also maintain, change, or eliminate legal distinctions, that are embodied in current law, based on whether the government uses an electronic or mechanical device in the surveillance or other collection.\cite{22}

12. Type of Communication. In FISA, information acquired through electronic surveillance is either a wire communication, a radio communication, or neither; in Title III, the categories are wire, oral, and electronic communications.\cite{23} Perhaps the distinctions within each regime no longer make sense, and perhaps the distinctions between the regimes no longer make sense.

13. Real-Time Collection. An overhaul would need to consider whether to distinguish between real-time collection and after-the-fact collection even where the information to be collected is essentially the same.\cite{24} This is a distinction with historical
roots, but advances in the speed and nature of electronic record-keeping may call into doubt its continuing relevance.

14. **Content or Metadata.** An important question would be whether to continue to distinguish between collection of the content of communications (e.g., the words spoken in a telephone call), metadata (e.g., the numbers dialed in a telephone call), and/or perhaps borderline material that is not as easily classified as one or the other.[25]

15. **Role of Third Parties.** We would need to consider whether to continue to permit, or require, surveillance or other collection to proceed with voluntary or compelled third-party assistance, whether third parties may challenge an order or directive to assist in collection, and whether they should be immunized for providing assistance under certain circumstances.[26] Also, we would need to consider the significance of conveying information to third parties — e.g., e-mail to an Internet Service Provider — as Congress did when it enacted the Electronic Communications Privacy Act.[27]

16. **Purpose.** An overhaul would consider whether to distinguish based on the government’s programmatic purpose or individual purpose in conducting the collection, whether to distinguish based on the government’s ultimate purpose (e.g., to protect against foreign threats to national security) or the methods used to achieve that ultimate purpose (e.g., criminal prosecution as opposed to other methods), and whether to make the inquiry turn on primary purpose, significant purpose, or some other quantum of purpose.[28]

17. **Private Property and U.S. Residences.** There are many relatively precise distinctions in current law that could be reconsidered, including, for example, whether to impose special requirements where a search or surveillance requires or involves a physical entry on private property[29] or into a home.[30]

C. **Levels and Types of Approvals for Surveillance**

18. **Advance Approval.** A fundamental question in a blue-sky overhaul is whether and when to require approval for surveillance or other collection before the fact, after the fact, or not at all.[31] This set of distinctions tends to reflect a balance between speed and agility on the one hand, and protection for civil liberties on the other hand, and was obviously central in the process leading to enactment of the FAA.

19. **Approval by Whom.** A related question to be considered is whether the approval should be from the judicial branch, the executive branch, and/or another source;[32] and within the executive branch, the level of approval required,[33] including whether the President must individually authorize collection or delegate authority to do so.[34]

20. **Scope of Approval.** The scope of any required approval is also very important — i.e., whether surveillance approvals should be limited to individual persons or facilities (e.g., John Doe or a particular 10-digit telephone number), or can be broader (e.g., any member of al Qaeda or a gateway switch),[35] including (where approvals are more limited) whether to allow roving surveillance based on certain showings and whether to impose special reporting obligations in roving or other cases.[36]

21. **Emergency and Other Exceptions.** A blue-sky overhaul would consider whether to permit short-term collection without a required advance approval for short periods in certain circumstances subject to after-the-fact ratification.[37]
22. **Duration of Approval Period.** Current law allows certain approvals for a short period (e.g., 30 days), as well as longer periods (e.g., 60 days or 1 year), and allows different periods for different types of targets and/or collection techniques, and initial authorization orders as opposed to renewals of orders.[38] This complex regime could be reconsidered.

23. **Stages of Conduct Subject to Regulation and Approval.** A key question, as we move further into an era of larger haystacks of collectible data, is whether approvals should regulate (or focus most on regulating) acquisition, retention, and/or dissemination of information.[39] This is another important area where new approaches to managing large data sets could be valuable, and minimization doctrines could be updated.

**D. Use of Information Obtained or Derived from Surveillance**

24. **Procedures for Establishing Improper Collection.** A blue-sky overhaul would consider whether and how to conduct proceedings to determine whether information was improperly collected.[40]

25. **Defensive Remedies for Improperly Collected Information.** A related question would be whether to allow suppression of evidence or other defensive remedies where information was improperly collected.[41]

26. **Offensive Remedies for Improperly Collected Information.** Another related question is whether to impose civil or criminal liability for improper collection of information, or knowing use of improperly collected information, and in particular to identify the right *sciente* requirement with respect to such use where the government may not know if information, or an analytic product derived from multiple streams of information, is or may be tainted, in whole or in part, by underlying improper collection.[42] This is a very important question as the scale of surveillance and related activities increases.

27. **Coordination.** An overhaul would consider whether to limit or require federal-state coordination and sharing of information obtained or derived from surveillance.[43]

**E. Public and Congressional Reporting and Oversight**

28. **Reporting.** An overhaul would consider whether and how to require reporting on surveillance and collection[44] to the public,[45] to the Intelligence Committees and to the Judiciary Committees, as well as the rest of Congress.[46] Today, the reporting regime is very complex.

* * *

This list in this post is by no means complete, but it should convey the basic point I am trying to establish: there are many ways to slice the pie. A true blue-sky overhaul affords us tremendous freedom to consider, and reconsider, the distinctions we have used to classify surveillance into differently-regulated categories. Of course, our choices in this area are not entirely free, because some of the foregoing distinctions find roots in the Fourth Amendment. Absent a constitutional amendment (a bluer-sky approach than this series of posts imagines),[47] they will have to remain. Unfortunately, determining what the Fourth Amendment allows in this area is itself a staggering challenge, and one that must be refreshed quite often as the operational environment – particularly technology –
evolves. In other words, even without any statutory limits at all, finding the constitutional floor will be extremely daunting.

[2] The FBI’s Domestic Operations Guidelines, approved by the Attorney General in 2008, provide that “all of the FBI’s legal authorities are available for deployment in all cases” in order to “protect the public from crimes and threats to the national security, and to further the United States’ foreign intelligence objectives.” As a result, the FBI’s “information gathering activities” need not be “differentially labeled” as law enforcement, counterintelligence, or affirmative foreign intelligence, and its personnel need not be “segregated from each other based on the subject areas in which they operate.” The Attorney General’s Guidelines for Domestic FBI Operations at 7 (available at http://www.justice.gov/ag/readingroom/guidelines.pdf). The Guidelines are discussed in more detail in 1 NSIP §§ 2:15-2:18.
[4] Some of our values are enshrined, at some general level, in the Fourth Amendment (and case law), but even the Fourth Amendment depends in large part on what expectations of privacy society deems to be reasonable, see Katz v. United States, 389 U.S. 347 (1967). The blue-sky effort described here would not go so far as to consider repeal of the Fourth Amendment, although of course the Constitution provides for that possibility. As explained above, even starting from a statutory ground zero is likely too extreme ever to be implemented, and this series of posts is by no means a call for an actual overhaul; it is merely a thought-experiment as to how such an overhaul, even if never to be implemented, could be conceived, primarily to help guide more realistic, incremental change over time.
[5] See 1 NSIP § 16:2 at 529.
[8] See, e.g., 1 NSIP §§ 8:36-8:44.
[9] See, e.g., 50 U.S.C. § 1801(b)(1)-(2). Obviously, U.S. intelligence agencies cannot always know the citizenship or immigration status of parties to, or subjects of, an acquired communication. As explained in 1 NSIP § 9:3 (internal quotation omitted), “FISA’s legislative history mildly suggests, but certainly does not require, that persons in the United States might be presumed to be U.S. persons unless there is some reason to believe otherwise . . . .”
[18] See 1 NSIP Chapter 16, especially § 16:5.
On the Bulk Collection of Tangible Things

David S. Kris

Beginning in June 2013, in response to a series of unauthorized disclosures of classified information, the government confirmed and revealed information about its use of FISA’s tangible-things provision, 50 U.S.C. § 1861, to acquire telephony metadata in bulk. This paper discusses that. Disclosure of the bulk metadata collection also contributed to a broader policy debate concerning the transparency and scope of intelligence activities, particularly signals intelligence, and the role of the FISA Court, among other issues. This paper also discusses those issues.2

Unauthorized Disclosures and Historical Context

On June 6, 2013, the Guardian newspaper posted on its website a four-page order signed by Judge Roger Vinson of the FISC, the authenticity of which the government later acknowledged.4 The order, directed at a subsidiary of a


5. 215 Bulk Secondary Order, supra note 3, at 2

6. Id.; see BLX RECORDS FISA TEAM, BUSINESS RECORDS FISA NSA REVIEW 15 (2009) (hereinafter NSA End-to-End Review), available at http://www.dni.gov/files/documents/section/pub/NSA%20Business%20Records%20FISA%20Review%202010%200909.pdf; August 2013 FISC Order, supra note 4, at 10, 11; of U.S. § 2510(8) (2012)(C006) (“Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978.”).


8. 215 Bulk Secondary Order, supra note 3, at 2; see August 2013 FISC Opinion, supra note 4, at 2 n.9. "Contents" is defined to include "any information concerning the substance, purport, or meaning of that communication." For a discussion of this definition and its relevance to FISA, see NSIP, supra note 1, at § 7.11, 18.2, 18.4.

9. 215 Bulk Secondary Order, supra note 3, at 2. For a discussion of non-disclosure requirements under the tangible-things provision, see NSIP, supra note 1, at § 19.5.
had not been confirmed by the government. In 2006, for example, USA Today published an article with the headline, “NSA Has Massive Database of Americans’ Phone Calls.” The 2006 article explained that shortly after September 11, 2001, NSA approached certain telephone companies and “told the companies that it wanted them to turn over their ‘call-detail records,’ a complete listing of the calling histories of their millions of customers. In addition, the NSA wanted the carriers to provide updates, which would enable the agency to keep tabs on the nation’s calling habits.” The article described how certain companies cooperated with NSA, but noted that one company, Qwest, refused: “Unable to get comfortable with what NSA was proposing, Qwest’s lawyers asked NSA to take its proposal to the FISA court. According to the sources, the agency refused.” A 2006 article in the New Yorker magazine alleged more details on the collection, as did a 2008 article in Newweek.

A second document published by the Guardian purported to be a March 2009 “working draft” of the NSA Inspector General’s report on the President’s Surveillance Program (PSP). According to the purported draft report, and as in fact, available the Internet, but without any suggestion that it is or is not what it purports to be, or that any statements within it are accurate. The point of referring to them here is to describe the context in which the ongoing public debate is occurring, not to verify the accuracy of any alleged facts that have not been officially acknowledged, because the public understanding is significant in and of itself, whether or not it is factually accurate in all respects.

10. See, e.g., Heping v. AT & T. 439 F. Supp. 974, 978 (N.D. Cal. 2006) (“Plaintiffs allege that AT & T Corporation (AT & T) and its holding company, AT & T Inc., are collaborating with the National Security Agency (NSA) in a massive warrantless surveillance program that illegally tracks the domestic and foreign communications and communication records of millions of Americans.”). 11. Leslie Cauley, NSA Has Massive Database of Americans’ Phone Calls, USA Today, May 11, 2006. 12. Descriptions of this and other news articles or documents not officially acknowledged by the government should not be understood as an endorsement or verification of any statement made in those articles; the point here is only that the general subject of bulk telephony metadata collection was under discussion accurately or inaccurately, prior to the June 2013 disclosures.

13. Id. 14. Id. For an interesting discussion of the legality of the collection in 2007, see PBS Newshour, From The Archives: NSA Surveillance Seven Years Earlier, PBS (June 6, 2013), http://www.pbs.org/newshour/randow/two07/06/from-the-archives-nsa-surveillance-seven-years-earlier.html. 15. Seymour Hersh, Listening In, The New Yorker (May 29, 2006), http://www.newyorker.com/ archive/2006/06/30/06062613a1_16. Daniel Klaidman, Now We Know What the Battle Was About, Newsweek (Dec. 12, 2006), http://www.thedailybeast.com/newsweek/2006/12/13/now-we-know-what-the-battle-was-about.html. The article referred to “vast and indiscriminate collection of communications data,” and “a system in which the National Security Agency, with cooperation from some of the country’s largest telecommunications companies, was able to vacuum up the records of calls and e-mails of tens of millions of average Americans between September 2001 and March 2004.” As part of that program, the article continued, “NSA’s powerful computers became vast storerooms of ‘metadata.’ They collected the telephone numbers of callers and recipients in the United States, and the time and duration of the calls.” 16. Nat’l Sec. Adm’r’s Office of the Inspector Genc., Working Draft ST-09-0002 (2009) [hereinafter NSA IG Working Draft Report], available at http://www.guardian.co.uk/world/interactive/2013/jun/27/nsa-inspector-general-report-data-document-collection; see Charlie Savage, New Leak Suggests Ash- ccraft Confrontation Was Over N.S.A. Program, N.Y. Times, June 27, 2013, at A6. An unclassified summary of a report by several Inspectors General on the PSP had been released in 2009, but it referred only to the Terrorist Surveillance Program (TSP), which collected the content of communications and is discussed in Chapters 13 and 16 of NSIP, supra note 1, and “Other Intelligence Activities,” without specifying those or other activities involved. See OFFICE OF INSPECTORS GEN., UNCLASSIFIED REPORT ON THE PRESIDENT’S SURVEILLANCE PROGRAM 6 (2009), available at http://www.justice.gov/scg/special/ ogp._other_intelligence_activities.pdf. The report’s omission of NSA’s bulk telephony metadata collection and its failure to discuss it for certain other unlawfully disclosed documents, and thus it is referred to here only as a document that is, 17. See Unclassified Declaration of Frances J. Fleisch, National Security Agency, at 18-19, Jewel v. NSA, No. C-04-4373-JW (D. Cal. Dec. 20, 2013) (hereafter December 2013 FLEisch Declaration) (“Starting on October 4, 2001, President Bush authorized the collection,” available at http://www.dni.gov/files/documents/120NSA%20%20Fleisch%20201310%20Jewel%20Declaration%20 Unclassified.pdf). 18. NSA IG Working Draft Report, supra note 16, at 1. According to the purported report, the Presiding Judge of the FISA Court was first informed of the collection on January 31, 2002, and the remaining Members of the Court were briefed in January 2006. Id. at 24, 37. At least one company referred to in the purported draft report as COMPANY F “did not participate in the PSP because of corporate liability concerns.” Id. at 30, but others did. 19. See, e.g., Dan Eggen & Paul Karr, Gonzales Hospital Episode Detailed, Wash. Post, May 16, 2007, at A1 (reporting on “vivid” Congressional testimony by James Comey); Memorandum for the Attorney General (May 6, 2004) [hereinafter May 2004 OLC PSP Opinion], available at http://www.justice.gov/docmemo/president-surveillance-program.pdf. 20. NSA IG Working Draft Report, supra note 16, at 33. The purported NSA Inspector General’s draft report explains that the Department of Justice’s Office of Legal Counsel (OLC) “found three of the four types of collection authorized under the PSP to be legally supportable. However, it determined that, given the method of collection, bulk Internet metadata [collection] was prohibited by the terms of FISA and Title III,” the criminal wiretapping statute. Id. at 37. The government has since acknowledged and released FISA Court orders authorizing bulk collection of Internet metadata. See, e.g., FISCA Redacted Orders and Orders, available at http://www.dni.gov/files/documents/118CLEANEDPRRT%20pdf.pdf. 21. NSA IG Working Draft Report, supra note 16, at 37. See also id. at 39 ("According to NSA personnel, the decision to transition Internet metadata collection in a FISC order was driven by DoJ."); According to the purported draft report, until this confronation with DOJ, NSA took the position that it could "obtain bulk Internet metadata because the NSA did not actually ‘acquire’ communications until specific communications were selected," e.g., by querying the database containing all the communications. Id. at 38. For a discussion of a similar theory in a different context, see NSIP, supra note 1, at 7-9. 22. See December 2013 Fleisch Declaration, supra note 17, at 19. 23. NSA IG Working Draft, supra note 16, at 39. Those limits are said to include having "specified- 24. Later confirmed by an official disclosure in December 2013, both content and Internet and telephony metadata were collected outside the ambit of FISA beginning in October 2001, shortly after the September 11 attacks. In March 2004, a disagreement between the White House and the Department of Justice, which has been recounted in vivid detail elsewhere, apparently caused the President to "discontinue bulk collection of Internet metadata" under the PSP and seek authorization from the FISA Court, but allowed the remaining elements of the program, including collection of content and telephony metadata, to continue without FISA Court authorization. The court issued its first order authorizing bulk collection of Internet metadata under FISA’s pen-trap provisions in July 2004, which "essentially gave NSA the same authority to collect bulk Internet metadata that it had under the PSP," with a few additional limits. However, collection of bulk telephony metadata is described as having
September 2013, the FISA Court released an opinion and order (issued in August 2013) that re-authorized the bulk collection of telephone metadata and

explained the court's reasoning,28 and subsequent court authorizations were also released to the public.29 Together, these official disclosures revealed the following:

1. The FISA Court order disclosed in June 2013 is designated a "Secondary Order" and is directed at a telecommunications provider;30 the court also issued a "Primary Order" to the government,31 setting out various requirements and limits on the collection and use of the telephony metadata.32 The primary and secondary orders are issued by the FISC every 90 days,33 and have been renewed consistently since May 2006— including after the unauthorized disclosures.34 Altogether, as of July 2013, "the court [had] authorized the program on 34 separate occasions by 14 different judges."35 Although only one secondary order, directed at one company, was disclosed, the government has confirmed that the "FISA Court has repeatedly approved orders directing several telecommunications companies to produce the telephony metadata,"36 and in public remarks in July 2013, the General Counsel of the NSA referred to "three...

37. Raj De, Remarks at the Aspen Institute, Counterterrorism, National Security and the Rule of Law (July 18, 2013), available at http://aspensecurityforum.org/2013-video (remar k is at approximately 18:06 in video). As of December 2013, the government continues to resist formally identifying providers who assisted with bulk metadata collection. See December 2013 Fleisch Declaration, supra note 17, at 27-28 (although the participation of a Verizon subsidiary for one 90-day period has been acknowledged, "the continued protection of whether or not, or to what extent, a particular telecommunications provider assisted the NSA under FIS C order or otherwise [as to bulk collection of telephony metadata] remains an extraordinarily sensitive and significant matter that the Government continues to protect to avoid even greater harm to national security than has already occurred since June 2013 ... I am also supporting the DNI's state secrets privilege assertion, and asserting NSA's statutory privilege, over information relating to which carriers have assisted the NSA under presidential authorization and other authorities.").

38. August 2013 FISC Opinion, supra note 4, at 2 n.2. For a discussion of the term "contents" as used in FISA and Title III, see federal wiretap statute, see NSIP, supra note 1, at 157-111, 18.2. The bulk collection order is explicit in using the definition from Title III. 18 U.S.C. § 2510(8). 215 Bulk Secondary Order, supra note 3, at 2.

39. June 2013 FISC Open Hearing, supra note 27 (statement of Chris Ingalls) (Question: "So there are no names and no addresses affiliated with these phone numbers?"") Answer: "No, there are not, sir."); August 2013 FISC Opinion, supra note 4, at 2 n.2.

40. August 2013 FISC Opinion, supra note 4, at 2, n.2, 4 n.5; June 6, 2013 DNI Statement on Recent Unauthorized Disclosures, supra note 4, at 1; June 2013 NSA Section 215 Backgrounder, supra note 27, at 1 ("This program concerns the collection only of telephone metadata. Under this program, the government does not acquire the content of any communication, the identity of the party to the communication, or any cell-site location information."); June 2013 HPSCI Open Hearing, supra note 27 (statement of Keith Alexander) (Question: "Does the American government have a database that has the GPS location/whereabouts of Americans, whether it's by our cellphones or by other tracking device? Is there—is there a known database?" Answer: "NSA does not hold such a database."). Question: "can you figure out the location of the person who made a particular phone call?" Answer: "No beyond the area code."); Question: "Do you have any information about signal strength or tower direction? Answer: "We don't have that in the database.""); In its August 2013 opinion, the FISA Court stated: "In the event that the government seeks the production of CSLI (cell site location information) as part of the bulk production of call detail records in the future, the government would be required to provide notice and briefing to this Court pursuant to FISCA Rule 11."); August 2013 FISC Opinion, supra note 4, at 4 n.5.

41. June 2013 HPSCI Open Hearing, supra note 27 (statement of Chris Ingalls); see id. (statement of James Cole) ("It is the number that was dialed from, the number that was dialed to, the date and length of time. That's all we get under 215. We do not get the identity of any of the parties to this phone call. We don't get any cell site or location information as to where any of these phones were located and... we don't get any content under this.")).

42. June 2013 HPSCI Open Hearing, supra note 27, at 2; June 2013 NSA Section 215 Backgrounder, supra note 27, at 1 ("This metadata is stored in repositories within secure networks, must be uniquely marked, and can only be accessed by a limited number of authorized personnel who have received appropriate and adequate training."); June 2013 HPSCI Open Hearing, supra note 27 (statement of Keith Alexander) ("So each set of data that we have—and in this case, let's say the business records FISA—you have to have specific certificates. . . . He would have to get one of those certificates to..."
4. The stored metadata "may be queried only when there is a reasonable suspicion, based on specific and articulated facts, that an identifier [e.g., a telephone number that is used as the query] is associated with specific foreign terrorist organizations." The queries may not relate to any other foreign intelligence purpose, such as counter-espionage. The government submits and the FISA Court approves a specific list of terrorist groups or targets to which a query must relate.

5. A finding of reasonable, articulable suspicion (RAS) supporting a query must be made initially by one of 22 persons at NSA (20 line personnel and two supervisors); certain selectors as to which the FISC has already found probable cause pursuant to a traditional FISA order (not a FISA Amendments Act directive) for full content surveillance may be deemed to be RAS-approved. The RAS determinations generally must be made in writing, in advance of the query being submitted, and are subject to after-the-fact auditing and review by actually enter that area [of NSA's network or databases]. Does that make sense? In other words, it's a key.

July 16, 2013 Letter to Sentenbrenner, supra note 27, at 2 ("only specially cleared counterterrorism personnel specifically trained in the court-approved procedures can access the records to conduct queries"); August 2013 FISC Order, supra note 4, at 4-5 & nn.2-3.

43. June 2013 IC Backgrounder, supra note 27, at 1; see June 2013 HPSCI Open Hearing, supra note 27 (statement of Chris Inglis); July 2013 HUC Hearing, supra note 27 (statement of James Cole); July 16, 2013 Letter to Sentenbrenner, supra note 27, at 2; August 2013 FISC Order, supra note 4, at 6-11.

44. June 2013 HPSCI Open Hearing, supra note 27 (statement of Chris Inglis) ("It cannot be used to do anything other than terrorism"); July 16, 2013 Letter to Sentenbrenner, supra note 27, at 7; July 2013 Litt Speech, supra note 27, at 13 ("we only look at a tiny fraction of it, and only for a carefully circumscribed purpose -- to help us find links between foreign terrorists and people in the United States"); cf. 215 Bulk Primary Order, supra note 27, at 7-9.

45. June 2013 NSA Section 215 Backgrounder, supra note 27, at 1 ("this metadata may be queried only when there is a reasonable suspicion that the identifier is associated with specific foreign terrorist organizations"); June 2013 HPSCI Open Hearing, supra note 27 (statement of James Cole) ("there needs to be a finding that there is reasonable suspicion that the person whose phone records you want to query is involved with some sort of terrorist organization. And they are defined -- it's not everyone, they are limited in the order"); July 16, 2013 Letter to Sentenbrenner, supra note 27, at 2 ("[T]he FISC allows the data to be queried for intelligence purposes only when there is reasonable suspicion, based on specific facts, that a particular query term, such as a telephone number, is associated with a specific foreign terrorist organization that was previously identified and approved by the court."); Id. (RAS standard requires linking to "a specific foreign terrorist organization that was previously identified and approved by the court"); July 2013 Litt Speech, supra note 27, at 14 ("the Government's applications to collect the telephony metadata have identified the particular terrorist entities that are the subject of the investigations.")

46. June 2013 NSA Section 215 Backgrounder, supra note 27, at 1; June 2013 HPSCI Open Hearing, supra note 27 (statement of Chris Inglis) ("it must be approved by one of those 20 plus two individuals, 20 analysts, specially trained analysts, or their two managers, such that it might then be applied as a query against the data set... Any analyst that wants to form a query, regardless of whether it's this authority or any other, essentially has a two-person control rule. They would determine whether this query should be filed, and there is someone who provides oversight on that"); 215 Bulk Primary Order, supra note 27, at 2 ("[NSA has reported that fewer than 300 unique identifiers were used to query the data after meeting this standard"). It appears that the actual number of identifiers used may have been 288, although the matter is not entirely clear. See July 2013 SFC Hearing, supra note 27 (statement of Senator Feinstein) ("[M.] Inglis's statement makes public for the first time a fact, and it's an important fact... But and quote, in 2012 on those fewer than 300 selectors, that's queries, which actually were 288 for Americans... ").

51. June 2013 IC Backgrounder, supra note 27, at 1; July 16, 2013 Letter to Sentenbrenner, supra note 27, at 2 ("NSA has reported that fewer than 300 unique identifiers were used to query the data after meeting this standard"). It appears that the actual number of identifiers used may have been 288, although the matter is not entirely clear. See July 2013 SFC Hearing, supra note 27 (statement of Senator Feinstein) ("[M.] Inglis's statement makes public for the first time a fact, and it's an important fact... But and quote, in 2012 on those fewer than 300 selectors, that's queries, which actually were 288 for Americans... ").

52. June 2013 HPSCI Open Hearing, supra note 27 (statement of Chris Inglis) ("So only less than 300 numbers were actually approved for query against that database. Those might have been queried for other elements of the Executive Branch.") A RAS determination endures for 180 days for selectors associated with U.S. persons, and for one year for selectors associated with non-U.S. persons. The FISA Court itself does not routinely approve or review individual queries, and it does not receive regular reports on individual queries, although its sets the criteria for queries and receives regular reports (every 30 days) on the number of identifiers used to query the collected metadata as well as the number of instances in which query results that contain U.S. person information are disseminated by NSA. The Congressional Intelligence Committees also receive regular reporting.

6. In 2012, "less than 300 unique identifiers met this [RAS] standard and were queried," although it is clear that at least some of the RAS-approved identifiers were used in multiple queries. Initial queries may also produce two
additional "hops"—i.e., numbers that are connected to numbers that are responsive to queries. As the government explained, "(under the FISC's order, the NSA may also obtain information concerning second and third-tier contacts of the identifier (also referred to as 'hops'). The first 'hop' refers to the set of numbers directly in contact with the seed identifier. The second 'hop' refers to the set of numbers found to be in direct contact with the first 'hop' numbers, and the third 'hop' refers to the set of numbers found to be in direct contact with the second 'hop' numbers." Some of the querying is automated and some is manual. Extending three hops from 300 seed identifiers clearly could in theory embrace a large quantity of telephone numbers, but altogether, in 2012, the NSA reviewed approximately 6,000 telephone numbers as a result of all queries conducted through all hops, and "provided a total of 12 reports to FBI, which altogether 'tipped' less than 500 numbers" generated by the initial queries and hops.

53. July 2013 HUC Hearing, supra note 23 (statement of Chris Ingals) ("the court has given permission to do, not just first-hop analysis, meaning what numbers are in contact with that selector [that is used for the initial query] but then to those numbers, go out two or three hops.") See July 2013 SIC Hearing, supra note 27 (statement of Chris Ingals) ("...they try to be judicious about choosing when to do a second hop or, under the court's authorization, a third. Those aren't always exercised."). See NSA IG Working Draft, supra note 16, at 13 n.6 ("Additional charging can be performed on the associates' contacts to determine patterns in the way a network of targets may communicate. Additional degrees of separation from the initial target [query] are referred to as 'hops.'"). For example, a direct contact is one hop away from the target.

54. White Paper, supra note 27, at 4. In his January 17, 2014 speech, the President directed that effective immediately, only two hops, not three, would be permitted. POTUS Signt Speech, supra note 49.

55. 215 Bulk Primary Order, supra note 27, at 11. The President's Civil Liberties Oversight Board (PCLOB) reported that the "ultimate result of the automated query process is a repository, the corporate store, containing the records of all telephone calls that are within those 'hops' of every currently approved selection term. Authorized analysts looking to conduct intelligence analysis may then use the records in the corporate store, instead of searching the full repository of records. According to the FISA, corporate store, records that have been moved into the corporate store may be searched by authorized personnel for "specific foreign intelligence purposes." Without the requirement that these searches use only RAS-approved selection terms. Analysts therefore can query the records in the corporate store with terms that are not reasonably suspected of association with terrorism. They also are permitted to analyze records in the corporate store through means other than individual contact- querying queries, the agency is allowed to apply other analysis methods and techniques to the query results.


57. July 2013 SIC Hearing, supra note 27 (statement of Chris Ingals). In prior years, the number of tips apparently has been somewhat higher. See, e.g., In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted]. No. 07-04 at 6-8 (FISA Ct. May 4, 2007) ("The Court understands that NSA expects that it will continue to provide on average approximately three telephone numbers per day to the FBI, available at http://www.dns.gov/files/documents/11714fISFC%20Order%20BBA%2007-04.pdf.")

58. June 2013 HPSIC Open Hearing, supra note 27 (statement of Keith Alexander); see August 2013 FISC Order, supra note 4, at 5 n.7 ("A selection term that meets specific legal standards has always been required. The Court has not authorized government personnel to access the data for the purpose of wholesale 'data mining' or browsing."). Prior to initiation of the FISC-approved bulk collection of telephony metadata in 2006, NSA had developed an "alert list" process to assist in prioritizing its review of the telephony metadata it received. The alert list contained telephonic identifiers that NSA was targeting for collection, including some that had not met the RAS standard, and NSA used an automated system to compare incoming telephony metadata against the alert list identifiers, which was a violation of the FISC's orders. See Memorandum of the United States in Response to the Court's Order Dated January 28, 2009, No. BR-09-13 (FISA Ct. Feb. 17, 2009), available at www.dni.gov/files/documents/selections.pdf; PAR-2012-02009-Memorandum%20PDF.pdf.

59. Contact-chaining involves the use of "computer algorithms... [to create] a chain of contacts linking communications and identifying additional telephone numbers, IP addresses, and e-mail addresses of intelligence interest." Memorandum for the Attorney General, from Kenneth L. Wainstein, Assistant Attorney General, at 2 (November 20, 2007), available at http://www.guantan.com/uk/world/ interactive/2013/01/27/fisa-data-collection-justice-department.htm[hereinafter Wainstein Contact Chaining Memo]. As with the NSA Draft IG Report, the government has not acknowledged or declassified this memorandum, as it has for certain other unlawfully disclosed documents, and thus it is referred to here only as a document that is, in fact, available on the Internet, but without any suggestion that it is or is not what it purports to be, or that any statements within it are accurate. The 215 Bulk Primary Order discusses contact chaining through queries. 215 Bulk Primary Order, supra note 27, at 6.

60. See August 2013 FISC Order, supra note 4, at 11-13.

61. Alternative methods of collection would include non-bulk FISA orders, or what prior NSA Directors in the past have referred to as "vacuum cleaner" surveillance outside the ambit of FISA, under Executive Order 12,333 and its subordinate procedures, such as DOD 5240.1-R, and perhaps voluntary production if not otherwise prohibited by law. See NSA End-to-End Review, supra note 6, at 15; August 2013 FISC Order, supra note 4, at 10 n.10 ("The Court understands that NSA receives certain call detail records pursuant to other authority, in addition to the call detail records produced in response to this Court's Orders."); cf. 18 U.S.C. § 2511(2)(f) ("Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a method other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance (now International Telecommunication) Act of 1978"). A purported September 2006 letter from the Acting General Counsel of NSA to the Counsel for Intelligence Policy at DOJ, Attachment B to the Wainstein Contact Chaining Memo, notes that "NSA acquires this communications metadata... under Executive Order 12,333. All of the communications metadata that NSA acquires under this authority should have at least one communicant outside the United States." For a discussion of "vacuum cleaner" surveillance, see NSIPR supra note 1, at § 16.5 & on an 14-31, § 16.12-16.17. For a discussion of Executive Order 12,500, see NSIPR supra note 1, at §§ 2.7-2.9, Appendix J. The purported Wainstein Contact Chaining Memo discusses such contact chaining with respect to the "large amount of communications metadata," including
technicians may access the metadata to make the data more useable — e.g., to create a "defeat list" to block contact chaining through "high volume identifiers" presumably associated with telemarketing or similar activity.62

8. When a query produces information of interest, and the information pertains to a U.S. person, one of 11 persons (holding any of seven senior positions at NSA) must approve before the information may be disseminated outside of NSA (e.g., to the FBI), and it may be disseminated only if it pertains to counterterrorism and is necessary to understand counterterrorism information, or assess its importance.63

9. Metadata that has not been reviewed and minimized is retained for five years, consistent with the general five-year retention period for NSA data set out in USSID-18,64 and is purged automatically from NSA’s systems on a rolling basis.65 Data that is determined to have been improperly collected, e.g., due to a compliance problem, is also purged, as the Deputy Director of NSA explained:

It gets fairly complicated very quickly, but we have what are called source systems of record within our architecture, and those are the places that we say, if the data element has a right to exist [e.g., was properly collected and has not expired] it’s attributable to one of those. If it doesn’t have the right to exist, you can’t find it in there. And we have very specific lists of information that determine what the provenance of data is, how long that data can be retained. We have on the other side of the coin purge lists that . . . if we were required to purge something [e.g., due to an improper collection], that item would show up explicitly on that list. And we regularly run that against our data sets to make sure that we’ve checked and double-checked that those things that should be purged have been purged.66

10. The bulk telephony metadata collection program has suffered a number of compliance issues,67 and the FISA Court has been very concerned about the

62. See 215 Bulk Primary Order, supra note 27, at 5-6; August 2013 FISC Order, supra note 4, at 5-6.

63. June 2013 NSA Section 215 Backgrounder, supra note 27, at 1; June 2013 HPSICI Open Hearing, supra note 27 (statement of Chris Inglis) (“Only seven senior officials at NSA may authorize the dissemination of any information we believe that might be attributable to a U.S. person . . . . And thus dissemination in this program would only be made to the Federal Bureau of Investigation, after determining that the information is related to and necessary to understand a counterterrorism initiative.”); July 2013 FISC Hearing, supra note 27 (statement of Chris Inglis); 215 Bulk Primary Order, supra note 27, at 13. This standard is similar in certain ways to the minimization standards governing dissemination of other FISA information. For a discussion of FISA minimization, see NSIP, supra note 1, at §§ 9.1 et seq. In June 2009, the government informed the FISC that “unminimized results of some queries of metadata [redacted] had been ‘uploaded’ [by NSA] into a database to which other intelligence agencies . . . had access.” In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things [Redacted], No. BK-09-06 (FISA CA, June 22, 2009) (square bracketed material pertaining to NSA and ellipsis in original), available at http://www.dni.gov/files/documents/seclaw/9-22-2009%20Order.pdf. For a discussion of USSID-18, and the five-year retention period, see NSIP, supra note 1, at §§ 2; 7; 2:18.

66. June 2013 NSA Section 215 Backgrounder, supra note 27, at 2; June 2013 HPSICI Open Hearing, supra note 27 (statement of Chris Inglis) (Metadata collected under this program “simply ages off . . . at the expiration of those five years [and] is automatically taken out of the system . . . . just deleted from the system . . . . It’s destroyed when it reaches five years of age.”); 215 Bulk Primary Order, supra note 27, at 14; August 2013 FISC Order, supra note 4, at 14.

67. June 2013 HPSICI Open Hearing, supra note 27 (statement of Chris Inglis) (Metadata collected under this program “simply ages off . . . at the expiration of those five years [and] is automatically taken out of the system . . . . just deleted from the system . . . . It’s destroyed when it reaches five years of age.”); 215 Bulk Primary Order, supra note 27, at 14; August 2013 FISC Order, supra note 4, at 14.
issues, issuing strong rebukes and adding new restrictions to the program. According to the government, none of the compliance incidents reported to the FISC has been intentional and, since 2009, none has involved application of the RAS standard. In a July 2013 letter, the DNI stated that since “the telephony metadata program under section 215 was initiated [in May 2006], there have been a number of compliance problems that have been previously identified and detailed in reports to the Court and briefings to Congress as a result of Department of Justice reviews and internal NSA oversight. However, there have been no findings of any intentional or bad-faith violations.”

---

![Image of a page from a document]
discussed in § 2:18 of NSIP, the FBI's Consolidated Domestic Operations Guidelines (DOG), approved by the Attorney General under Executive Order 12333, divide investigative activity into three or four main categories: assessments (formerly known as "threat assessments," the term used in the tangible things statute); preliminary investigations; full investigations; and enterprise investigations (which are a species of full investigation). Under the DOG, an assessment must have an authorized purpose but does not require any factual predicate — e.g., it does not require any suspicion that someone is committing a crime. A preliminary investigation requires information that a crime or national security threat "may occur" or may have occurred, or that affirmative foreign intelligence "may" be obtained. A full or enterprise investigation requires "an articulable factual basis" to believe that the "may occur" standard has been met. As described in the DOG, an enterprise investigation is broad in scope:

The distinctive characteristic of enterprise investigations is that they concern groups or organizations that may be involved in the most serious criminal or national security threats to the public — generally, patterns of racketeering activity, terrorism or other threats to the national security, or the commission of offenses characterizedly involved in terrorism as described in 18 U.S.C. 2332b(g)(5)(B). A broad examination of the characteristics of groups satisfying these criteria is authorized in enterprise investigations, including any relationship of the group to a foreign power, its size and composition, its geographic dimensions and finances, its past acts and goals, and its capacity for harm.16

Section 106 of the conference report is a compromise between section 107 of the House bill and section 7 of the Senate amendment. This section of the conference report amends section 215 of the USA PATRIOT Act to clarify that the tangible things sought by a section 215 FISA order ("215 order") must be "relevant" to an authorized preliminary or full investigation to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities. The provision also requires a statement of facts to be included in the application that shows there are reasonable grounds to believe the tangible things sought are relevant, and, if such facts show reasonable grounds to believe that certain specified connections to a foreign power or an agent of a foreign power are present, the tangible things sought are presumptively relevant. Congress did not intend to prevent the FBI from obtaining tangible items that it currently can obtain under section 215.


It is quite easy to believe — in fact, it would be difficult not to believe — that the FBI has opened full or enterprise investigations into al Qaeda and other international terrorist groups under this authority. As noted above, the government confirmed that the bulk telephony metadata order involves several listed terrorist organizations that are specified in the application and the FISA Court's primary order, and that "we can investigate the organization, not merely an individual or a particular act, if there is a factual basis to believe the organization is involved in terrorism." These investigations have an extremely wide aperture when it comes to the terrorist groups in question, meaning that the FBI seeks to know essentially everything about the groups and how they operate. The FBI could have thousands of open full or enterprise investigations on terrorist groups or targets, and/or their sponsors, some or all of which could underlie the bulk telephony metadata collection applications and orders.

If the authorized "investigations" concern the specified terrorist groups, the question remains whether "there are reasonable grounds to believe" that bulk telephony metadata is "relevant" to those investigations. In its August 2013 opinion, the FISC concluded that there are, explaining: "Because known and unknown international terrorist operatives are using telephone communications, and because it is necessary to obtain the bulk collection of a telephone company's metadata to determine those connections between known and unknown international terrorist operatives as part of authorized investigations, the production of the information sought meets the standard for relevance under Section 215."17 The FISA Court concluded, by analogy to the standard articulated in§ 772, that information was "relevant" if it "has some bearing on [the government]s investigations of the identified international terrorist organizations,"17 and that bulk collection is necessary to find the relevant connections between terrorists.17 Because the subset of terrorist communications is ultimately contained within the whole of the metadata produced, but can only be found after the production is aggregated and then queried using identifiers determined to be associated with identified international terrorist organizations, the whole production is relevant to the ongoing investigation out of necessity.18

75. July 2013 FISC Opinion, supra note 27, at 7; supra note 27, at 6-7; supra note 27, at 6-7. See, for example, July 2013 FISC Opinion, supra note 27, at 6-7 ("it is reasonable to believe that the FBI's bulk collection of telephony metadata has identified the particular terrorist entities that are the subject of the investigations."); supra note 27, at 6-7; supra note 27, at 6-7; supra note 27, at 6-7.

76. See White Paper, supra note 27, at 6-7 (noting that "there has been no evidence that the FBI investigations have been hindered by the lack of the bulk telephony metadata records that are relevant").
This reasoning, echoed by the government in its White Paper and a letter to Congress, is quite similar to arguments made in favor of relevance by outside observers. One of the clearest such arguments is that "large databases are effective in establishing patterns only to the extent they are actually comprehensive"; that when they are comprehensive they can "reveal the organizational details of social structures" like terrorist groups and activities; and that accordingly there are "reasonable grounds to believe that the telephone call metadata database is relevant to the discovery of that structure and therefore relevant to an investigation of those terrorists." As a former government official put it in testimony before the House Judiciary Committee in July 2013, "the telephone metadata is 'relevant' to counterterrorism investigations because the use of the database is essential to conduct the link analysis of terrorist phone numbers... and this type of analysis is a critical building block in these investigations. In order to 'connect the dots,' we need the broadest set of telephone metadata we can assemble, and that's what this program enables."

Kieran Henley (a sociology professor at Dike) - "Using Metadata to Find Paul Revere." Healy did a very simple form of matrix analysis using only two factors -- the name of a person and the name of the political clubs he belonged to -- and applied it to the colonial revolutionaries. The names were familiar -- Sam and John Adams -- as were the clubs (the North Party and the Long Room Club, for example). He used data collected from historical records by David Hackett Fischer that might well have been available to the British at the time of the revolution. The results demonstrate the power of matrix analysis. And, notably, this is only analysis of metadata (who belonged to which clubs) and not all related to any of the content of what happened inside those clubs.

What he found is quite stunning for those who don't know big data. Perhaps it's a bit of a spoiler to say so (and I urge you, if you are interested, to read the whole paper, which is quite entertaining) but it turns out that the data pop out one man as the lynxhipton for a large fraction of the organizations of the clubs and the men in Boston — Paul Revere. And while, in historical retrospect he may not have been THE leader of the revolution, it's pretty clear that he was a significant operative in the revolutionary operations. And with just two fields of data British counter-intelligence of the era might have learned about his significance. (Note, of course, that more fields of data gives even greater granularity and tidiness to the conclusions.) And that, I think, is the answer to the relevancy question. It is quite easy, in fact, to say that the large data set can, with appropriate manipulation, reveal the organizational details of social structures. Terrorist activities are social structures of that sort. To my mind it is pretty clear that there are reasonable grounds to believe that the telephone call metadata database is relevant to the discovery of that structure and therefore relevant to an investigation of those terrorists. I'm not at all surprised that the FISA Court agreed.

84. July 2013 HJC Hearing, supra note 23 (statement of Stephen Bradbury). One of the clearest counter-arguments is simply that, in the words of a capable observer, "if that constitutes relevance for purposes of [the tangible things provisions] than isn't it all data relevant to all investigations?" Benjamin W. Lees, A Correction and a Retraction, LawAnd (June 6, 2013), http://www.lawand.org/20130606/ correction-and-a-retraction. The blog post explains in more detail the reasoning underlying this concern.

So presumably, the theory would have to be that the "tangible things" here are the giant ongoing flood of data from the telecommunications companies and that they are "relevant to an authorized investigation," perhaps of Al Qaeda, "to protect against international terrorism." That reading seems oddly consistent with the statute text, which may be why the intelligence committee leadership seems so comfortable with the program.

But that still leaves the question of how it's possible to regard metadata about all calls to and from a Donizzi Pizza in Peruca, Illinois or all calls over a three month period between two small businesses in Juneau, Alaska as "relevant" to an investigation to protect against terrorism. I think the only possible answer to this question is that a dataset of this size could be "relevant" because there are ways of analyzing big datasets algorithmically to yield all kinds of interesting things -- but only if the dataset is known to include all of the possibly relevant material. The individual data may be not relevant, but the dataset or data stream is relevant because it is complete -- and therefore is sure to include any communications by whomsoever we turn out to be concerned about.

But here's the problem: if that constitutes relevance for purposes of Section 215 then isn't it all data relevant to all investigations? Grand jury subpoenas, after all, are issued not just on the basis of relevance too -- albeit relevance to a criminal investigation. Why couldn't the FBI obtain all...
As discussed in §§ 19-1 and 19-5 of NSIP, the tangible things provision states that an order “may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things.”

In the grand jury context, where the test governing a challenged domestic metadata on the theory that some sort of data-mining would be useful in a mod investigation—and that a complete database is therefore “relevant” to it?

85. 50 U.S.C. § 1861(e)(2)(D). There is no question that telephony metadata records generally can be produced via grand jury subpoena, see 18 U.S.C. § 2703(c)(2), and to the extent that this provision limits the general type of information that may be obtained, it is clearly satisfied here. For a discussion of the issues pertaining to the amount of information that can be obtained, or whether data sets rather than individual pieces of data can be collected by grand jury subpoena, see discussion in the text.

In 2008, the FSCC issued an opinion addressing whether the tangible things provision could be used to collect telephone business records in light of 18 U.S.C. § 2702(d). Supplemental Opinion, In re Production of Tangible Things From (Redacted); No. BR 08-13 (FSCC; C- Dec. 12, 2008), available at http://www.dni.gov/files/documents/section/pbk_dni/2012%2008-20Supplemental%20Opinions %20frntm%20fr%20FSCC.pdf. The court concluded, after a brief analysis, that it could. The issue has nothing to do with bulk collections per se, but instead concerns whether the tangible things provision may be used to collect telephone records at all, even on an individual basis.

As one capable commentator has explained, see Marty Lederman, The Kris Paper and the Problematic FISC Opinion on the Section 215 ‘Metadata’ Collection Program, In JustSecurity (Oct. 27, 2013), http://justsecurity.org/2013/10/01/kris-paper-legality-section-215-metadata-collection/, 18 U.S.C. § 2702(a)(5) generally prohibits a telephone company from providing call detail records to the government, and (via 18 U.S.C. § 2702(b)(3)) provides several exceptions under which a provider "shall disclose to a governmental entity" such records (as specified in the statute), including "when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State Regulation," or a "grand jury or trial subpoena." 18 U.S.C. § 2702(b)(2). A "grand jury or trial subpoena" is a court order "if the grand jury or trial subpoena . . . (A) is served on a provider; (B) is signed by a judge; (C) contains a description of the tangible thing[s] requested; and (D) is directed to a provider which is a provider of Internet access service, a remote computing service, or a provider of a mass storage communication service that is engaged in providing a service to the grand jury or trial subpoena." a provider which is a provider of Internet access service, a remote computing service, or a provider of a mass storage communication service that is engaged in providing a service to the grand jury or trial subpoena.

Subpoena is whether there is any "reasonable possibility" that the materials sought "will produce information relevant to the general subject matter of the grand jury's investigation," the results often depend on the facts, as illustrated by three cases discussed below.

In re Grand Jury Proceedings, the Tenth Circuit held that it was "legal error" for a district court to "definit[e] the categories of material sought by the Government in order to assess relevancy and further engaging in a document-by-document and line-by-line assessment of relevancy"; that the court was "bound to assess relevancy based on the categories of materials sought by the government;" and that the court could not "create new categories for purposes of assessing relevancy." Although it could "sympathize with the district court's desire to prevent the grand jury from subpoenaing wholly irrelevant information," the court of appeals observed that "incidental production of irrelevant documents . . . is simply a necessary consequence of the grand jury's broad investigatory powers and the categorical approach to relevancy adopted" by the Supreme Court. Although it appears to require an all-or-nothing approach with respect the contrary, it appears to have been assumed that the FISC would continue to enjoy authority to issue such "pure" tangible-things orders as needed. See, e.g., 151 Cong. Rec. S14006-01 (Dec. 19, 2005), Statement of Senator Specter (referring to Attorney General Gonzales' testimony on the tangible-things provision, "if they exist, they can be obtained telephone records.

The 2006 legislation amended the tangible-things provision itself, as discussed in NSIP, supra note 1, at §§ 19-1 and 19-2, but the Conference Report explained that "Congress does not intend to prevent the FBI from obtaining tangible items that it currently can obtain under section 215." H.R. Rep. No. 109-133, at 91 (2005) (Conf. Rep.). Whatever the technical merits as a textual matter prior to 2006, it seems that all three branches of government publicly understood Section 215 to permit orders for call detail records, and that Congress renounced the Patriot Act with that interpretation in mind. As such, there is an argument for ratification of the interpretation through enactment of the 2006 legislation, under the standards discussed in the text infra. Ironically, if the tangible things provision had been interpreted to exclude telephone records, the government apparently could have obtained the information in bulk by using the pen/trap provisions of FISA, which as noted above were amended expressly to authorize collection of the information in 2006, and which underlay the bulk collection of Internet metadata beginning as early as 2004 as mentioned in the text, supra. In December 2013, a district court in the Southern District of New York rejected a claim based on Section 2102, concluding that when "[t]o be in harmony, the Stored Communications Act does not limit the Government's ability to obtain information from communications providers under section 215 because section 215 orders are functionally equivalent to grand jury subpoenas. Section 215 authorizes the Government to seek records that may be obtained with a grand jury subpoena, such as telephony metadata under the Stored Communications Act." ACLU v. Clapper, No. 13 Civ. 3994(WHP) (S.D.N.Y. Dec. 27, 2013), 2013 WL 6819708 at *13.


87. In re Grand Jury Proceedings, 616 F.3d 1186 (10th Cir. 2010).

88. Id. at 1202.

89. The facts in this case are quite different than in the context of bulk collection of telephony metadata. The subpoena in question sought documents "regarding an employee's involve- in completing" certain forms for the company that employed him, and following an in camera review, the district court rejected the production of some, but not all, of the documents within the scope of the subpoena, and allowed redactions of other documents. Id. at 1191-1192.
to the categories (or sub-categories) of information sought and specified in the subpoena, and despite some expansive language, the decision is not properly read to hold that the presence of even one relevant document in a larger category of documents would support production of the entire category, no matter how broadly it is defined.

A second case, interesting not only because of its holding but also because of its author, is Judge Mukasey's decision In re Grand Jury Subpoena Duxes Tecum Dated November 15, 1993.90 There, the court held that two grand jury subpoenas were overbroad in seeking entire hard drives and related floppy disks from the computers of certain employees of a company, as part of an investigation of securities fraud and possible obstruction of justice.91 There was no question, and the government conceded, that the hard drives and disks contained some material that was wholly irrelevant to the grand jury's investigation, such as a draft will for one employee.92 The question, then, was whether the appropriate "category of materials" to be assessed was "the information-storage devices demanded, or... the documents contained within them."93 The court held that it was the documents, in part because "the government has acknowledged that a 'key word' search of the information stored on the devices would reveal 'which of the documents are likely to be relevant to the grand jury's investigation,' but still tried to insist on receiving all of the storage devices in full."94 Judge Mukasey's decision seems to depend in substantial part on the idea that the government had at its disposal a feasible method of pre-filtering the information to be collected -- a concession that the government has not made with respect to its bulk collection of telephony metadata.

Perhaps the closest analogue in the grand jury context, albeit on a much smaller scale than the FISC's order, is In re Grand Jury Proceedings: Subpoena Duxes Tecum.95 In that case, "the United States Attorney caused two grand jury subpoenas duxes tecum to be served on employees of appellant Western Union Telegraph Company" for records of its customers' wire transfers.96

90. In re Grand Jury Subpoena Duxes Tecum, 846 F. Supp. 11 (S.D.N.Y. 1994) (Mukasey, J.). Judge Mukasey was Attorney General from November 2007 through the end of President George W. Bush's second term. As explained above, the bulk telephony metadata collection was underway in the FISC during this period. Of course, by the time Judge Mukasey was sworn in, the FISC had already approved the bulk collection numerous times, and it is quite different to allow continuation of judicially-approved investigative activity than to attempt to initiate it.

91. As described by the court, the "subpoenas demand that X Corporation provide the grand jury with the central processing unit (including the hard disk drive) of any computer supplied by X Corporation for the use of specified officers and employees of X Corporation, or their assistants. It demands also all computer-accessible data (including floppy diskettes) created by any of the specified officers and employees or their assistants," id. at 12.

92. Id.

93. Id.

94. Id. at 13.


96. Id. at 302.

The first subpoena requested production of Western Union's Agency Monthly Summary of Activity Report of wire transactions at the Royale Inn, Kansas City, Missouri for the period January, 1985 through February, 1986. The second subpoena requested production of Western Union's Telegraphic Money Order Applications for amounts of $1,000.00 or more from the Royale Inn for the period January, 1984 through February, 1986. The Royale Inn is Western Union's primary wire service agent in the Kansas City area.97

In response to Western Union's motion to quash the subpoena, the government maintained that along with law-abiding persons, "drug dealers in Kansas City frequently use Western Union to transmit money in drug deals" under both true and fictitious names.98 This was enough for the court of appeals to reject Western Union's constitutional and statutory arguments, despite the company's claim that "the subpoena may make available to the grand jury records involving hundreds of innocent people."99

The court left open the possibility of narrowing the subpoena on remand, allowing the district court to consider "the extent to which the government would be able to identify in advance those patterns or characteristics [of wire transfers] that would raise suspicion."100 While it endorsed the idea that a "common law right does not in any way restrict the grand jury's access to records for which the government can make a minimal showing of general relevance," it also allowed the district court to consider "evidence of potentially adverse effects on Western Union's business should it be compelled to produce an overabundance of irrelevant data concerning its customers' transactions" -- a factor that seems more significant after the June 2013 disclosures than it did previously.101

In the context of administrative or civil subpoenas, which are expressly cross-referenced along with grand jury subpoenas in FISA's tangible things provision,102 and which also turn on a relevance determination, the courts have upheld relatively broad subpoenas, but as in the grand jury context, no single subpoena discussed in a reported decision is as broad as the FISC's telephony

97. Id. at 13.

98. Id.

99. Id. at 305.

100. Id. at 306. See also State ex rel. Goddard v. Western Union Financial Services, Inc., 166 P.3d 916 (Ariz. App. 2007) (quashing administrative subpoena under state statute for "data reflecting any wire-transfers made in an amount of $300 or more to any location in Sonora, Mexico from any Western Union location worldwide for a three year period."), cert. denied, 131 S. Ct. 151 (2010).

metadata orders. 103 For example, in Gonzales v. Google, 104 in connection with a facial challenge to the Child Online Protection Act, 105 the Department of Justice issued a subpoena to Google "to compile and produce a massive amount of information,"106 and the court found "that 50,000 URLs randomly selected from Google’s data base for use in a scientific study of the effectiveness of filters is relevant."107 In High Point SARL v. Sprint Nextel Corp., 108 although Sprint had produced a spreadsheet containing "over 1.1 million entries" concerning certain handover components on a network, the court ordered production of the entire database from which the spreadsheet was derived, despite claims that "the ... database in its entirety includes tremendous quantities of irrelevant information."109 The court also granted a motion to compel in connection with a demand to "[i]dentify all revenue received by Sprint directly or indirectly from operation of the Sprint CDMA Network (including service revenue and product sales revenue) on a monthly basis since December 1, 2002, with such revenue broken down by each category of revenue separately tracked by Sprint, including by type of traffic (e.g., voice versus data), by geographic location, and by supplier or manufacturer of the Infrastructure Products."110

As a matter of the tangible things provision’s statutory text, there are at least four ways to approach the issue. First, there is the question of what might be called the relevance ratio – i.e., the ratio of the number of terrorist-related calls to the total number of calls on which metadata is collected. As discussed above, there is language in some cases suggesting that even a single needle will justify collection of a large haystack, but there obviously must be some limiting principle, beyond the government’s ability to describe it in the subpoena or court order, on the maximum size of the haystack and the minimum ratio required. Second, there is the related question whether the data set as a whole is somehow more “relevant” than the sum of its parts – e.g., whether the haystack is relevant because it contains all of the needles and allows searches for them in a comprehensive and/or efficient manner that would be impossible if the data were disaggregated. Third, expressing the same idea in the language of a different statutory term, what is the tangible “thing” that must be relevant and that the government may seek – i.e., what is the unit of analysis for evaluating

111. A related question is whether electronic records are “tangible things” within the meaning of the PISAA provision. It is reasonably clear that they are, because the statute refers to “any tangible things (including books, records, papers, documents, and other items).” 50 U.S.C. § 1861(a)(1). As used in the provision, therefore, “records” embraces something different from mere paper “documents.” See H.R. Rep. No. 109-748 at 17 (2006).


113. See, e.g., June 2013 IC Backgrounder, supra note 27, at 1. On August 17, 2009, the Directors of FBI and NSA submitted affidavits to the FISC describing the value of the bulk telephony metadata collection program. See Affidavit of Robert S. Mueller III & Declaration of L. Gen. Keith B. Alexander, U.S. Army, Dir. of the Nat’l Sec. Agency, In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted], N.Y. BR 09-09, at 5 (FISA Ct. 2009), available at http://www.dni.gov/files/documents/section/pub August%2019%202009%20Report%20On%20the%20US%20with%20Attachments%2020130910.pdf. In its August 2013 Justice Department amicus, it argued that the collection, the FISC had determined “although not required by the collection, the government has demonstrated through its written submissions and oral testimony that this production has been and remains valuable for obtaining foreign intelligence information regarding international terrorist organizations.” August 2013 FISC Order, supra note 4, at 5-6. One district judge concluded that the bulk collection program was not very valuable: “Given the limited record before me at this point in the litigation – most notably, the utter lack of evidence that a terrorist attack has ever been prevented because searching the NSA database was faster than other investigative tactics – I have serious doubts about the efficacy of the metadata collection program at a moment of mounting time-sensitive investigations in cases involving imminent threats of terrorism.” Klayman v. Obama, No. 13-0851 (D.C. Cir. 2013) (D.C. Cir. Dec. 16, 2013) [hereinafter December 2013 Klayman Opinion]. Another district judge referred to the collection as a “vital tool” and concluded: “Any individual call record alone is unlikely to lead to matter that may pertain to a terrorism investigation . . . . But aggregated telephony metadata is relevant because it allows the querying technique to be comprehensive. And NSA’s warehousing of that data allows a query to be instantaneous. This new ability to query aggregated telephony metadata significantly increases the NSA’s capability to detect the faintest patterns left behind by individuals affiliated with foreign terror organizations.” ACLU v. Clapper, No. 13 Civ. 3994 (WHP), 2013 WL 6819708, at *18, *27 (S.D.N.Y. Dec. 27, 2013) [hereinafter ACLU Opinion]. The President’s Review Group stated that “there has been no instance in which NSA could say with confidence that the outcome could have been different without the section 215 telephony meta-data program. Moreover, now that the existence of the program has been
It is also clear that only the tiniest fraction of the data collected reflects communications between suspected terrorists and persons in any way associated with terrorism — as noted above, fewer than 300 different seed selectors were run against the metadata in 2012, causing NSA to review approximately 6,000 numbers in total. But having the larger data set on hand for five years may allow for real-time (and after-the-fact) mapping of terrorist networks in a way that individualized collection obviously could not achieve, especially given the providers’ inconsistent retention of records over time, and the fact that each provider retains only its own records, even though calls are obviously made from one provider’s network to another’s. As noted above, that is the government’s basic argument and the FISA Court’s basic conclusion: the telephony metadata must be available in bulk to allow NSA to identify the records of terrorist communications because without access to the larger haystack of data, it cannot find the needles using the much narrower querying process.

Perhaps the best assessment of the program’s value was provided by Chris Inglis, the departing Deputy Director of NSA, in January 2014. Inglis explained the limited purpose of the bulk metadata program, which was “precisely defined to cover a scan exposed in the 9/11 terrorist attacks,” where “we could see...
I think we as a nation have to ask ourselves the policy question of what risks do we want to cover? Do we want to cover 100 percent of the risk? Or do we want to perhaps take a risk that from time to time something will get through? 9/11 was the single execution, it was the execution of a single plot with multiple threats. And about 3,000 people lost their lives that day. That’s one terrorist plot coming to fruition.

If that is an acceptable cost, if we can say, we can take the risk that we’ll miss something, then we don’t need to have all of the tools that cover these various seams. We don’t need to have the belts and suspenders and Velcro that essentially will overlap in an interlocking way. The 215 is designed to essentially cover a seam that we don’t know any other way to cover. 124

In keeping with this assessment, although the tangible things provision refers to “an investigation” in the singular, it appears (as discussed above) that the bulk collection was conducted in respect of many investigations of multiple, named terrorist targets and/or groups. 123 This raises a separate interpretive question about whether the singular can include the plural, 125 but with respect to the scope of the collection, it suggests that the relevant comparison may not be to any grand jury or other subpoena issued in a single investigation, but instead to the aggregate of subpoenas that could be or were issued in all of what may be thousands of specified terrorism investigations that underlie the bulk metadata collection. 124 In a way, the bulk collection orders represent a kind of aggregation of terrorism-related collection – one-stop shopping across a potentially very large number of ongoing full or enterprise investigations. It reflects the fact that the bulk collection occurs in a unique context.

2. FISA’s tangible things provision is unusual in that it discriminates among federal agencies, referring specifically to the FBI rather than any other agency. 125 It authorizes certain FBI officials to make the necessary application, 126 and requires approval from a high-ranking FBI official if the tangible things sought are particularly sensitive (e.g., library patron lists). 127 Its language also strongly suggests that the FBI will receive the tangible things pursuant to the FISA Court’s order. Thus, for example, it requires the Attorney General to “adopt specific minimization procedures governing the retention and dissemination by the Federal Bureau of Investigation of any tangible things, or information therein, received by the Federal Bureau of Investigation in response to an order under this title,”128 and requires the application to include “an enumeration of those minimization procedures . . . applicable to the retention and dissemination by the Federal Bureau of Investigation of any tangible things to be made available to the Federal Bureau of Investigation based on the order requested in such application.”129 The statute restricts the use of information “acquired from tangible things received by the Federal Bureau of Investigation in response to an order . . . concerning any United States person.”130 The nondisclosure provision of the statute warns that in general, “No person shall disclose to any other person that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to an order under this section.”131

The FISA Court’s bulk collection order disclosed in June 2013 (and other publicly available documents) makes clear that the application underlying the collection was made by the FBI, as required by the statute. 132 But the order directs “the Custodian of Records to produce to the National Security Agency (NSA) . . . an electronic copy of the [specified] tangible things,” 133 and the nondisclosure directive refers to the fact “that the FBI or NSA has sought or obtained tangible things under this Order.”134 As such, the order seems to rest on a principle of minimization that national security agencies may share data freely with one another, without alteration, processing, or minimization, in some circumstances. Such an approach would have many practical advantages, particularly in terms of optimizing resources among the agencies. It has roots in FISA’s 1978 minimization provisions, as discussed in § 9.3, in situations where one agency is providing technical assistance to another (e.g., decryption), and it may be within the discretion of the FISC to approve, especially if, as may be the case here, the sheer volume of information is challenging for FBI to ingest and retain, and NSA’s bandwidth and other technical assistance is therefore required.

3. The tangible things provision states that an order “shall include the date on which the tangible things must be provided, which shall allow a reasonable period of time within which the tangible things can be assembled and made

121. Id.
122. See, e.g., August 2013 FISC Opinion, supra note 4, at 5 (referring to “one of the identified international terrorist organizations”).
123. The general rule is that it can, and there does not appear to be anything in the context of FISA or the tangible things provision to counsel against the application of this general rule. See 1 U.S.C. § 1 (“In determining the meaning of any Act of Congress, unless the context indicates otherwise . . . words importing the singular include and apply to several persons, parties, or things.”).
124. June 2013 NSA Section 215 Backgrounder, supra note 3, at 1 (“This metadata may be queried only when there is a reasonable suspicion . . . that the identifier . . . is associated with specific foreign terrorist organizations”); June 2013 HPSCI Open Hearing, supra note 27 (statement of James Cole) (“There needs to be a finding that there is reasonable suspicion . . . that the person whose phone records you want to query is involved with some sort of terrorist organization. And they are defined – it’s not everyone; they are limited in the order”).
125. This is not unprecedented – for example, national security letter statutes apply in various ways to various agencies, as discussed in Chapter 20 of NSIP, supra note 1 – but most other provisions of FISA do not distinguish between agencies.
128. See chapter 11.
130. 50 U.S.C. § 1881(h).
131. 50 U.S.C. § 1806(g)(1).
132. 215 Bulk Secondary Order, supra note 3, at 1; August 2013 FISC Opinion, supra note 4, at 1; August 2013 Order at 1.
133. 215 Bulk Secondary Order, supra note 3, at 1-2.
134. Id. at 2; see id. at 3.
available.” The FISC’s order disclosed in June 2013 directs the Custodian of Records to produce records “upon service of this Order, and continue production on an ongoing daily basis thereafter for the duration of this Order.” The FISC’s conclusion, apparently accepted by the Custodian of Records, is that a rolling production ending on the last day of the period specified in the order is within the statutory language. Rolling production is a relatively common approach in grand jury and other subpoena-related cases. As one commentator has explained, “[i]n many instances, the [grand jury] subpoena will require millions of pages of documents to be located, retrieved, reviewed and produced within an unrealistically short time period. Defense counsel can typically negotiate a phased or rolling production that extends over weeks or months.”

The federal courts have on occasion required production of documents created after the date on which a subpoena was issued, or even after the subpoena’s return date. The alternative would be to issue multiple, separate orders seeking the same information on a daily basis; it is easy to see how the government, the FISC, and the Custodian of Records might all prefer the integrated approach actually used by the FISC.

4. The various restrictions on the use and dissemination of the data as described above, including the RAS query standard, originate from minimization as defined in FISA. As explained in § 9:10 of NSIP, the tangible things provision requires the government to adopt minimization procedures governing retention and dissemination of information (there is no requirement for minimization at the acquisition stage of a tangible things collection, because the scope of the authorized acquisition is defined by the court’s order itself). Minimization is the clearest statutory source of authority for the limited access and training obligations within NSA, the RAS standard for querying the data and the small number of officials who may approve RAS findings, the limited purpose of the queries (counter-terrorism only), and the procedural and substantive limits on dissemination of information to other agencies that are described above.

These limits are significant not only in and of themselves, insofar as they may affect the overall reasonableness and constitutionality of the telephony metadata collection, but also because of how they reveal the FISA Court and the government working with what is sometimes referred to as “big data.” As discussed in a 2009 essay, “the overwhelming increase in the volume and use of digital information left by individuals in the hands of third parties” in recent years “may in the future compel more attention to standards governing retention and dissemination of information. The next generation of surveillance statutes will need to reflect the fact that countless digital footprints left by individuals in the course of modern life – particularly in combination with one another – may contain revealing information. Many of the hardest decisions will lie in balancing privacy interests against investigative needs.” The FISC’s tangible things order, it appears, represents such an approach, with a vast collection at the front end of the program, and greater restrictions limiting access and use of the data downstream. It contrasts with a more traditional approach in which collection is relatively restricted (e.g., by a requirement to show probable cause for collection of data pertaining to a particular target), but downstream access and use of the collected data is relatively free.

A big-data compliance regime is harder to administer, and harder to follow, than a traditional regime. It is simpler to restrict collection and permit broad access and use of collected data, than it is to permit broad collection and restrict access and use. Big data is inherently hard to manage. That is not to excise the NSA’s compliance problems, or to suggest the inevitability of significant compli-
It is only to say that, on average, big-data collection regimes will inherently pose greater compliance challenges than traditional collection regimes.

5. It is also worth exploring briefly whether and to what extent the legal arguments in support of bulk telephony metadata collection could apply to other kinds of business records. At a June 2013 hearing of the House Intelligence Committee,\(^\text{147}\) a July 2013 hearing of the House Judiciary Committee,\(^\text{148}\) and a July hearing of the Senate Judiciary Committee,\(^\text{149}\) the issue was raised but not resolved. In a July 2013 letter to Congress, the DNI confirmed the prior use of “FISA authorities” to collect “bulk Internet metadata,” but said that “NSA has not used USA PATRIOT Act authorities to conduct bulk collection of any other types of records,” did not refer to other agencies or other collection methods, and did refer to “[a]dditional information” provided in a classified supplement to the letter.\(^\text{150}\) However, the express reference to grand jury subpoenas in the tangible things statute, coupled with the Western Union case described above, suggests that the legal logic behind the FISC’s telephony metadata order might extend to other forms of metadata held by other providers, regardless of whether or not it has in fact been so extended.

On the other hand, the government has expressly disclaimed the universal availability of bulk collection under FISA. The August 2013 White Paper argues that the legality of bulk telephony metadata collection “does not mean that any and all types of business records — such as medical records or library or bookstore records — could be collected in bulk under this authority.”\(^\text{151}\) The government explained that the telephony metadata is “relevant” to FBI investigations in part because it involves communications, “in which connections between individual data points are important, and analysis of bulk metadata is the only practical means to find those otherwise invisible connections.”\(^\text{152}\)

In a brief filed in the U.S. Supreme Court in October 2013, the government stated:

> The conclusion that the Telephony Records Program complies with Section 1861 does not suggest … that the “relevance” standard has no meaning. The government does not contend that Section 1861 — which applies to all “tangible things,” not only telecommunications records — may be used to collect in bulk records of any type. Rather, telecommunications records have characteristics not common to other types of records — specifically, their highly standardized and inter-connected nature — that make them readily susceptible to analysis in large datasets to bring previously unknown connections between and among individuals to light. The same cannot be said of myriad other types of records that might be subject to a Section 1861 order. In the distinctive and particularly critical context of telecommunications, all of the records are relevant to an authorized investigation, because it is only with the full set that this investigative tool can be used most effectively.\(^\text{153}\)

Additional insight into any other bulk metadata collection, perhaps not involving communications, will need to await further disclosures.

6. A final issue concerns the constitutionality of the bulk metadata collection. In Smith v. Maryland,\(^\text{154}\) the Supreme Court held that telephone company customers have no Fourth Amendment rights in the dialing information that they convey to the telephone company. The Court in Smith relied on its prior decision in United States v. Miller,\(^\text{155}\) which found no Fourth Amendment rights of a customer in his bank records held by the bank. As the Court explained in 1984,\(^\text{156}\) rejecting constitutional challenges to enforcement of an administrative subpoena, “[i]t is established that, when a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities.”\(^\text{157}\)

In its August 2013 opinion, the FISC relied on Smith and third-party doctrine to conclude that there was no Fourth Amendment violation in the bulk telephony metadata collection (and also noted that none of the providers had invoked a statutory procedure to challenge the orders in the FISC).\(^\text{158}\)

\(^{146}\) Some of NSA’s compliance problems in this area may stem from its changing mission after September 11, 2001, and the different legal rules that govern surveillance in the U.S. or involving U.S. persons, including the FAA, as discussed in Chapter 17 of this Report.\(^{147}\) In this respect, NSA may resemble to some degree a corporation that expands suddenly into a new market, and faces challenges in ensuring that its compliance capabilities keep pace with its operations.\(^{148}\) June 2013 HPCIC Open Hearing, supra note 27. At the hearing, the following colloquy occurred between a Member of the Committee and the Deputy Attorney General:

**Rep. Thompson:** Have you previously collected anything else under that authority?

**Mr. Cole:** Under the 215 authority?

**Rep. Thompson:** Correct.

**Mr. Cole:** I’m not sure, beyond the 215 and the 702, that — answering what we have and haven’t collected has been declassified to be talked about.

\(^{149}\) July 2013 HJC Hearing, supra note 23 (statement of James Cole) (Question: “Could you demonstrate—could you argue with a straight face you could demonstrate to the court to create a database of everybody’s Visa and MasterCard, every transaction that happened in the country because Visa and MasterCard only keep those for a couple years?” Answer: “It is not a simple yes or no. Black or white issue. It’s a very complicated issue.”).

\(^{150}\) July 2013 HJC Hearing, supra note 23 (statement of Senator Leahy) (“If our phone records are relevant, why wouldn’t our credit card records be relevant?”).

\(^{151}\) White Paper, supra note 27, at 5 (italics in original).

\(^{152}\) Id.


\(^{154}\) Smith v. Maryland, 442 U.S. 735 (1979).


\(^{157}\) See, e.g., Couch v. United States, 409 U.S. 322, 335 (1972). With respect to the rights of the telephone companies, see generally U.S. v. Powell, 379 U.S. 48 (1964) (discussing standards for enforcement of administrative subpoenas); Donovan v. Luna Stein, Inc. 464 U.S. 408 (1984) (recipient of a subpoena may complain if the subpoena is too burdensome and unreasonable).

\(^{158}\) August 2013 FISC Order, supra note 4, at 6-9, 14-16.
Judicial reaction outside the FISC has been mixed. In November 2013, a judge in the Southern District of California agreed with the FISC and denied a motion for new trial in a criminal case based on claims that the NSA's collection of bulk telephony metadata violated the Fourth Amendment. In that opinion, Justice Sotomayor wrote that it was possible that the program might be a violation of the Fourth Amendment, and that the risks associated with the collection were serious. She also noted that the program was a violation of the Constitution and that it should be stopped.

In a separate opinion, Justice Breyer concurred with the FISC's decision. He noted that the government had a strong interest in collecting metadata, but that the court should consider the specific circumstances in each case before allowing such a collection. He also noted that the government had not provided adequate justification for the collection of metadata, and that the court should consider whether the collection was likely to be successful.

In December 2013, a judge in the District of Columbia agreed with the FISC's opinion, finding that the collection of bulk telephony metadata violated the Fourth Amendment. He noted that the government had not shown that the collection was necessary to prevent imminent danger, and that the collection was likely to be ineffective. He also noted that the collection was a violation of the Constitution and that it should be stopped.

In 2014, the court in DC relied on the conclusion that Smith v. Maryland was outdated, and the logic of Justice Sotomayor's concurring opinion in Jones. In that opinion, the court noted that the collection of bulk telephony metadata violated the Fourth Amendment. It noted that the government had not shown that the collection was necessary to prevent imminent danger, and that the collection was likely to be ineffective. It also noted that the collection was a violation of the Constitution and that it should be stopped.
disagreed with the district court in DC and upheld the bulk collection program. As a statutory matter, the Southern District court found that “Congress ratified [50 U.S.C. § 1861] as interpreted by the Executive Branch and the FISC, when it reauthorized FISA.” Rejecting the DC district court’s reasoning explicitly, the Southern District court stated:

Some ponder the ubiquity of cellular telephones and how subscribers’ relationships with their telephones have evolved since Smith. While people may “have an entirely different relationship with telephones than they did thirty-four years ago,” this Court observes that their relationship with their telecommunications providers has not changed and is just as frustrating. Telephones have far more versatility now than when Smith was decided, but this case only concerns their use as telephones. The fact that there are more calls placed does not undermine the Supreme Court’s finding that a person has no subjective expectation of privacy in telephony metadata. Importantly, “what metadata is has not changed over time,” and “[a]s in Smith, the types of information at issue in this case are relatively limited: [telephone numbers dialed, date, time, and the like].” Because Smith controls, the NSA’s bulk telephony metadata collection program does not violate the Fourth Amendment.

Although not a judicial body, the President’s Civil Liberties Oversight Board (PCLOB) issued a report in January 2014 concerning the bulk telephony metadata program. Three members of the board concluded that “Section 215 [of the Patriot Act] does not provide an adequate legal basis to support the

program,”176 that Congress did not ratify the FISC’s contrary interpretation when it reenacted the statute,177 and that the program “raises concerns under both the First and Fourth Amendments to the United States Constitution.”178 Two other members of the board disagreed with these legal conclusions.179 Interestingly, although the Board found the program to be illegal, and a violation of FISA, it “recognize[d] that the government may need a short period of time to explore and institutionalize alternative approaches, and believes it would be appropriate for the government to wind down the 215 program over a brief interim period.”180

THE FISA COURT

The June 2013 disclosures gave rise to public discussions concerning the FISC, and in particular concerning (1) the selection method for its judges; and (2) the possibility of something approaching inter partes litigation on at least certain matters before the court. Although there is no real evidence of problems in the current process for selecting FISA Court judges, under which the Chief Justice makes the appointments,181 the vast majority of the Members of the FISC were appointed by Republican Presidents, and it would be relatively easy to change the selection process if desired. The possibility of a civil liberties advocate in the FISC is a more significant and difficult issue.

1. With respect to the selection of FISA Court judges, there have been claims that Chief Justice Roberts has chosen judges appointed by Republican Presidents, and that this has skewed the court in the government’s favor.182 In response, one commentator has observed, “the claim that Chief Justice Roberts’s appointments have ‘reshaped’ the Court to favor the executive branch

176. Id. at 10.
177. Id. at 10-11.
178. Id. at 11.
179. Id. at 209-210 (Statement of Rachel Brand); Id. at 214 (Statement of Elisabeth Collins Cook).
180. Id. at 17. It is not entirely clear how the PCLOB could recommend a wind-down period, other than an immediate stop, for a collection program it believes is unlawful. The PCLOB did recommend adoption of several privacy enhancements during the wind-down period, but none of them appear to affect the legality of the program. See id. The report states: “To be clear, the Board believes that this program has been operated in good faith to vigorously pursue the government’s counterterrorism mission and appreciates the government’s efforts to bring the program under the oversight of the FISA court. However, the Board concludes that Section 215 does not provide an adequate legal basis to support this program. Because the program is not statutorily authorized, it must be ended.” Id. at 57.
181. For a discussion of the FISC, including the Chief Justice’s authority to appoint judges to it, see NSIP, supra note 1, at § 5.1 et seq. and especially § 5.3.
182. For the current membership of the FISA Court, see The Foreign Intelligence Surveillance Court, Fed. on Am. Spectrums, https://www.fisa.gov/spagency/doj/fisa/court2013.html.

13. See, e.g., Sen. Richard Blumenthal, FISA Court Scrutiny Must End, POLITICO (July 14, 2013), http://www.politico.com/story/2013/07/fisa-court-process-cannot-be-unveiled-941417.html (“My proposal, which I plan to introduce this month, will bring transparency to the process for selecting FISA court judges and ensure a broader diversity of views on the bench. It also will ensure that FISA court rulings are the product of a process in which both sides have the opportunity to be heard, a process designed to keep the government honest and allow for balanced consideration of difficult issues.”).
in applications for warrants does not withold a moment's scrutiny. That's because the Court's approval rate has always hovered near 100% - both before and after the Roberts era. No discernable reshaping has occurred. Whatever the ideological makeup of the current FISC, as a simple matter of timing, Chief Justice Roberts was confirmed in September 2005, and as noted above the FISC first approved the bulk telephony metadata collection in May 2006, before he had any real impact on the Court's membership.

More broadly, it is important to consider the context in which the FISA Court initially approved the bulk collection. As noted above, bulk telephony metadata collection was occurring before May 2006 pursuant to Presidential authorization and voluntary cooperation from the telecommunications providers. Accordingly, the practical question before the FISC in 2006 was not whether the collection should occur, but whether it should occur under judicial standards and supervision, or unilaterally under the authority of the Executive Branch.

Nonetheless, if desired, it would be possible formally to dispense the authority to select FISA judges. For example, the Chief Judges of the regional courts of appeals could each name a judge, as long as there was some weighting mechanism to ensure a sufficient number of DC-area judges to handle emergencies, and with some reasonable system of rotation to account for the fact that

184. Steven Aftergood, Did Justice Roberts Reshape the FISA Court?, SECURITY NEWS (July 29, 2013), http://blogs.fas.org/security/2013/07/roberts-reshape/. See also Editorial, More Independence for the FISA Court, N.Y. TIMES, July 29, 2013, at A16 (“All 11 of the current members were assigned to the court by Chief Justice John Roberts Jr. In the nearly eight years he has been making his selections, Chief Justice Roberts has leaned about as far right as it is possible to go. Ten of those 11 members were appointed to the bench by Republican presidents; the two previous chief justices put Republican-appointed judges on the court 66 percent of the time.”). As the Presiding Judge of the FISA Court has pointed out, the approval rate for Title III warrant applications, which are used in ordinary criminal cases, is similar to the approval rate for FISAs. See Letter from Judge Reggie Walton to Senator Patrick Leahy (July 29, 2013) at 2 n.3 (hereafter July 2013 Walton-Leahy Letter). (the approval rate for Title III warrant applications, . . . . is higher than the approval rate for FISAs. See Letter from Judge Reggie Walton to Senator Patrick Leahy (July 29, 2013) at 2 n.3 (hereafter July 2013 Walton-Leahy Letter) at 2 n.3 (hereafter July 2013 Walton-Leahy Letter). The letter contains a 14-page Appendix to the letter, dated January 10, 2014, and describes itself as “setting forth the Judge’s comments concerning certain potential changes to FISA and proceedings before the FISC and the Foreign Intelligence Surveillance Court of Review.” It explains that “[t]raditionally, the view of the Judiciary on legislative matters are expressed through the Judicial Conference of the United States, for which I serve as secretary. However, because the matters at issue here relate to special expertise and experience of only a small number of judges on two specialized courts, the Conference has not at this time been engaged to deliberate on them.” In preparing the letter, Judge Bates, himself a former Presiding Judge of the FISC, “consulted with the current Presiding Judges of the FISC and the Court of Review, as well as with other judges who serve or have served on those courts.” Id. at 1.

185. See December 2013 Fleisch Declaration, supra note 17, at 5, 13, 18-19.

186. With respect to metadata concerning foreign-to-foreign communications, which the FISC’s order expressly does not address, see 18 U.S.C. § 2511(2)(f). Section 2511(2)(f) exempts from the prohibitions in Title III certain types of production of data by telecommunications providers. As Chris Ingels, Deputy Director of NSA explained, the unauthorized disclosures have “strained” relationships between NSA and the private sector. See Chris Ingels NPR Interview, supra note 56. As discussed in NSIP, supra note 1, at § 165, Ken Wainstein, the former Assistant Attorney General for National Security, explained the importance of those relationships: “we rely on the communications providers to do our intelligence surveillances . . . . And there’s cooperation and there’s cooperation . . . . Yes, we can compel the phone companies, or compel the communications providers to do a surveillance, and even if they . . . resist a directive . . . we can go the FISA Court to get our orders enforced. Problem is, throughout that time, we’re stuck on whatever surveillance it is that we want to use on.” American Bar Association, Breakdown Proposed on FISA Reform (March 3, 2008), available at http://www.americanbar.org/natsec/jury/ multimedia/FISA_reform_panel_March_3_2008_WS_30144.mp3.

187. Another option would be to expand the court, although it is already a relatively large court, especially considering that its members sit part time and are geographically dispersed. See NSIP, supra note 1, at 5-3.

188. Testimony of Judge James G. Curi before the Senate Judiciary Committee (July 31, 2013) (discussing how Chief Judge Martin forwarded his name to the Administrative Office of the U.S. Courts, which led to his appointment to the FISC by the Chief Justice), available at http://www.judiciary.senate.gov/hearings-testimony.cfm?lid=0493953/18989773040106531641dec8w1&id=0493953 18989773040106531641dec8w1 (last visited June 24, 2014). See also Review Group Report, supra note 113.

189. Letter from Judge John Bates to Senator Diane Feinstein (Jan. 13, 2014) (hereinafter January 2014 Bates Letter), available at http://www.fas.org/sgp/wgwoi/2014/jan13bates.pdf. The letter contains an 14-page Appendix to the letter, dated January 10, 2014, and describes itself as “setting forth the Judge’s comments concerning certain potential changes to FISA and proceedings before the FISC and the Foreign Intelligence Surveillance Court of Review.” It explains that “[t]raditionally, the view of the Judiciary on legislative matters are expressed through the Judicial Conference of the United States, for which I serve as secretary. However, because the matters at issue here relate to special expertise and experience of only a small number of judges on two specialized courts, the Conference has not at this time been engaged to deliberate on them.” In preparing the letter, Judge Bates, himself a former Presiding Judge of the FISC, “consulted with the current Presiding Judges of the FISC and the Court of Review, as well as with other judges who serve or have served on those courts.” Id. at 1.
the person who normally assigns other judges to serve "on special courts." Such a strongly-worded letter from the Judicial Branch, on matters other than the budget of the federal courts, is quite notable, not only because it apparently reflects the views of the Chief Justice, but also because of the excellent reputation that Judge Bates enjoys.

2. As to the second proposal, concerning a civil liberties advocate in the FISC, the issue is more complex. There are at least three possible views of such an advocate, each with various costs and benefits, and other possibilities could also be considered. Most of the sensible possibilities are fundamentally designed to provide a counter-weight to the government's advocacy in a very small number of important cases, at the discretion of the FISC judges.

First, the FISC could call on external lawyers, in private practice, on a case-by-case basis as desired in the court's discretion. As noted above, such external advocacy would be needed very rarely, but would be potentially valuable where it is needed. Apart from the discretion of the FISC itself, which would properly control whether an advocate should be appointed, one possible guideline could be FISC Rule 11(b), which requires the government to submit a special memorandum when it presents a new issue to the court, including but not limited to "novel issues of technology or law." Such an approach might assist the FISC, and increase public confidence in its rulings.

However, the use of ad hoc external advocates might also be challenging, especially in the FISC as opposed to the Court of Review. At the outset, it might require a more robust form of adversary system than is commonly understood. One of the main challenges in some cases before the FISC is the intersection of complex law and complex facts, particularly concerning rapidly evolving technology, as Rule 11 itself recognizes. An adversary system, therefore, might require a developed approach for cross-examination or deposition of NSA engineers, and perhaps other methods of factual education, in support of an opposing brief written by advocates with very limited, episodic understanding of the technology in question. With respect to non-technological facts – e.g., concerning a potential target – the process for education might also be challenging, although in different ways. As former FISC President Judge Bates put it, "an advocate would not be able to conduct an independent factual investigation, e.g., by interviewing the target or the target's associates," and often "would impair rather than improve the FISC's ability to receive information and rule on applications in an effective and timely manner."

Moreover, these advocates also would not be aware of the FISC's jurisprudence on an ongoing basis, so the time needed for them to come up to speed might be significant. Finally, they would need special arrangements for writing and storing highly classified pleadings. All of these issues could be addressed, perhaps, but the process may be more involved, cumbersome, logistically challenging, and perhaps slower than is commonly understood. If it were used very rarely, and when time is not of the essence, it might be made to work, but it would not be a trivial undertaking.

Another option would be to use full-time, executive branch personnel to present the opposing arguments, such as staff in the National Security Division's Oversight Section. This has the virtue of using lawyers with ongoing experience, but also has its own disadvantages.
issues noted above. One concern, of course, would be that such an approach would give the opposing lawyers an advantage, through their informal interactions with the FISC judges, but this would probably be manageable. Approaching the issue from the other direction, as long as the role of the “red team” was properly defined and supported by the judges, there would be little risk of the designated Legal Advisors becoming “captured” and not vigorously opposing the government’s submissions.

This third approach has one additional feature, which is at least arguably a significant virtue, but which may not be widely understood: it maintains, at least formally, the ex parte nature of the FISC’s regular docket, even if it supplies an opponent to the government from within the court itself on the rare occasions when opposition is needed. Historically, the Department of Justice has taken very seriously the special obligations of candor that flow from the ex parte relationship with the FISA Court, and the institutional and long-term value of balanced, sober presentation. In some cases, indeed, the Department has been very strongly criticized for that approach, and for not being enough of an advocate. Creating a full-blown inter partes system in the FISC for a few key

information (e.g., a novel use of technology or a request to use a new surveillance technique) . . . . Court legal staff may not meet with the government as often as 2-3 times a week, or as few as 1-2 times a month.

209. Cf., e.g., ABA Model Rule 3.6(b) (“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 a reasoned decision, whether or not the facts are adverse.”) As the comment to ABA Model Rule 3.3 explains: 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 affirming 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.

Id. In his January 2014 letter to Congress, Judge Bates explained that “the government routinely discloses in an application information that is detrimental to its case,” January 2014 Bates Letter, supra note 189, at 5, and that “the current process benefits from the government’s taking on — and generally abiding by — a heightened duty of candor to the Court,” id. at 7.

210. See NSIP, supra note 1, at §§ 135 & 22; see also, e.g., 148 Cong. Rec. S6491-01 (reprinting article from The Washington Post, Dan Eggen and Susan Schmidt, Secret Court Rebuffs Adorff (Aug. 23, 2002)) ("FBI and Justice Department officials have said that the fear of being rejected by the FISA court . . . has at times caused both FBI and Justice officials to take a cautious approach to intelligence warrants. Until the current dispute, the FISA court had approved all but one application sought by the government since the court’s inception. Civil libertarians claim that record shows that the court is a rubber stamp for the government; proponents of stronger law enforcement say the record reveals a timid bureaucracy only willing to seek warrants on sure winners."); cf. 20 U.S.C. § 1804(d). As Carrie Cordero, formerly of the National Security Division at DOJ, testified before the Senate Judiciary Committee in October 2013:

On that point, it is worth noting that the FISA process, for approximately the preceding fifteen years, was applied to the exact opposite criteria that it seems to be today. The Department of Justice was accused of being too retilent, too cautious, too unwilling to be
cases might have some benefits, as discussed above, but could also result in the erosion of something that has proven valuable over time. The "red team" proposal is most likely to leave that cultural value intact, while still providing the court with the benefits of well-presented opposing viewpoints.

One of the main disadvantages of the red-team proposal—albeit at a political matter—is that it may not be, or appear to be, a sufficiently dramatic change from current practice. A variant on the approach designed to satisfy that concern would involve establishment of something like an Office of Defender of Civil Liberties (ODCL). As a formal matter, ODCL could operate as an arm of the FISC, by rough analogy to the Offices of the Federal Public Defender (FPD), which defend persons charged with federal crimes, and operate formally as arms of the various U.S. District Courts under the courts' plans for providing legal services to the indigent. Unlike FPD attorneys, however, the ODCL lawyers would likely not be busy defending civil liberties all of the time.
assistance to the Courts and minimizes disruption to their work. An advocate appointed at the discretion of the Court is likely to be helpful, whereas a standing advocate with independent authority to intervene at will could actually be counterproductive. 215

On January 17, 2014, in a speech delivered at the Department of Justice, President Obama appeared to agree with the approach preferred by the judiciary. He said: “To ensure that the court hears a broader range of privacy perspectives, I am also calling on Congress to authorize the establishment of a panel of advocates from outside government to provide an independent voice in significant cases before the Foreign Intelligence Surveillance Court.” 216 This brief statement contains three important elements. First, by referring to a panel of experts from “outside government,” the President seemed to be endorsing the first approach described above, in which the FISC calls on advocates from private practice, and rejecting the idea of a permanent ODCL or Public Advocate. Second, by referring to “significant cases,” the President seemed to recognize that participation of the outside advocates would be limited. Although he did not say who would determine which cases are “significant” enough to merit such participation, or the criteria used to determine “significance,” the likeliest approach seems to be to rely on the judges of the FISC. This was perhaps the most notable aspect of his statement: it did not call for mandatory participation by an outside advocate. Finally, however, by calling on Congress to authorize the panel of advocates, the President obviously left open the possibility that another approach might prevail. 217

SECRECY, TRANSPARENCY, AND THE SCOPE OF SIGNALS INTELLIGENCE

Apart from their impact on the FISC and its operations, the June 2013 disclosures and ensuing reaction also illustrate the tensions, and the ongoing need to calibrate, between the sometimes-competing values of secrecy and transparency. This tension exists both (1) within the federal government, and (2) between the federal government as a whole and the American people. 218 As to the first part of this issue, the historical record shows that the Executive Branch met its legal disclosure obligations to Congress. As to the second part, however, concerning disclosure to the public, it is clear that the American People did not understand that the bulk metadata collection was occurring or appreciate the legal interpretation that underlies it. Such a lack of understanding is, of course, the general rule with respect to classified intelligence activity; but the reaction to the June 2013 disclosures, and a particular focus on the perils of “secret law,” suggests that that rule may be subject to change, potentially with profound consequences.

1. The standards governing information-sharing between the Executive Branch and Congress in this area are clear, as discussed in Chapter 13 of NSIP. Under FISA, the Intelligence Committees, and in some cases the Judiciary Committees – but not the rest of Congress – are to be kept “fully informed” of most intelligence activities, including significant interpretations of FISA. 219 Of particular relevance here, FISA provides that on an annual basis, “the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate of all intelligence activities.” 220 That “fully informed” obligation does not extend to Congress as a whole, or to any Member outside the specified committees.

2. In 2004 and 2008, Congress directly addressed the issue of “secret law” by amending FISA to provide specifically for briefings, and submission of documents, on all significant interpretations of FISA. Again, however, Congress provided that the briefings and documents would be provided only to the Intelligence and Judiciary Committees, not the rest of Congress:

On a semiannual basis, the Attorney General shall submit to the Permanent Select Committee on Intelligence of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Senate, in a manner consistent with the protection of the national security…a summary of significant legal interpretations of this chapter involving matters before the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review, including interpretations presented in applications or pleadings filed with the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review by the Department of Justice; and…copies of all decisions, orders, or opinions of the Foreign Intelligence Surveillance

http://www.justice.gov/olopo/resource/2202001771216284;196693.pdf. Historians may also seek to view the disclosures against the backdrop of public assessments the nature of the threat posed by international terrorism, and the armed conflict with al Qaeda and its affiliates, a dozen years after 9/11.

219. See, e.g., 50 U.S.C. §§ 1801(a)(1) (electronic surveillance), 1826 (physical searches), 1846(a) (post/trap surveillance), 1862(a) (tangible things), 1881f (FISA Amendments Act).

These legal standards reflect long-standing traditions governing disclosures owed to Congress by the Executive Branch in the area of intelligence. They represent the fundamental balancing of secrecy and transparency between the two political branches, and the essential idea behind creation of the Intelligence Committees. In 1976 and 1977, as discussed in §§ 2.6-2.7 of NSP, recent times have witnessed an increasing effort by the Judiciary Committees to become involved in classified matters regulated by law, but the balance remains still stuck in favor of mandatory disclosure to the (two or four) committees, and against general disclosure of highly classified information to Congress as a whole.221

a. The record shows that the government met its disclosure obligations to Congress. Senators Diane Feinstein and Saxby Chambliss, Chair and Vice Chair of the Senate Intelligence Committee, responded to the June 2013 FISA Court order by observing, as Senator Feinstein put it, that “this is the exact three-month renewal of what has been the case for the past seven years. This renewal is carried out by the court under the business records section of the Patriot Act. Therefore, it is lawful. It has been briefed to Congress.”222 The two senators also issued a written statement on the Committee’s website explaining that “[t]he executive branch’s use of this authority has been briefed extensively to the Senate and House Intelligence and Judiciary Committees, and detailed information has been made available to all members of Congress prior to each congressional reauthorization of this law.”223

221. 50 U.S.C. § 1871(a). The Senate Intelligence Committee’s report on its activities from January 2009 to January 2011 noted that the “Committee utilized reporting required under provisions in FISA and the USA PATRIOT Act Improvement and Reauthorization Act, including the annual and semiannual reports from the Director of National Intelligence, the DNI, and relevant reports from the Attorney General, the DNI, and relevant agencies, including from being able to review decisions, orders, and opinions, as well as the related pleadings, applications, and memoranda of law, that include “significant construction or interpretation of any provision of FISA that are required to be submitted to the oversight committees under 50 U.S.C. 1871(c),” S. Rep. No. 112-3, at 31 (Mar. 17, 2011) [hereinafter SSCI March 2011 Activities Report]. The report explained that “[t]hese documents were routinely the subject of subsequent briefings by officials of the Department of Justice and the Intelligence Community, in Committee spaces and at the relevant agencies.” Id. at 31.


224. Press Release, Senate Select Committee on Intelligence, Feinstein, Chambliss Statement on NSA Phone Records Program (June 6, 2013) [emphasis added], available at http://www.intelligence.senate.gov/press/record.cfm?id=343993. Given that history, objections to the activity from civil libertarians tended to reflect a basic disagreement with the policy judgments reached and maintained over the preceding seven years by the Executive, Legislative, and Judicial Branches. As Anthony Romero, the head of the American Civil Liberties Union put it: “A pox on all the three houses of government.”

Similarly, Representatives Mike Rogers and Dutch Ruppersberger, the Chair and Ranking Member of the House Intelligence Committee, released a statement the day after the FISA Court order was published saying that the collection described in the order is consistent with the Foreign Intelligence Surveillance Act (FISA) as passed by Congress, executed by the Executive Branch, and approved by a Federal Court. The FISA business records authorities are used to track foreign intelligence threats and international terrorists. It is important that the American people understand that this information does not include the content of anyone’s conversations and does not reveal any individual or organization names. This important collection tool does not allow the government to eavesdrop on the phone calls of the American people. When these authorities are used, they are governed by court-approved processes and procedures. Moreover, the use of these authorities is reviewed and approved by federal judges every 90 days. Additionally, the Committee reviewed all FISA activities. Importantly, these activities have led to the successful detection and disruption of at least one terrorist plot on American soil, possibly saving American lives. Understanding the necessity of the public’s trust in our intelligence activities and out of an abundance of caution, the Committee will review this matter to ensure that it too complies with the laws established to protect the American people.225

Between June 2008 and June 2012, the Senate Intelligence Committee “received and scrutinized unredacted copies of every classified opinion of the Foreign Intelligence Surveillance Court (FISA Court) containing a significant construction or interpretation of the law, as well as the pleadings submitted by the Executive Branch to the FISA Court relating to such opinions.”226 It also reprinted without rebuttal the government’s statement that it had complied with the Court’s order to produce the interpretive documents.

The Department of Justice wrote a letter to Congress in July 2013 confirming
that "[t]he classified details of the program have been briefed to the Judiciary and Intelligence Committees on many occasions." 228 Also in July 2013, the DNI wrote to Senator Ron Wyden that "as Congress required, the Executive Branch fully and repeatedly briefed the Intelligence and Judiciary Committees of both Houses about the program and timely provided copies of the relevant classified documents to the Committees." 229 In its August 2013 White Paper, the government explained that

In early 2007, the Department of Justice began providing all significant FISC pleadings and orders related to the bulk telephony metadata collection program to the Senate and House Intelligence and Judiciary Committees. By December 2008, all four committees had received the initial application and primary order authorizing the telephony metadata collection. Thereafter, all pleadings and orders reflecting significant legal developments regarding the program were produced to all four committees. 230

In the fall of 2009, at least three Members of the House Judiciary Committee, including then-Chairman John Conyers and Representative Jerrold Nadler, separately engaged in explicit, classified correspondence with the Department of Justice concerning the bulk telephony metadata collection program. There is no question, based on this correspondence, that they were aware of the collection under FISA’s tangible-things provision (as well as a program of bulk internet metadata collection under FISA’s pen-trap provisions). 231 In May 2011, Representative Lamar Smith, then Chairman of the House Judiciary Committee, stated:

During the last 3 months, the House Judiciary Committee has thoroughly reviewed the Patriot Act and how its provisions are used in national security investigations. The Crime Subcommittee has held three hearings specifically on the Patriot Act, the full committee held oversight hearings of the FBI and the Department of Justice, and all committee members were provided a classified briefing by the Administration. . . . The business records provision allows the FBI to access third party business records in foreign intelligence, international terrorism, and espionage cases. Again, this provision requires the approval of a Federal judge. That means the FBI must prove to a Federal judge that the documents are needed as part of a legitimate national security investigation. [This provision has] been effectively used for the last 10 years without any evidence of misuse or abuse. . . .

On July 17, 2013, in a hearing of the House Judiciary Committee, there was no rebuttal from any Member when Bob Litt, General Counsel of ODNI, stated that the interpretive documents had been provided to the Committee, or when James Cole, the Deputy Attorney General, later made the same assertion. 233 Chris Inglis, Deputy Director of the NSA, testified in the July 17, 2013 hearing without challenge that "[w]e also offered classified briefings to members of this committee. And I recall participating in one of those briefings." 234

On March 5, 2009, and again on September 3, 2009, the Department of Justice sent to the Intelligence and Judiciary Committees a series of classified documents pertaining to compliance issues that had arisen in connection with the bulk telephony metadata collection. The September cover letter accompanying those documents explained that "these documents were described, in pertinent part, in briefings provided to the House and Senate Intelligence and Judiciary Committees in March, April, and August 2009." 235

The Senate Judiciary Committee was sufficiently aware of the bulk metadata collection that it included language in two of its reports designed to ensure continuation of the collection. When the Committee considered amendments to the tangible-things provision in 2009 and 2011 (the amendments ultimately were not enacted), it was careful in doing so not to avoid any suggestion that those amendments would undermine the bulk collection program, explaining in Committee reports that the proposed changes to the tangible things provision were "not intended to affect or restrict any activities approved by the FISA court under existing statutory authorities." 236

235. Letter from the U.S. Department of Justice to Congressional Intelligence and Judiciary Committees (Sept. 3, 2009) (emphasis added). The letters are available at http://congressionalrecord.tumblr.com/. The documents themselves, which are also publicly available on the same Intelligence Community website as the letters, are described as "several Foreign Intelligence Surveillance Court opinions and Government filings relating to the Government’s discovery and remediation of compliance incidents in its handling of bulk telephony metadata under docket number BR 08-13;" and "the Government’s report to the Court and NSA’s end-to-end review describing its investigation and remediation of compliance incidents in its handling of bulk telephony metadata under docket number BR-09-09." See IC On the Record, http://congressionalrecord.tumblr.com/; For a summary of the nature of the compliance incidents, see note 67.
236. The Senate Judiciary Committee’s reports on 5 1/6, 2009, the USA Patriot Act Sunset Extension Act of 2009, S. Rep. No. 111-92, at 7 (Oct. 28, 2009), and S. 193, the USA Patriot Act Sunset Extension Act of 2011, S. Rep. No. 112-13, at 10 (Apr. 5, 2011), discuss certain proposed minor amendments to the requirements for a tangible-things application. The 2009 report explains that "[t]he changes are not intended to affect or restrict any activities approved by the FISA court under existing statutory authorities," and the 2011 report explains that "[t]he language in the bill does not raise the standard for obtaining an order and is not intended to affect or restrict any activities approved by the FISA Court under existing statutory authorities." Nearly identical language also appears on page 23 of the 2011 report; see also page 29 of the 2009 report. The 2011 report also includes a letter from the Justice Department to the Chairman of the Senate Judiciary Committee dated September 14, 2009, and a similar letter to the Speaker of the House and Majority Leader of the Senate dated February 19, 2010, both stating that some tangible-things orders were "used to support important and highly sensitive intelligence collection operations" of which Members of the Intelligence Committees and their staff
b. Apart from briefings for, and documents submitted to, the four designated committees, the record shows that classified briefings were offered to all Members of Congress. On July 31, 2013, the DNI declassified and released letters and redacted briefing papers provided to the House and Senate Intelligence Committees in December 2009 and February 2011. The letters explained that "making this document [the 2011 briefing paper] available to all Members of Congress, as we did with a similar document in December 2009, is an effect of wanting to inform the legislative debate about reauthorization of Section 215 of the Patriot Act. 237 The letters also stated that "Executive Branch officials will be available nearby [to the Intelligence Committees' SCIFs] during certain, pre-established times to answer questions should they arise."

The classified briefing papers themselves, which are written in relatively plain language and are five pages long, explained that the FISC’s “orders generally require production of the business records … related to substantially all of the telephone calls handled by the [telephone] companies,” including “both calls made between the United States and a foreign country and calls made entirely within the United States.” 239 The briefing papers described the program explicitly as involving “bulk” collection, and stated that it “operate[s] on a very large scale,” even though “only a tiny fraction of [the collected] records are ever viewed by NSA intelligence analysts.” 240 The briefing papers also described “a number of technical compliance problems and human implementation errors” that were discovered beginning in 2009 “as a result of Department of Justice (DOJ) reviews and internal NSA oversight.” But noted that neither the government nor the FISC “found any intentional or bad-faith violations.”

The availability of the classified briefings and documents was publicized within Congress. Senators Feinstein and Chambliss wrote two “Dear Colleague” letters, in 2010 and 2011, inviting all Members of Congress to classified briefings on the bulk collection, 242 and statements in the Congressional Record show that they offered briefings to Members during debates over reauthorization of the Patriot Act. For example, in 2011, Senator Feinstein made the following floor statement:

The third authority covered by this [proposed] legislation [to reauthorize the Patriot Act] is known as the business records provision and provides the government the same authority in national security investigations to obtain physical records that exist in an ordinary criminal case through a grand jury subpoena. … some business records orders have been used to support critically important and highly sensitive intelligence collection activities. The House and Senate Intelligence Committees have been fully briefed on that collection. Information about this sensitive collection has also been provided to the House and Senate Judiciary Committees, and information has been available for months to all Senators for their review. The details on how the government uses all of these authorities are classified and discussion of them here would harm our ability to identify and stop terrorist attacks and espionage. But, if any Senators would like further details, I encourage them to contact the Intelligence Committee, or to request a briefing from the Intelligence Community or the Department of Justice. 243

Similarly, Rep. Hastings, a Member of the House Intelligence Committee, stated in February 2010:

Mr. Speaker, I rise to inform Members that the Intelligence Committee has received a classified document from the Department of Justice that is related to the PATRIOT Act authorities currently set to expire at the end of the month. The House may consider a 1-year extension of the PATRIOT Act today so the Intelligence Committee will be making this document available for Member review in the committee offices located in HVC 304. Staff from the Intelligence and Judiciary Committees, as well as personnel from the Justice Department and with the Office of the Director of National Intelligence, will be available to answer any questions that Members may have. Members who want to review the document should call the Intelligence Committee to schedule an appointment. 244

Senator Wyden (a Member of the Intelligence Committee) also cited the availability of a briefing document and encouraged his colleagues to read it, noting that “the Attorney General and the Director of National Intelligence have prepared a classified paper that contains details about how some of the Patriot


239. 2011 Briefing Documents, supra note 27, Cover Letter at 2.

240. Id. at 1, 3. The publicly released version of the briefing paper redacts more than four lines of text immediately following the statement that the program operates on a "very large scale" and immediately before the statement that analysts only view "a tiny fraction of such records." It therefore appears that the redacted information provides more detail about the precise scope and scale of the collection.

241. Id. at 4.

242. The "Dear Colleague" letters, dated February 2010 and February 2011, offered Members of Congress the opportunity to review documents related to the collection, and included an offer to meet with DOJ and Intelligence Community personnel. The letters are available at http://big.assets.huffingtonpost.com/Site3/CommitteeIntelligenceFeb13.pdf.


Act’s authorities have actually been used, and this paper is now available to all members of Congress, who can read it in the Intelligence Committee’s secure office spaces. He went on to observe that “[p]roviding this classified paper to Congress is a good first step, and I would certainly encourage all of my colleagues to come down to the Intelligence Committee and read it,” although he also strongly urged release of the information to the general public. The Department of Justice also informed the Chairman and other Members of the House Judiciary Committee of its plan to make the information available.

In an unclassified report published in March 2011, the Senate Intelligence Committee emphasized that it had offered a briefing to all Members of Congress concerning the bulk telephony metadata collection:

Prior to the extension of the expiring FISA provisions in February 2010, the Committee acted to bring to the attention of the entire membership of the Senate important information related to the nature and significance of the FISA collection authority subject to sunset. Chairman Feinstein and Vice Chairman Bond notified their colleagues that the Attorney General and the DNI had provided a classified paper on intelligence collection made possible under the Act and that the Committee was providing a secure setting where this classified paper could be reviewed by any Senator prior to the vote on passage of what became Public Law 111-141 to extend FISA sunsets.

The Attorney General and/or the DNI had themselves offered such briefings in writing as early as 2009, as described in an unclassified letter sent by both officials to the Majority Leader of the Senate and the Speaker of the House on February 19, 2010:

As we previously noted in a September 14 [2009] letter from the Department of Justice to Senator Patrick Leahy, the business records authority of FISA has been used to support important and highly sensitive intelligence collection operations, of which both Senate and House leadership, as well as Members of the Intelligence and Judiciary Committees and their staffs are aware. We can provide additional information to Members concerning these and related operations in a classified setting.

In 2013, the White House released to members of the news media a list of 13 classified briefings, for members of the Intelligence and Judiciary Committees, Congressional Leadership, the House Democratic Caucus, and others, conducted between 2009 and 2011, on the tangible things provision. It is not clear whether the list is complete, or whether some briefings were intentionally or accidentally omitted (the list appears to omit the briefings conducted in March, April and August 2009, discussed above). The list of briefings, as published in Politico, was as follows:

- Sept. 22, 2009: HJC Hearing USA Patriot Act (Unclassified) DOJ NSD Deputy Todd Hinnen
- Sept. 23, 2009: SJC Hearing Reauthorizing the Patriot Act, Kris
- Nov. 29, 2010: Leadership Meeting House and Senate Leadership Staff (Classified)
- Feb. 14, 2011: Senate All Senators were offered the opportunity discuss Sec. 215 of the Patriot Act in the VPOTUS office off of Senate Floor, Director of National Intelligence James Clapper, FBI Director Robert Mueller, Alexander
- Feb. 28, 2011: SJC/SSCI Briefing Patriot Act reauthorization (Classified)
- Feb. 28, 2011: HJC Briefing Patriot Act reauthorization (Classified)
- March 9, 2011: HJC Hearing Patriot Act reauthorization (Unclassified), Hinnen
- March 15, 2011: Meeting Durbin Patriot Act amendment (Classified)
- March 17, 2011: HPSCI Hearing Patriot Act reauthorization, Hinnen, FBI’s Sean Joyce, Alexander
- March 30, 2011: HJC Hearing Patriot Act Reauthorization (Unclassified), Hinnen

In July 2013, the DNI wrote to Senator Wyden that “the Executive Branch undertook special efforts to ensure that all Members of Congress had access to information regarding this classified program prior to the USA PATRIOT Act’s reauthorization in 2011, including making a detailed classified white paper

---

248. SSCI March 2011 Activities Report, supra note 221, at 31 (emphasis added).
available to all Members."^{251} The DNI's letter went on to explain that "in December 2009, the Department of Justice and Intelligence Community provided a classified briefing paper to the Senate and House Intelligence Committees that could be made available to all Members of Congress regarding the telephony metadata program. Both Intelligence Committees made this document available to all Members prior to the February 2010 reauthorization of Section 215. That briefing paper was then updated and provided to the Senate and House Intelligence Committees again in February 2011 for all Members in connection with the reauthorization that occurred later that year."^{252}

Many Members of Congress acknowledged having been briefed, or at least having had the opportunity to be briefed, on the bulk collection program. For example, the Senate Majority Leader, Harry Reid, said: "For senators to complain that 'I didn't know this was happening,' we've had many, many meetings that have been both classified and unclassified that members have been invited to. If they don't come and take advantage of this, I can't say enough to say they shouldn't come and say 'I wasn't aware of this,' because they've had every opportunity to be aware of these programs."^{253} Senator Leahy acknowledged receiving classified briefings. Even Senators Wyden and Udall, perhaps the most outspoken Congressional critics of the program, conceded in March 2012 that the existence of the program, and underlying legal interpretation, "has been acknowledged on multiple occasions by the Justice Department and other executive branch officials," and noted that the Executive Branch had, "to its credit, provided this information in documents submitted to Congress."^{254}

252. Id. at 1. See also White Paper, supra note 27 at 11-13. Although the House Intelligence Committee did notify Members of the House of the classified documents and briefings in 2010 (when it was led by Chairman Silvestre Reyes), it may not have done so in 2011, when it was led by Chairman Mike Rogers. See White Paper, supra note 27, at 11-13. US EURC BIO, supra note 153, at 14-15 (referring only to the 2010 documents). In the summer of 2013, the House Intelligence Committee denied requests from certain Members of the House to view certain classified materials concerning FISA. See Glenn Greenwald, Members of Congress Denied Access to Basic Information About FISA, The Guardian (Aug. 4, 2013), http://www.theguardian.com/commentisfree/2013/aug/04/congress-madened-access; see also Josh Gersten, House panel nixes Grayson's Request for Syria Intelligence, POLITICO (Oct. 18, 2013), http://www.politico.com/blogs/under-the-radar/2013/10/house-panel-nixes-graysons-request-for-syria-intelligence-175396.html?hp=c2. The Rules of the House Intelligence Committee set out a detailed procedure under which Members of Congress who do not serve on the Committee may gain access to classified information. Under Rule 146(b), the Committee considers written requests for access by non-Members using at least the following criteria:

(A) The sensitivity to the national defense or the confidential conduct of the foreign relations of the United States of the information sought;

(B) The likelihood of its being directly or indirectly disclosed;

(C) The jurisdictional interest of the member making the request; and

(D) Such other concerns, constitutional or otherwise, as may affect the public interest of the United States.

The Rules also contain detailed provisions under which the Committee can, on its own initiative, bring matters to the full House. See Rules of Procedure for the House Permanent Select Committee on Intelligence, 113th Cong., available at http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/HPSCI/2013/20130207Rules%20of%20the%20House%20of%20Representatives.pdf. The Senate Intelligence Committee has similar rules. See Rules of Procedure for the Select Senate Committee on Intelligence, United States Senate, Rules 9-5, 9-9, available at http://www.intelligence.senate.gov/pdfs/113th/sap1137.pdf. Regardless of any intra-congressional issues in 2011, as a matter of inter-branch relations, it is clear that the Executive Branch provided the materials with the intent that they be made available to all Members of Congress, as they had been in 2009.

253. See, e.g., June 2013 Open HPSCI Hearing. Statement of Chairman Mike Rogers ("The committee has been extensively briefed on these efforts over [sic] a regular basis as part of our ongoing oversight responsibility ... the collection efforts under the business records provision [and] in Section 702 of the Foreign Intelligence Surveillance Act are legal, court-approved and subject to an extensive oversight regime."); Statement of Ranking Member Dutch Ruppersberger ("I reiterated a lot of what the Chairman has said ... We need to work with these authorities are legal. Congress approved and reauthorized both of them over the last two years.").
Although at least one member of the House Judiciary Committee publicly stated that he intentionally eschews classified briefings—on the ground that they are a “rope-a-dope operation”—none appears credibly to have denied the fact that briefings occurred or that the relevant interpretive documents were delivered.

Testified before the Senate Judiciary Committee in 2009 that the tangible-things provision was “morally analogous to the authority available to FBI agents investigating criminal matters through the use of grand jury subpoenas, and also stated that “[s]o many Members are aware, some of these (Section 215) orders were used to support important and highly sensitive intelligence collections. The Department can provide additional information to Members or their staff in a classified setting.” Testimony of David Kris, Assistant Attorney General, before the Senate Judiciary Committee (Sept. 23, 2009), available at http://www.justice.gov/jsc/hearings/11-1/2009-09-23-donald-kris-patent-ac.pdf. See also Peter Wallsten, Lawmakers Say Administration’s Lack of Candor on Surveillance Weakens Oversight, Wash. Post, July 10, 2013, available at http://www.washingtonpost.com/politics/lawmakers-say-administrations-lack-of-candor-on-surveillance-weakens-oversight/2013/07/10/b2756d6e-8e7a-11e2-aaf4-c072e2e342-story.html.

Representative James Sensenbrenner was quoted in the Washington Post as follows: Sensenbrenner, who had access to multiple classified briefings as a member of the Judiciary Committee, said he does not typically attend such sessions. He called the practice of classified briefings a “rope-a-dope operation” in which lawmakers are given information and then forbidden from speaking about it. Members are not permitted to discuss information disclosed in classified briefings. “It’s the same old game they use to suck members in,” he said.

Id. Representative Sensenbrenner did not explain how or why he expected to receive a classified briefing and also be authorized to discuss that briefing publicly.

One notable example of a Member of Congress who denied knowledge of the bulk collection was Representative Sensenbrenner, who wrote a letter to the Attorney General on June 6, 2013, explaining that he had “closely monitored and relied on testimony from the Administration about how the [Patent Act] was being interpreted to ensure that abuses had not occurred,” and had been “left with the impression that the Administration was using the business records provision sparingly, and for specific materials,” in contrast to the “recently released FISA order,” which “could not have been drafted more broadly.” Letter from Rep. James Sensenbrenner to Attorney General Eric Holder (June 6, 2013), available at http://sensenbrenner.house.gov/uploadedfiles/sensenbrenner_letter_to_attorney_generaleric_holder.pdf.

As evidence that he had not been properly informed, Representative Sensenbrenner cited in his letter the testimony of a DOJ official, as follows, with the ellipsis included in the letter:

Section 215 has been used to obtain driver’s license records, hotel records, car rental records, apartmentleasing records, credit card records, and the like. It has never been used against a library to obtain circulation records... On average we seek and obtain section 215 orders less than 40 times per year.

This description of the government’s use of the tangible things provision, Representative Sensenbrenner asserted, did not adequately advise the Committee of the classified bulk collection program.

Unfortunately for Representative Sensenbrenner, the ellipsis in his letter replaced the following sentence from the DOJ official’s testimony:

Some orders have also been used to support important and highly sensitive intelligence collection operations, and others that are in this committee and others that have been separately briefed.

Such a highly classified briefing for all Members of Congress, rather than just for those serving on the Intelligence Committees (and perhaps also the Judiciary Committees), is very unusual. It is understandable that the Executive Branch wanted to brief all Members of Congress “as an effective way to inform the legislative debate about reauthorization of Section 215” of the Patriot Act. But the briefings were, without question, a departure from the legal requirements and cultural and historical norms in this area. As Senator Feinstein stated in July 2013, referring to the bulk telephony metadata collection program, “Balancing privacy rights with our nation’s security is difficult to achieve, but I know of no federal program for which audits, congressional oversight and scrutiny by the Justice Department, the intelligence community and the courts are stronger or more sustained.”

The briefings and other historical evidence raise the question whether Congress was aware of the full scope of the telephony metadata collection program when he voted to reauthorize section 215 and that “he had been fully informed that he would not have voted to reauthorize section 215 without change.” Br. of Amicus Curiae of J. John Bolton, supra note 12, at 9–10 (ECP No. 56). This is a curious statement: Congressmen Sensenbrenner not only had access to the five-page report made available to all Congressmen, but he also, as a “long-serving member of the House Judiciary Committee,” was a member of the independent Executive Branch that included “a summary of significant legal interpretations of section 215 involving matters before the FISA” and “copies of all decisions, orders, or opinions of the FISC that include significant construction or interpretation of section 215.” 50 U.S.C. § 1871. ACLU Opinion, supra note 113, at *16.

Another Member of Congress who complained of being misled was Rep. Jerrold Nadler, also of the House Judiciary Committee. In a Washington Post story published in July 2013, Rep. Nadler was quoted as saying, “The national security story has grown so that any administration now is not up to date, incorrect, and that it is an imbalance that is going on in our government, and one that we have to correct.” The article also quoted Rep. Nadler as follows: “I don’t know if it was an oversight, but it was certainly misleading to what was going on,” said Nadler, who was a member of the committee that heard from Hoenen in 2009.” Peter Wallsten, Lawmakers Say Administration’s Lack of Candor on Surveillance Weaks Oversight, Wash. Post Digital (July 10, 2013), http://www.washingtonpost.com/ politics/lawmakers-say-administrations-lack-of-candor-on-surveillance-weaks-oversight/2013/07/10/8275dedb-4e9a-11e2-a09f-c03572de342_story.html. As it turns out, however, Rep. Nadler was in fact aware of the bulk metadata collection in 2009, and (as discussed in the text) wrote to the Department of Justice about the collection at that time. In response, DOJ sent him a letter in December 2009 noting that the government was making available to all Members of Congress information about the bulk collection and compliance issues that had arisen. Letter from Ronald Weich, Assistant Attorney General, to Rep. Jerrold Nadler (Dec. 17, 2009), available at http://www.doi.gov/files/documents/501/Letter%20to%20Weich%20Dec%202009.pdf. There is no question whatsoever, based on the letters exchanged with the Department of Justice, that Rep. Nadler was aware of the bulk metadata collection program in 2009.

For a more complete discussion of Congressional oversight of national security matters, see NSIP, supra note 1, at § 13.1 et seq.

260. 2011 Briefing Documents, supra note 27, Cover Letter at 1.


262. Lorillard v. Pons, 434 U.S. 575, 580 (1978); see also Kemen Corp. v. United States, 508 U.S. 202, 212–13 (1993). Cf. In re sealed Case, 310 F.3d 717, 725 (FISCR 2002) (“In short, even though we agree that the original FISA did not contemplate the ‘false dichotomy,’ the Patriot Act actually did—which makes it no longer false.”)

263. One possibility, discussed briefly at the June 2013 HPSCI hearing, and again at the July 2013 SJC hearing, would be to store data with providers, requiring them to keep it for 5 years, and then conduct emergency or court-authorized queries based on a showing of reasonable suspicion. Depending on the number of "boys" and perhaps other factors, however, this would be challenging unless the providers link and make common their databases; another possible approach could be to use a third party custodian for all participating providers’ data, even if the infrastructure for the data had to be supplied by NSA. Appropriate legislation, developed in coordination with the government and the providers, could support and require such an approach. See July 2013 SJC Hearing, supra note 27, Statement of Chris Inglis ("I think we can take a look at whether this is stored at the provider, so long as you have some confidence you can do this in a timely way"). See also Review Group Report, supra note 113, at 17 ("In our view, the current storage by the government of bulk meta-data creates potential risks to public trust, personal privacy, and civil liberty. We recognize that the government might need access to such meta-data, which should be held instead either by private providers or by a private third party.").

264. Such legislation might also have expressed Congressional intent, in line with the Steel Seizure case, that the President or executive agencies, in this area, as in the case of the Patriot Act, would not be able to implement the Executive Branch to rely on any inviolable Article II authority or to use grand juries or other extraneous statutory authorities. For a discussion of FISA’s “exclusivity provision” governing electronic surveillance, and the Steel Seizure case, Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952), see NSIP, supra note 1, at § 15.3.

265. It is extremely interesting to consider whether, under current law and the FISA Court’s orders interpreting it, the government’s theory of “relevance” would permit an approach in which the haystacks of metadata remain with the providers. As discussed in the text, the government’s theory is that it must collect the haystacks to find the needles representing terrorist communications, and that the haystacks are therefore relevant. Leaving the metadata with the telecommunications providers and simply running queries against it (directly or through the providers) would not necessarily accord with that theory. The providers might agree to voluntarily run queries (or otherwise permit to do so), and in that event the results of those queries might indeed establish relevance to collect the responsive records, but it is far from clear that FISA’s tangible things provision could be used to compel the providers to run the queries in the first place. This does not, of course, call into question Congress’s ability to enact new legislation that would compel providers to retain and query the data under certain conditions.

266. See Office of the Clerk of the U.S. House of Representatives-Final Vote Results for Roll Call 412, http://clerk.house.gov/evtserv/DV13041412.xml. The bill provided as follows:

None of the funds made available by this Act may be used to execute a Foreign Intelligence Surveillance Court order pursuant to section 501 of the Foreign Intelligence Surveillance Act
longer term, of course, a failure to enact legislation restricting or terminating the bulk metadata collection, and/or a reenactment of Section 215 of the Patriot Act without change or with changes that permit the program to continue, after the public debate that has occurred, would be extremely telling.)

Of course, it would be ridiculous to presume that Congress adopted a classified interpretation of a law of which it could not have been aware. As described above, however, the historical record shows that many Members were aware, and that all Members were offered briefings on the FISC’s interpretation, even if they did not attend the briefings. Even in an ordinary legislative setting, of course, many Members may not actually be aware of a prior judicial interpretation, but that has never been formally part of the doctrine. Here, post-disclosure briefings, conducted in July 2013, also drew sparse attendance, apparently to a degree that frustrated Senator Feinstein, who was quoted as saying, “It’s hard to get this story out. Even now we have this big briefing — we’ve got [NSA Director] Alexander, we’ve got the FISA Court, we’ve got the Justice Department, we have the FISA Court there, we have [DNI] Clapper there — and people [Members of Congress] are leaving.” Although the Supreme Court has never applied the presumption of Congressional awareness and adoption in this setting, the government would seem to have some arguments that it should

of 1978 (50 U.S.C. 1861) that does not include the following sentence: “This Order limits the collection of any tangible things (including telephone numbers dialed, telephone numbers of incoming calls, and the duration of calls) that may be authorized to be collected pursuant to this Order to those tangible things that pertain to a person who is the subject of an investigation described in section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861).”


266. Cf. William N. Eskridge, Jr., Interpreting Legislative Inaction, 87 Mich. L. Rev. 67, 81 (“While the Court in these cases often invokes the requirement rule without a specific showing that Congress was aware of the judicial interpretations, the Court usually makes an effort to demonstrate that the Court could have articulated the required statement.”). See also Klonoski v. Allen, 168, 185 n.21, 192-194 (1969) (With respect to the doctrine of legislative acquiescence, rather than reenactment, “the verdict of quiescent years cannot be invoked to baptize a stationary gloss that is otherwise impermissible. This Court has many times reconsidered statutory constructions that have been passively abided by Congress. Congressional inaction frequently betokens unconsciousness, preoccupation, or paralysis. It is at best treacherous to find in Congressional silence alone the adoption of a controlling rule of law. Its significance is greatest when the area is one of traditional year-by-year supervision, like tax, where watchdog committees are considering and revising the statutory scheme.” (internal quotation and citation omitted)).

267. According to The Hill, a briefing for Senators on June 13, 2013 attracted less than half of the Senate. Alexander Boiton, Senators Skip Classified Briefing on NSA Snooping to Catch Flights Home, THE HILL (June 15, 2013) (“Only 47 of 100 senators attended the 2:39 briefing, leaving dozens of chairs in the secure meeting room as [DNI] Clapper, [NSA Director] Alexander and other senior officials told lawmakers about classified programs to monitor millions of telephone calls and broad swaths of Internet activity. . . . The exodus of colleagues exacerbated Senate Intelligence Committee Chairwoman Diane Feinstein (D-Calif.), who spent a grueling week answering colleagues’ and media questions about the program. ‘It’s hard to get this story out. Even now we have this big briefing — we’ve got Alexander, we’ve got the FISA Court, we’ve got the Justice Department, we have the FISA Court there, we have Clapper there — and people are leaving.’”)). http://thehill.com/home/headlines/senate/305765-senATORS-skipped-classified-briefing-on-nsa-snooping-to-catch-flights-home.


269. POTUS Signat Speech, supra note 49.

270. August 2013 FISC Order, supra note 4, at 24. The court did not discuss the issue of the House Intelligence Committee’s possibly refusing to honor the Executive Branch’s request to provide information to all Members of the House in 2011, as discussed above.

271. ACLU Opinion, supra note 113, at *16.


273. Id. at 3.

274. 152 S. Ct. 945 (2013). See August 2013 FISC Opinion, supra note 4 at 3 n.4.

275. Judge McLoughlin stated: Justice Sotomayor stated in her concurring opinion in Jones that it may be necessary for the Supreme Court to “reconsider the premise that an individual has no reasonable expectation of be applied. On the other hand, there would be no serious argument that the FISC’s decisions established a “public” understanding of the tangible things provision before it was reauthorized, and that could undermine reliance on the doctrine. In his speech in January 2014, the President seemed to endorse the argument that Congress had been adequately briefed, observing that “the telephone bulk collection program was subject to oversight by the [FISC] and has been reauthorized repeatedly by Congress,” even though “it has never been subject to vigorous public debate.”

Evaluating these arguments in August 2013, the FISA Court concluded without difficulty that Congress had been sufficiently briefed, and so had incorporated the FISC’s interpretation in reauthorizing the law. The court explained: “Congress re-authorized Section 215 of the PATRIOT Act without change in 2011,” and was sufficiently aware of the FISC’s interpretation of the statute to satisfy the legal requirements for ratification through reenactment. In December 2013, a district judge in the Southern District of New York reached the same conclusion: “viewing all the circumstances presented here in the national security context, this Court finds that Congress ratified section 215 as interpreted by the Executive Branch and the FISC, when it reauthorized FISA.”

In October 2013, the FISC released an opinion again authorizing the bulk collection. This opinion, written by Judge Mary McLoughlin, was noteworthy in at least three respects. First, it explicitly endorsed the August 2013 opinion, including the ratification argument, which had been written by another FISC judge; but the October opinion stated that this was the “first time” that Judge McLoughlin herself had “entertained an application requesting the bulk collection of call detail records,” making clear that she was not locked in to a prior position. Second, unlike the August opinion, which had explicitly disclaimed any reliance on the government’s White Paper and (at least implicitly) publicly-available criticism of the White Paper and the FISC’s own prior rulings, including constitutional attacks based on the Supreme Court’s decision in U.S. v. Jones, the October opinion explicitly discussed Jones and concluded that it posed no barrier to the collection. Third, although Judge
McLaughlin of course did not say so in his opinion, she was appointed to the federal bench by President Clinton — a notable fact in light of the media attention paid to the composition of the FISC in the context of its rulings on bulk metadata collection, as discussed above. Whatever the FISC’s actual motivations for writing and releasing the October opinion, therefore, it could be viewed as noteworthy in that it was written by a Democratically-appointed judge who had not previously reviewed the bulk collection program and who specifically addressed and rejected the main constitutional claim advanced by critics of the program since its public debut.

2. Unlike Members of Congress, most Americans had no opportunity to become aware of the bulk collection program, at least through official channels. While reasonable minds may disagree as to whether the FISC was correct (in the first instance) to accept the government’s legal interpretation of the tangible things provision — particularly the argument that the bulk metadata is “relevant” — it seems clear that the interpretation was not obvious, not something that would inevitably have occurred to an outsider observer. This is probably the case even after accounting for media reporting (based on prior leaks) that bulk telephony metadata collection was in fact occurring, as noted above.276 And the government, by determining that the interpretation was classified, or at least that disclosure of the interpretation would inevitably result in disclosure of classified information, kept the information from the public. The following exchange between Chairman Goodlatte and Bob Litt, the General Counsel to the ODNI, at a July 2013 hearing of the House Judiciary Committee, captures the point:

**QUESTION:** Did you think a program of this magnitude gathering information involving a large number of people involved with telephone companies could be indefinitely kept secret from the American people?

**ANSWER:** Well, we tried.277

a. At one level, of course, keeping classified information from the American People is exactly what the Intelligence Community is supposed to do, because there is no way to inform the American People without also informing the People’s adversaries. There is no serious debate about that general proposition, which amounts only to the familiar idea that some information is indeed properly classified. The United States is a representative democracy, not a direct

---

276. As explained in Chapter 15 of NSID, supra note 1, it was possible, based solely on publicly available information, to guess at the legal arguments now disclosed to have underlay the TSP, in part because the government confirmed the existence of the TSP after it was leaked in 2005, much as it did eight years later with respect to the bulk metadata collection after it was leaked in June 2013.


279. 158 Cong. Rec. S941 (Dec. 27, 2012) (statement of Sen. Chambliss). For an interesting assessment of the evolution of oversight by the Intelligence Committees, written by a longtime observer, see Steven Aftergood, *Intelligence Oversight Stays Back from Public Accountability*, Seattle News (Jan. 2, 2013), http://blogs.fas.org/secrecy/2013/01/public_accountability/. As former Representative Jane Harman put it in July 2013, “the tradition has always been that the Members of the Intelligence Committees, which are leadership committees ... were treated with a lot of secrets that weren’t shared with others; the reason for that was ... sources and methods have to be protected.” Aspen Institute, Countermaintenance, National Security and the Rule of Law (July 18, 2013) (statement of Jane Harman at approximately 1:05:32), available at http://aspensecurityforum.com/2013/video. The Constitution itself provides for secret proceedings in Congress: Under Article I, Section 5, Clause 3, each House of Congress “shall keep a journal of its proceedings, and from time to time publish the same, excepting such parts as may in their judgment require secrecy.” U.S. Const. art. I, §5, cl. 3.

280. See 28 C.F.R. § 17.14. The prolonged, intense prepublication review process for the first edition of NSID is described in the Preface and Foreword, and the review process for this paper is described in note 1, supra.

281. 50 U.S.C. § 413b.

282. See generally ALFRED CUMMINGS and RICHARD A. BEST, JR., CONG. RESEARCH SERV., R40691, STIPEND COVERT ACT ACTION NOTIFICATIONS: OVERSIGHT OPTIONS FOR CONGRESS (Jan. 10, 2006).

283. 50 U.S.C. § 413(c)(3).

284. 50 U.S.C. § 413(a)(5).
specifically warns that “No covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or militia.”285 Without making any comment, express or implied, on any actual or hypothetical covert action, or even acknowledging that any covert action of any kind has ever actually taken place, it is quite obvious that each of those elements of the statute could raise enormously difficult and complex interpretive questions, some of which might affect many Americans.286 Yet it might be impossible, in many cases, to explain those interpretations without revealing the most sensitive classified information.287

With respect to bulk metadata collection, the Intelligence Community seems to have concluded, over a long period of time across two Presidential Administrations, that the legal interpretation was so embedded in its factual and operational context that revealing it would harm national security. Nor did any Member of Congress, including Senators Wyden and Udall, or the FISA Court itself, find a satisfactory way to reveal the legal issue without causing collateral damage. The FISC rejected as unrealistic a request from the Senate Intelligence Committee to prepare unclassified summaries of its opinions, explaining that “in most cases, the facts and legal analysis are so inextricably intertwined that excising the classified information from the FISC’s analysis would result in a remnant void of much or any useful meaning.”288 Until the June 2013 unauthorized disclosures, none of the three branches of government had found a safe way to disclose to the public the “secret law” underlying the bulk telephony metadata collection program.

The difficulty, as Senators Wyden and Udall explained in their many public statements on this issue, arises when a leak reveals “secret law” involving a

286. Put differently, it would be easy for even a relatively competent law professor, with no classified information, to write a challenging law school exam based on the language of the covert action statute.
287. For a humorous take on the potential implications of this very serious issue taken to a ridiculous extreme, see 231 CIA Agents Killed in Covert Ops Mission, The Onion (Mar. 6, 2013), http://www.theonion.com/articles/231-cia-agents-killed-in-covert-ops-mission.315553/3?ref=auto.
288. Senators Wyden and Udall, along with Senators Feinstein and Merkley, sent a letter to the FISA Court in February 2013, in which they “requested that the Court consider writing summaries of its significant interpretations of the law in a manner that separates the classified facts of the application under review from the legal analysis, so as to enable declassification.” Letter from Senators Ron Wyden, Tom Udall, Dianne Feinstein, Jeff Merkley to the FISA Court (Feb. 13, 2013), available at http://www.fas.org/irp/agency/doi/fisa/fisc-021313.pdf. In a letter dated March 27, 2013, Judge Walton, the Presiding Judge of the Court, replied that there were “serious obstacles . . . regarding your request for summaries of FISC opinions,” including the risk of “misunderstanding or confusion regarding the court’s decision or reasoning,” and for “FISC opinions specifically . . . the very real problem of separating the classified facts from the legal analysis . . . As members of Congress who have seen the opinions knowing, most FISC opinions rest heavily on the facts presented in the particular matter before the court. Thus, in most cases, the facts and the legal analysis are so inextricably intertwined that excising the classified information from the FISC’s analysis would result in a remnant void of much or any useful meaning.” Letter from Judge Walton, the Presiding Judge of the FISA Court, to Senator Dianne Feinstein (Mar. 27, 2013), available at http://www.fas.org/irp/agency/doi/fisa/fisc-032713.pdf.
Second, Congress could take measures to help ensure broader public understanding, still without departing too far from the traditional approach. One obvious possibility would be to revive the annual reports from the Intelligence Committees that were required for the first five years of FISA’s existence. Those reports, which were very well done and extremely informative, are cited throughout this treatise. Such public reporting could be conducted pursuant to statute or even in the absence of new legislation. It would require considerable and sustained effort from the two political branches, working together, but it could be done. Of course, as noted above, significant limits would remain, meaning that much would need to remain secret, but it would be reasonable to expect at least incremental gains in transparency and public understanding. It would facilitate a more informed debate over the broad policy choices and challenges in the area, but limit disclosure of operational details and related information concerning specific intelligence programs. In some cases, those details are important to understanding the programs and their legality, so this approach would not allow for a “fully and currently informed” public debate.

Third and finally, we could significantly re-calibrate the balance between secrecy and transparency, revealing significantly more information publicly, and thus reducing reliance on proxy oversight through select Congressional Committees. Although the matter is not entirely clear, that appears to be the Obama Administration’s intent, at least to a substantial degree. In June 2013, President Obama stated through a spokesperson that he “welcomes the discussion of the trade-off between security and civil liberties,” and that he “look[s] forward to continuing to discuss these critical issues with the American people” as well as with Congress. At a press conference held on August 9, 2013, the President stated:

we can, and must, be more transparent. So I’ve directed the intelligence community to make as much information about these programs as possible. We’ve already declassified unprecedented information about the NSA, but we can go further.... probably what’s a fair criticism is my assumption that if we had checks and balances from the courts and Congress, that that traditional system of checks and balances would be enough to give people assurance that these programs were run probably – that assumption I think proved to be undermined by what happened after the leaks.... I’m going to be pushing the IC to do is rather than have a trunk come out here and leg come out there and a tail come out there, let’s just put the whole elephant out there so people know exactly what they’re looking at.

In his January 2014 speech at the Department of Justice, President Obama promised to “reform programs and procedures in place to provide greater transparency to our surveillance activities,” and noted that the government had “declassified over 40 opinions and orders” of the FISC. The speech identified two additional initiatives directly in support of transparency.

First, the President directed the DNI, in consultation with the Attorney General, “to annually review for the purposes of declassification any future opinions of the [FISC] with broad privacy implications, and to report to me and to Congress on these efforts.” This may effectively mirror in a public fashion the obligations currently owed by statute to the Intelligence and Judiciary

---

293. As the President noted in January 2014. ("the challenge is getting the details right, and that is not simple") POTUS Sigh Post, supra note 49. Moreover, the Administration has not publicly described the philosophical approach underlying the already-significant disclosures it has made, the limits on such disclosures, or a comparison between the current attitude and historical standards -- although such thinking may well exist behind the scenes.

294. Chris Inglis, Goldfeder, Alexander and Ingilis Letter to the NSA-CSS Family and the USG's Unconscionably Weak Defense of NSA, LEOSE, (Sept. 20, 2013), available at http://www.lawfareblog.com/2013/09/alexander-and-inglis-letter-to-the-nsa-css-family-and-the-ngs-unconscionably-weak-defense-of-usa. It is far from clear that his views are aligned with those of the President and the President's closest advisers, but Chris Inglis, NSA's departing Deputy Director, described an important distinction between transparency in aid of broad policy debate, and transparency concerning operational matters, in an interview given a week before the President's January 2014 speech:

We're trying to strike that right balance. The balance today I think has a policy component of whether it's broadly permissible, useful, effective to give the kinds of authorities to NSA that we do. And that I think should have a fuller public discussion. But when you get down to the very discreet, right, somewhere between strategic and tactical choices about how you then implement that, I think that we need to then have a closed in discussion between three branches of government, those who stand in the shoes of the American public, so that we can have a fully informed decision that then results from that fully informed dialogue. But I am not at this point saying that I would bring all of NSA's capabilities out into the open. Not because I'm in any way, shape or form thinking that the American public would be shocked or outraged by those but because I really don't think we can afford to give those capabilities away to our adversaries.

Chris Inglis NPR Interview, supra note 56.


296. Statement by the Press Secretary on the Amash Amendment (July 23, 2013) (“In light of the most recent unauthorized disclosures, the President has said that he welcomes a debate about how best to simultaneously safeguard both our national security and the privacy of our citizens. The Administration has taken various proactive steps to advance this debate including the President’s meeting with the Privacy and Civil Liberties Oversight Board, his public statements on the disclosed programs, the Office of the Director of National Intelligence’s release of its own public statements, ODNI General Counsel Bob Litt’s speech at Brookings, and ODNI’s decision to declassify and disclose publicly that the Administration filed an application with the Foreign Intelligence Surveillance Court. We look forward to continuing to discuss these critical issues with the American people and the Congress.”), available at http://www.whitehouse.gov/the-press-office/2013/07/23/statement-press-secretary-amash- amendment, see also The White House, Office of the Press Secretary, Background on the President’s Statement on Reforms to NSA Programs (“President Obama believes that there should be increased transparency and reforms in our intelligence programs in order to give the public confidence that these programs have strong oversight and clear protections against abuse.”), available at http://www.whitehouse.gov/the-press-office/2013/08/09/background-president-s-statement-reforms-nsa-programs.

Committees of Congress under 50 U.S.C. § 1871. Regular efforts to review and declassify FISA Court opinions have been ongoing for years, but the Presidential imprimatur may help the Intelligence Community lean forward in assessing what can be disclosed without harming national security. As the President noted, “we have declassified over 40 opinions and orders” from the FISC since the June 2013 unauthorized disclosures, which is in itself an unprecedented level of transparency.

Second, the President also seemed to endorse increased disclosure of specific investigative details in some cases, including to the subjects of national security investigations. He directed the Attorney General “to amend how we use national security letters,” which (the President explained) “can require companies to provide specific and limited information to the government without disclosing the orders to the subject of the investigation.” Under the amended approach, “this secrecy will not be indefinite,” and “will terminate within a fixed time unless the government demonstrates a real need for further secrecy.” As discussed in § 20.8 of NSIP, the FBI annually issues tens of thousands of national security letters. It is possible to imagine a process under which the President’s directive results only in a (potentially significant) administrative burden for the FBI and DOJ, by requiring periodic re-certification of the basis for the initial secrecy directive that is always invoked for each NSL with directives being allowed to lapse only rarely and after relatively long periods of time. But it is also possible to imagine a more significant effect, where the FBI discloses large numbers of NSLs after relatively short periods of secrecy.

Of course, as the President recognized, a central “challenge is getting the details right, and that is not simple.” Moreover, it remains unclear whether and to what extent increased transparency will extend further, to other intelligence programs – e.g., those involving Humint or covert action – that have not been subjected to the same level of prior, unauthorized disclosure. The focus since June 2013 has been on signals intelligence, because that was the subject of the unauthorized disclosures, but the logic animating efforts towards transparency could extend further, to other forms of intelligence activity. To some observers, the President and his closest advisors seem to be charting a course for an environment in which the basic existence of all (or most) intelligence programs, or at least signals intelligence programs, is publicly disclosed, with information about certain operational details (e.g., providers and targets) still mostly secret. They may face resistance from the Intelligence Community in staying that course over time, but if they are successful, it would represent a very significant recalibration.

The effects of such a broad re-calibration could be felt in at least two ways beyond the government’s own, voluntary actions. First, official disclosures of previously classified information will resonate through FOIA and State Secrets doctrine, where the government’s litigating positions will be tested for consistency with the logic implicit in the voluntary transparency. It therefore may be difficult to predict exactly how such official disclosures may beget additional disclosures as compelled by the courts, especially in the absence of any overtly described philosophical approach.

Second, and perhaps more importantly, there is a potential interaction be-

298. See June 2013 HPSCI Open Hearing, supra note 27, Statement of Bob Litt (“It’s been a very difficult task … The facts frequently involve classified information, sensitive sources and methods. And what we’ve been discovering is that when you remove all the information that needs to be classified, you’re left with something that looks like Swiss cheese and is not really very comprehensible.”). July 2013 SIC Hearing, supra note 27, Statement of Bob Litt (“I’d like to strive for the maximum possible transparency about the activities of the court, consistent with the need to protect sensitive sources and methods. We have been working for some time to declassify the court’s opinions to the extent possible. But legal discussions and court opinions don’t take place in a vacuum. They depend on the facts of the particular – of the particular case. And I want to quote here from Paul Walton, who is now the Chief Judge of the FISC, who said in a letter to the foreign – to the Senate Intelligence Committee, quote, ‘Most FISC opinions rest heavily on the facts presented in the particular matter before the court. Thus, in most cases, the facts and legal analysis are so inextricably intertwined that excising the classified information from the FISC analysis would result in a remnant void of much or any useful meaning,’ close quote. That’s an excellent and pithy summary of the challenge we face in trying to declassify these opinions.”).

299. POTUS Signing Statements, supra note 49.

300. On January 27, 2014, the Department of Justice announced an agreement to settle litigation in the FISA Court brought by telecommunications providers and other companies. Under the terms of the agreement, providers may publish certain data about information requests from the government, in the aggregate, in bands of 1000 (e.g., 0-999 requests, 1000-2000 requests), divided into content and non-content categories, with a time lag between receipt of the requests and publication of the data. See Notice filed in the Foreign Intelligence Surveillance Court, Nos. 13-03 to 13-07 (Jan. 27, 2014), available at http://legalitities.typepad.com/files/lsa-notice-1.pdf. Publicly available pleadings filed in the FISA Court after June 2013 are available at http://www.uscourts.gov/vocuments/court/psc/is/index.html.

301. POTUS Signing Speech, supra note 49.

302. Id.

303. For a discussion of the certification process, see NSIP, supra note 1, at § 20.10.

304. In a July 2013 speech, Bob Litt, General Counsel of ODNI, reiterated that “[e]ven before the recent disclosures, the President said that we welcomed a discussion about privacy and national security, and we are working to declassify more information about our activities to inform that discussion.” July 2013 Litt Speech, supra note 27, at 21-22. But he also recognized that the “level of detail in the current public debate certainly reflects a departure of the historic understanding that the sensitive nature of intelligence operations demanded a more limited discussion,” and that the “discussion can and should, have taken place without the recent disclosures.” Id. at 22. As Mr. Litt put it at the July 2013 SIC hearing, “we are having a public debate now, but that public debate is not without cost.” July 2013 SIC Hearing, supra note 27, Statement of Bob Litt. At his August press conference, President Obama said that although “Mr. Snowden’s leaks triggered a much more rapid and passionate response” than otherwise would have been the case, “I actually think we would have gotten to the same place.” August 2013 Remarks by the President, supra note 297: On the other hand, he also said that the disclosures “pulled at risk our national security and some very vital ways that we are able to get intelligence that we need to secure the country,” and that the voluntary disclosures were designed to address the unfortunate fact that:

Once the information is out, the administration comes in, tries to correct the record. But by that time, it’s too late or we’ve moved on, and a general impression has, I think, taken hold not only among the American public but also around the world that somehow we’re out there wilfully just sucking in information on everybody and doing what we please with it.

between increased transparency and the scope of intelligence activity. Intelligence activity that helps the U.S. government when done covertly may harm it when done overtly. For example, clandestine surveillance of foreign government officials may aid U.S. foreign policy — e.g., by giving U.S. treaty negotiators insight into their foreign counterparts’ instructions. As such, foreign policy makers may support and even require such surveillance from the Intelligence Community. On the other hand, however, transparent surveillance of foreign government officials may have precisely the opposite effect, creating challenges that cause policy makers to require less surveillance.306 If less surveillance leads to a perceived intelligence failure, of course, resulting demands to expand surveillance may cause the pendulum to swing back.307

306. In October 2013, revelations that the NSA had allegedly been spying on world leaders, including the German Chancellor, created a diplomatic furor. See, e.g., James Kanter and Alan Cowell, "Amid New Storm in U.S.-Europe Relationship, a Call for Talks on Spying," N.Y. Times, Oct. 26, 2013, at A4. Regardless of the sincerity of these expressions of shock and outrage, they clearly had an impact on U.S. policymakers.

307. It is worth recalling that the debate about surveillance of foreign governmental and diplomatic personnel is not new. The 1978 legislative history of FISA makes absolutely clear that the law was intended to allow surveillance of foreign diplomatic facilities in the United States. See H.R. Rep. No. 95-1283, at 27 (1978) (FISA authorizes surveillance of “foreign embassies and consulates and similar ‘official’ foreign governmental establishments”). S. Rep. No. 95-604, at 19 (1978), reprinted in 1978 U.S.C.C.A.N. 3904. This approach represented a dramatic change from the position of at least some elements of the United States government in the years prior to World War II, perhaps best summarized by the斩首 response attributed to U.S. Secretary of State Henry Stimson, that “gentlemen do not read each other’s mail.” More context for that statement is provided from a 1982 New York Times review of James Bamford’s book about the NSA, The Puzzle Palace: FIFTY-THREE years ago, in the early months of Herbert Hoover’s Administration, Secretary of State Henry L. Stimson was presented with a small batch of Japanese intercepts that had been deciphered by a highly secret American code-breaking organization known as the Black Chamber. Appalled at the invasion of another nation’s private communications, Stimson immediately cut off funding to the cryptologists with the admonishment “Gentlemen do not read each other’s mail.” It was not one of the more prescient decisions in American history. Driven by the experiences of World War II and then the Cold War and drawing on advances in computers and electronics, in 1952 the Government created a new version of the Black Chamber — the National Security Agency, which is the largest, most sensitive and potentially most intrusive American intelligence agency.


307. One outside observer described the pendulum effect in more stark terms: This is speculation. I have no hard facts or evidence to support it. But I am convinced to a moral certainty that NSA is scaling back certain collection.

That is not something I say with pleasure or triumph but, rather, with frustration, sadness, and worry.

Imagine you were a high-level decision maker in a clandestine intelligence agency. Imagine that you had played by the rules Congress had laid out for you, worked with oversight mechanisms to fix errors when they happened, and erected strict compliance regimes to minimize mistakes in a mind-bogglingly complex system of signals intelligence collection. Imagine further that when the programs became public, there was a firestorm anyway. Imagine that nearly half of the House of Representatives, pretending it had no idea what you had been doing, voted to end key collection activity. Imagine that in response to the firestorm, the President of the United States — after initially defending the intelligence community — stepped in and said that what was really needed was more transparency and described the debate as healthy.

Imagine that journalists construed every fact they learned in light of the need to keep feeding at the trough of a source who had stolen a huge volume of highly classified materials and taken it to China and Russia.

What would you do? Here’s what: You’d take a hard look at your most forward-leaning programs — and you’d turn them off. You would do this using words like “prudential” and “current environment” — of course standing by the fact that you had a legal basis, just as the president has stood by you in some formal sense. But just as the president has let the intelligence community swing in the wind, limiting his own exposure by making the problem all your own, you would cut your losses — even if you weren’t even wrong to do so.

And you would do it knowing somewhere in your heart that some day, the pendulum would swing the other way and there would be recriminations for having turned those programs off, just as there are now recriminations for having such programs online. You would even know that many of the same people would be responsible for the mutually contradictory recriminations. You would know that after some big attack or intelligence failure, the scoop that you turned off collection tailored to the sort of information you needed to stop that event would be just as irresistible to the Washington Post and the Guardian as was the story that you ran over Americans’ civil liberties. You would know that the papers would be just as ruthless with the facts. You would know that the same members of Congress who are today outraged at what your agency is doing would be outraged then at what it isn’t doing. And you would know that almost nobody will bother to know what they are talking about before having very strong opinions about how you fell down on the job and thus bear responsibility for both the smoldering mines of some federal building somewhere and for destroying American values.

As I say, I have no evidence that this scaling back is taking place, and I don’t know if programs or activities on the blade of the prudential meat axe look like — so until you look out over those smoldering mines, feel free to disregard this post and regard it as the alarmist fear-mongering of an apologist for the national security state. But for the record, I dissent from the retrenchment I believe is going on. And here’s the standard I would propose for the reevaluation of collection programs and activities that might seem too edgy today given the circumstances. If they were lawful and defensible and necessary pre-Snowden, they are lawful and defensive and necessary today.


282 JOURNAL OF NATIONAL SECURITY LAW & POLICY | Vol. 7:209
personal privacy and individual freedom.310 The President stated soon thereafter that he "thought they did an excellent job," and promised to deliver a more "definitive" assessment of the Review Group's recommendations in January 2014.311 In his January 2014 speech, and an accompanying Presidential Policy Directive on signals intelligence,312 the President made several determinations and issued several directives to the Attorney General and the Director of National Intelligence (DNI). Many of the President's directives leave options open, and require choices to be made, so their full effect is difficult to measure as of this writing.

First, as noted above, the President endorsed creation of an outside "panel of advocates" to "provide an independent voice in significant cases before the Foreign Intelligence Surveillance Court."313 He called on Congress to enact legislation on this topic, which injects a significant degree of uncertainty until the legislation is finalized.

Second, the President directed the Attorney General and the DNI to adopt what amount to more stringent minimization procedures under Section 702 of the FISA Amendments Act, 50 U.S.C. § 1881a. The President did not mention


- Surveillance of U.S. persons (e.g., "important restrictions on the ability of the Foreign Intelligence Surveillance Court (FISC) to compel third parties such as telephone service providers) to disclose private information to the government," and "similar restrictions on the issuance of National Security Letters ... [including] prior judicial review except in emergencies," as well as putting an "end" to the current bulk telephony metadata collection program and "transition[ing] to a system in which such metadata is held privately," and requiring greater transparency).
- Surveillance of Non-U.S. persons (e.g., "not targeting any non-U.S. person "based solely on that person's political views or religious convictions");
- Setting Priorities and Avoiding Unjustified or Unnecessary Surveillance (e.g., "with a small number of closely allied governments, meeting specific criteria, the US Government should explore understandings or arrangements regarding intelligence collection guidelines and practices with respect to each others' citizens (including, if and where appropriate, intentions, structures, or limitations with respect to collection");
- Organizational Reform (e.g., splitting NSA from Cybercom, and creating a Public Interest Advocate to oppose the government in the FISC);
- Global Communications Technology (e.g., the U.S. government should be "fully supporting and not undermining efforts to create encryption standards" and making clear that it will not in any way subvert, undermine, weaken, or make vulnerable generally available commercial encryption [and (3) supporting efforts to encourage the greater use of encryption"); and
- Protecting What We Do Collect (e.g., reverting to need-to-know principles, rather than need-to-share principles, governing the dissemination of classified information within the government).

313. POTUS Signat Speech, supra note 49.

the FISA Court in this directive, so it may be that the restrictions will be internal to the executive branch, rather than official (and judicially enforceable) FISA minimization procedures,314 but they will still restrict the government's behavior, even if they do not create rights in any individual.315

These new restrictions, the President said, will be "on government's ability to retain, search, and use in criminal cases communications between Americans and foreign citizens incidentally collected under Section 702" of the FISA Amendments Act, 50 U.S.C. § 1881a.316 To understand these new restrictions, including what they mean and how they may work in practice, it is necessary first to understand the pre-existing rules, beginning with the idea of "incidental" collection.

As discussed in Chapter 17 of NSIP, Section 702 of the FAA allows the government to target non-U.S. persons reasonably believed to be located abroad. Incidental collection occurs under Section 702, as it does under all forms of electronic surveillance, because the government collects both sides of communications involving its surveillance target. In particular, under Section 702, when the government targets a non-U.S. person located abroad, it will acquire his communications with all interlocutors, including any who happen to be U.S. persons (or are located in the United States). Such incidental collection does not violate the FAA's explicit ban on "reverse targeting," in which, for example, the government pretends to be interested in Smith, a non-U.S. person located abroad, but is actually seeking information from or about Jones, a U.S. person (after becoming an invalid target), with whom Smith communicates.317 Properly targeting Smith will still result in incidental collection of some statements made by Jones.

Under existing procedures, the NSA generally may not retain information

314. For a discussion of the FAA, and minimization procedures issued under it, see NSIP, supra note 1, at Chapter 17.
316. POTUS Signat Speech, supra note 49.
317. For a discussion of reverse targeting and querying under Section 702 of the FAA, see NSIP, supra note 1, at Chapter 17. Chris Inglis, the Deputy Director of NSA, explained this issue in an interview conducted in January 2014.

So let's say that I'm going after ... the head of Al-Qaeda worldwide ... I collect some of his communications ... and they're now in a pile that I expect an analyst to then understand. ... The only way the U.S. persons could've gotten into that pile is that they are, in fact, on the other side of the communication of [him]. ... And the 702 provision goes so far as to say that we cannot use [it] ... to reverse-target Americans ... That's expressly prohibited by the law. ... So let's say some clever person says, you know, I'm not authorized to target Chris Inglis overly, unless I go get a warrant and he's not done anything to show himself as being a threat to the nation. But I know that he's always in contact with somebody that I am legitimately authorized to go after or I could make some plausible case for that. So why don't I go after Party B because I know that Chris is always in contact with him and I'll just collect enough communications that gives me insight into Chris Inglis? That is expressly prohibited by the law. It's written in that you cannot use that as a back door, as a 702 back door, the authority being '702, to target Chris Inglis. It's called reverse targeting.

Chris Inglis NPR Interview, supra note 56.
acquired under Section 702 that is recognized to be "of" or "concerning" a U.S. person, but it is permitted to retain such information in two main instances. First, NSA may retain U.S. person information if it constitutes "foreign intelligence information" as defined in FISA, including both "protective" and "affirmative" foreign intelligence information. That is, NSA may retain U.S. person information that is necessary to the ability of the United States to "protect" against several specified threats to national security, such as attack, sabotage, espionage, and terrorism, and it also may retain U.S. person information if it is affirmatively necessary to the national defense, national security, or the conduct of the foreign affairs of the United States. Second, NSA may also retain U.S. person information if it constitutes evidence of a crime, including crimes that are wholly unrelated to foreign intelligence and national security (e.g., gambling or child pornography). And NSA may also share such information with law enforcement agencies for use in a criminal prosecution of the U.S. person. Finally, under pre-existing rules, although information acquired from "upstream" collection under Section 702 may not be queried using U.S. person identifiers (e.g., a U.S. person's name, email address, or telephone number), information collected from "downstream" collection (e.g., directly from Internet Service Providers) may be so queried, as long as there is a valid foreign intelligence purpose for the querying. The new restrictions will presumably limit both the retention and dissemination of U.S. person information that is evidence of a crime. One possible approach would be to retain only evidence of "foreign intelligence crimes," such as espionage or terrorism, but that would essentially eliminate law enforcement retention and dissemination altogether, because evidence of such crimes is always independently "foreign intelligence information." Another approach, perhaps more likely, is to identify a group of more serious crimes, whether or not related to foreign intelligence, as to which evidence obtained through Section 702 may be retained and disseminated. 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 by subject to approval by the FISA Court (perhaps with an emergency procedure).  

(1) the name, unique title, or address of a United States person; or (2) other personal identifiers of a United States person when appearing in the context of activities conducted by that person. A reference to a product by brand name, or a manufacturer's name or the use of a name in a descriptive sense, e.g., "Monroe Doctrine," is not an identification of a United States person. Office of the Dir. of Nat'l Intelligence, 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, available at http://www.nsa.gov/files/documents/Minimization%20Procedures%20as%20they%20have%20be%20implemented%20under%20Section%20702.pdf. The minimization procedures define communications "of" a U.S. person in all communications "to which a United States person is a party," and communications "concerning" a U.S. person as "all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly-available information about the person." Id. at §§ 2(c). For a more complete discussion of minimization, see NSISP, supra note 1, at Chapter 9.


320. See 50 U.S.C. §§ 1801(e)(1)-(2) (definitions of "foreign intelligence information"). 183(a) (incorporating these definitions for purposes of Section 702 of the FISA).

321. 2011 NSA 702 Minimization Procedures, supra note 318, at § 3(b)(4), 6(a)(3). Section 2.8(e) of Executive Order 12,333 provides for Intelligence Community elements to have procedures that allow collection, retention and dissemination of "incidentally obtained information that may indicate involvement in activities that may violate Federal, state, local, or foreign laws." This may need to be changed in light of the President's speech.

322. 2011 NSA 702 Minimization Procedures, supra note 318, at § 6(b)(8) ("dissemination of intelligence reports based on communications of or concerning a U.S. person may only be made to a recipient requiring the identity of such person for the performance of official duties...if....the communication or information is reasonably believed to contain evidence that a crime has been, is being, or is about to be committed"). Since 1978, FISA has allowed use of lawfully collected information for any kind of criminal prosecution, even while restricting the purpose of the collection. As discussed in Chapters 9 and 17 of NSISP, supra note 1, under 50 U.S.C. § 1801(b)(3), "minimization procedures" are defined to include procedures that "notwithstanding [other elements of minimization]...allow for the retention and dissemination of that 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)(3).

323. Under the NSA Section 702 minimization procedures (§ 2(f)), identification of a U.S. person means:...
proposes, and the court approves, the 2009 emergency protocol, or the more generous, standard FISA protocol for emergencies set out in 50 U.S.C. § 1805(e). 330

The second phase of the President’s directive concerning bulk telephony metadata is far more ambitious: by March 28, 2014, 331 he directed the identiﬁcation of “options for a new approach that can match the capabilities and ﬁll the gaps that the Section 215 program was designed to address without the government holding this metadata itself.” 332 The President recognized that there were “difﬁcult problems” with alternatives in which “the [telecommunications] providers or a third party retain the bulk records,” and that “more work needs to be done” on other approaches. As of this writing, it is not clear that a viable alternative will be found and/or implemented by March 28, although some possibilities do exist. 333

Fourth and ﬁnally, the President announced that he had “taken the unprecedented step” of extending to non-U.S. persons certain minimization and other protections governing retention and use of information that heretofore have been applied only to U.S. persons. 334 The President was correct in his characterization of this initiative, which represents a major conceptual shift. Depending on how it is implemented, the initiative could also yield some signiﬁcant operational consequences. 335

---

330. Under 50 U.S.C. § 1805(e), “the Attorney General may authorize the emergency employment of electronic surveillance” if, among other things, he 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.” 50 U.S.C. § 1805(e). In such a case, the President must then submit an application to the court within 7 days. Id.

331. March 28, 2014 may be the expiration date for the bulk telephony metadata collection order in effect at the time of the President’s speech, which was issued by the FISC on January 3, 2014 and published by the government on that date. See IC on the Record, http://icommissionrнный.nviml.com.

332. POTUS Sigan Speech, supra note 49.

333. One possibility would involve NSA continuing to collect, format and maintain physical custody of the data as it does today. But NSA would segregate repositories containing the data so that access is available only through specially credentialed members of a consortium of participating telecommunications providers, or perhaps some other entity from within the government or elsewhere. To be sure, co-locating representatives from providers in government ofﬁces has been associated with problems in the past. see, e.g., Department of Justice, Ofﬁce of the Inspector General, A Review of the FBI’s Use of Exigent Letters and Other Informal Requests for Telephone Records (Jan. 2010), available at http://www.justice.gov/oig/spcial/special1001s.pdf, and there would certainly be technical issues (including, e.g., non-query access to the data, for maintenance and other non-substantive purposes), but with appropriate attention to oversight, those problems could probably be avoided. Moreover, the cost of third-party personnel to staff the access point would be a tiny, tiny fraction of the cost of the data and maintaining it in the (less secure) private sector. The idea might not work, of course, but it seems worth exploring, especially if it can be credibly described as NSA not having “possession” of the data because of the access limits that require the participation of a third party before the data may be queried.

334. POTUS Sigan Speech, supra note 49. In particular, the President “directed the DNI, in consultation with the Attorney General, to develop these safeguards [for non-U.S. persons], which will limit the duration that we can hold personal information, while also restricting the use of this information.” Id.

335. As one thoughtful commentator put it, the President’s speech and PPD together were “a defense that signals a great deal more change spiritually than it promises in practical terms, but one that also has
The President elaborated on the conceptual shift through a Presidential Policy Directive, PPD-28, issued on the same day as his speech.346 The PPD’s fundamental insight is that signals intelligence must “take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside.” 337 It provides that “all persons have legitimate privacy interests in the handling of their personal information,” and it explicitly recognizes the “legitimate privacy and civil liberties concerns of U.S. citizens and citizens of other nations.” 338 Section 1 of the PPD, which sets out its basic principles, states that “[p]rivacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities,” and that “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.” 339 Section 2, which prescribes limits on bulk collection (discussed below), explains that the limits “are intended to protect the privacy and civil liberties of all persons, regardless of where they might reside.” 340 This applies to the safeguarding of personal information, repeats the idea that “[a]ll persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside,” and the recognition that “all persons have legitimate privacy interests in the handling of their personal information.” 341 This is in stark contrast to the language of Executive Order 12333, the main internal charter for the U.S. Intelligence Community, which focuses almost exclusively on privacy protections for U.S. persons. 342 As the President said, therefore, PPD-28 represents an unprecedented change in U.S. intelligence policy, at least at the rhetorical level.

The degree of substantive change that will follow from PPD-28 is less certain. Its directives can be divided into several groups according to their likely operational impact. At the outset, in some respects, the PPD serves what might be termed an educational function, explaining certain protections that already exist in the way the U.S. Intelligence Community does business.343 These include the requirement that all Sigint “shall be authorized by statute” or other authority, and be conducted strictly in accordance with the Constitution and U.S. laws, 344 that Sigint may not be used to offer a competitive advantage to U.S. businesses, 345 that Sigint requirements are to be established through the inter-agency process on an annual basis, 346 and probably that Sigint “shall be conducted exclusively where there is a foreign intelligence or counterintelligence purpose.” 347

In three other, related areas, the PPD may or may not lead to significant change. First, it requires that Sigint “should be as tailored as possible,”348 which differs slightly from the pre-existing requirement in EO 12333 that the Intelligence Community “shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad.” 349

342. Another way of putting this, as one commentator has, is that the PPD uses “values-based statements as justifications for policies that already exist, at least de facto, for purely functional reasons.” Winters Guide for the Perplexed, supra note 335.
343. PPD-28, supra note 312, at 2-3 (Section 1(a)).
344. Id. at 3 (Section 1(c)). The PPD is careful to note that “[c]ertain economic purposes, such as identifying trade or sanctions violations or government influence or direction, shall not constitute competitive advantage” for these purposes. Id. at 3 n.4.
345. Id. at 4 (Section 3).
346. Id. at 3 (Section 1(b)). The PPD cross-references Executive Order 12333’s definition of these terms. Id. at 2-2 (Introduction). Under Executive Order 12333 §§ 3.5(a) and (e), “Foreign intelligence means information gathered and activities conducted to identify, locate, exploit,iropr, protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or their agents, or international terrorist organizations or activities.” and “Foreign intelligence means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.” EO 12333 §§ 3.5(a), (e). For a discussion of the meaning of these terms, see NSP, supra note 1, at § 2.7. Under Section 2.3 of Executive Order 12333, the Intelligence Community may collect not only foreign intelligence and counterintelligence, but also, among others:

Information obtained in the course of a lawful foreign intelligence, counterintelligence, international drug or international terrorism investigation, ... Information needed to protect foreign intelligence or counterintelligence sources, methods, and activities from unauthorized disclosure; ... Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility [and] Information arising out of a lawful personal, physical, or communications security investigation.

EO 12333 § 2.3. Most of these additional categories can, in most cases, probably be fit under the broad rubric of “a foreign intelligence or counterintelligence purpose” as described by PPD-28, but there may be exceptions to that general rule. It is not clear why the PPD omitted these categories of information, and why it did not simply cross-reference Section 2.3 here, as it did elsewhere. If there was an intent to exclude some forms of Sigint, the intent was not communicated clearly.
347. PPD-28, supra note 312, at 3 (Section 1(d)).
348. EO 12333 § 2.4. The PPD “is not intended to alter the rules applicable to U.S. persons in Executive Order 12333” PPD-28, supra note 312, at n.9. Thus, as a technical matter, the PPD sets the “as tailored as feasible” standard for Sigint directed at non-U.S. persons located abroad, and the executive order continues to require the “least intrusive” standard for all collection techniques (including but not limited to Sigint) used in the U.S. or against U.S. persons abroad. It is not clear that there is
but also applies to Sigint collection directed against non-U.S. persons abroad. The extent of this tailoring, like the extent of the dignity and respect afforded to non-U.S. persons' privacy, will determine its significance. 549 A requirement that each instantiation of EO 12333 surveillance abroad be reviewed and approved individually by a high-level, inter-agency panel, for example, could substantially hinder the speed and agility (and perhaps, therefore, the effectiveness) of such surveillance, even if most surveillance is ultimately approved as sufficiently tailored.

Second, in the same vein, the PPD instructs the Intelligence Community to prioritize "appropriate and feasible alternatives to signals intelligence," such as information "from diplomatic and public sources" (but also presumably including Humint and other intelligence disciplines). 340 Again, the degree of such prioritization will determine the effects of this requirement. For example, if proponents of Sigint within the U.S. Intelligence Community must rebut a presumption against collection in each case, the effects could be substantial. Again, those effects could arise not only because of the ultimate scope of Sigint that is permitted, but also because of the demands of the process itself. If, on the other hand, the prioritization means only that the United States will attempt to work cooperatively with foreign partners on Sigint conducted in their territory, or will try to use overt diplomatic channels more frequently to gather information from or about allied government leaders (e.g., the Chancellor of Germany), it may not have as much of an impact.

Third, with respect to data collected in bulk, 251 the PPD provides that it may be used only for counterintelligence or protective intelligence purposes and law enforcement, not for affirmative foreign intelligence collection. 552 As noted above, the bulk telephony metadata program may only be used for counterterrorism, and so with respect to that particular program, the PPD represents an expansion of permitted purposes (of course, adherence to the narrower requirements set by the FISA Court is still required). However, the PPD provides for changes to the permitted purposes of bulk collection over time. 553 Not all of which must be made public. 554 Much will depend, therefore, on whether those permitted purposes are held static, expanded, or contracted over time. Implemented aggressively, each of the foregoing three directives could have a non-trivial effect on signals intelligence operations; but there is also room to apply them in ways that do not substantially curb existing activities.

The final element of the PPD is the one the President emphasized in his speech: its command that, "[t]o the maximum extent feasible consistent with the national security," the government adopt "policies and procedures . . . for safeguarding personal information collected from signals intelligence activities," and that those procedures be "applied equally to the personal information of all persons, regardless of nationality." 385 Conceptually, as noted above, this is a major change in U.S. policy. But the immediate, operational impact of the PPD in this area is probably more modest. The new policies and procedures required by the PPD are due within one year, must be disclosed publicly to the

any meaningful difference in these two formulations in practice. The concept of "narrow tailoring" is typically associated with jurisprudence involving the First Amendment rather than the Fourth Amendment. See, e.g., Boos v. Barry, 485 U.S. 312 (1988). Perhaps it is meant to address or create a presumption against bulk collection, although the PPD elsewhere addresses bulk collection directly, and it is not impossible to imagine some forms of "tailored bulk collection."

349. One thoughtful commentator assessed the PPD this way:

The United States is now on record as a formal matter of presidential policy announcing that it respects the privacy of non-citizens abroad and takes that into account when it conducts espionage; it doesn't just disseminate and retain information about people willy-nilly with no regard for the information's importance relative to that material's value to foreign intelligence. That's an amazing statement. But it actually does not require a revolution -- or even much change -- in intelligence affairs to implement. The reason is that the US, at least in the modern age, has not disseminated or retained willy-nilly private information about foreign individuals without regard for its intelligence value -- not because the intelligence community has been especially concerned about foreigners' privacy rights as such, but because indiscriminate collection and dissemination is integral to good intelligence product.

Witten Guide for the Perplexed, supra note 335. Although the PPD certainly does not 'require' a profound change in intelligence affairs, it could produce such change depending on how it is implemented over time.

350. PPD-28, supra note 312, at 3 (Section 1(d)).

351. The PPD defines "bulk" collection as "the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.)." PPD-28, supra note 312, at 3 n.5 (Section 2). This definition does not refer explicitly to what may be the key feature of bulk collection,
maximum extent possible consistent with national security, and must do all of
the following.\textsuperscript{356}

- **Retention:** allow retention of personal information "only if the retention of comparable information concerning U.S. persons would be permitted under section 2.3 of Executive Order 12333,"\textsuperscript{357} and "subject to the same retention periods as applied to comparable information concerning U.S. persons." Absent a determination of comparability, there is a five-year cap on retention "unless the DNI expressly determines that continued retention is in the national security interests of the

\textsuperscript{356} Id. at 7 (Section 4(a)).

\textsuperscript{357} As discussed in NSIP, supra note 1, at § 2:7, Section 2.3 of Executive Order 12,333 provides for procedures established by the head of each Intelligence Community element and approved by the Attorney General that "shall permit collection, retention, and dissemination of the following types of information:"

(a) Information that is publicly available or collected with the consent of the person concerned;

(b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the Federal Bureau of Investigation (FBI); or, when significant foreign intelligence is sought by other authorized elements of the Intelligence Community, provided that no foreign intelligence collection by such elements may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;

(c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international drug or international terrorism investigation;

(d) Information needed to prevent the safety of any persons or organizations, including those who are targets, victims, or hostages of international terrorist organizations;

(e) Information needed to protect foreign intelligence or counterintelligence sources, methods, and activities from unauthorized disclosure. Collection within the United States shall be undertaken by the FBI except that other elements of the Intelligence Community may also collect such information concerning present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for any such employment or contracting;

(f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;

(g) Information arising out of a lawful personnel, physical, or communications security investigation;

(h) Information acquired by overseas reconnaissance and not directed at specific United States persons;

(i) Incidentally obtained information that may indicate involvement in activities that may violate Federal, state, local, or foreign laws; and

(j) Information necessary for administrative purposes.

EO 12,333 § 2.3.

In addition, Section 2.3 provides that "elements of the Intelligence Community may disseminate information to each appropriate element within the Intelligence Community for purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it, except that information derived from signals intelligence may only be disseminated or made available to Intelligence Community elements in accordance with procedures established by the Director in coordination with the Secretary of Defense and approved by the Attorney General." Id.
• Oversight: "include appropriate measures to facilitate oversight over the implementation of safeguards protecting personal information, to include periodic auditing."\textsuperscript{364} Oversight and auditing remain an integral part of current intelligence operations, as discussed above and in Chapter 13 of NSIP, so this directive does not require a major change from current practice.

***

The unauthorized disclosures that began in June 2013, and the government's reaction to them, provoked a very strong public reaction. Indeed, it may be that the recurring cycle of U.S. intelligence expansion and retrenchment is now entering a period of significant retrenchment, although future events could obviously alter the swing of the pendulum. As part of that process, the President and his closest advisors have taken several bold steps to re-calibrate significantly the balance between secrecy and transparency in favor of the latter; and they have also taken at least some steps to reduce the scope of signals intelligence. But the President's January 2014 speech and PPD-28 will be fully understandable only in hindsight. Years from now, they may be viewed as the first articulation of a new paradigm of transparency, privacy, and internationalism in U.S. intelligence. However, it is also possible that they will be viewed as a collection of fairly modest changes, largely cosmetic in nature, that were designed to placate critics in the United States and abroad. Either way, the result will be praised by some and condemned by others. As Justice Stewart explained in his concurring opinion in the Pentagon Papers case more than 40 years ago, national security policy demands "judgment and wisdom of a high order,"\textsuperscript{365} and only time will tell whether we now possess those virtues in sufficient measure.

\textsuperscript{364} PPD-28, supra note 312, at 7 (Section 4(a)(iv)). When a "significant compliance issue occurs involving personal information of any person, regardless of nationality," the policies and procedures must ensure that the DNI is promptly informed. Id.

\textsuperscript{365} New York Times v. U.S., 403 U.S. 713, 728-29 (1971) (Stewart, J., concurring) ("In the absence of the governmental checks and balances present in other areas of our national life, the only effective restraint upon executive policy and power in ... national defense ... may lie in an enlightened citizenry ... Yet it is elementary that the maintenance of an effective national defense requires both confidentiality and secrecy."). Justice Stewart wrote:

I should suppose that moral, political, and practical considerations would dictate that a very first principle of that wisdom would be an insistence upon avoiding secrecy for its own sake. For when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion. I should suppose, in short, that the hallmark of a truly effective internal security system would be the maximum possible disclosure, recognizing that secrecy can best be preserved only when credibility is truly maintained.

Id.
Texas Law Review
June, 2010

Symposium: Law at the Intersection of National Security, Privacy, and Technology

III. Focus on FISA

PROGRAMMATIC SURVEILLANCE AND FISA: OF NEEDLES IN HAYSTACKS

William C. Banks [FN1]

Copyright (c) 2010 Texas Law Review Association; William C. Banks

Beginning in 1978, the Foreign Intelligence Surveillance Act [FN1] (FISA) authorized the means for electronic collection of foreign intelligence that served the nation well for many years. The basic idea was simple. Government may conduct intrusive electronic surveillance of Americans or others lawfully in the United States without traditional probable cause to believe that they had committed a crime if it could demonstrate to a special Article III court that it had a different kind of probable cause: reason to believe that targets of surveillance are acting on behalf of foreign powers. [FN2] Over time, FISA was amended several times to extend its procedures to conduct physical searches, [FN3] monitor suspected lone-wolf terrorists, [FN4] and accommodate evolving threats. [FN5]

Over the last decade, critics have argued that the patchwork-like architecture of FISA has become too rigid, complicated, and unforgiving to enable effective intelligence responses to crises. [FN6] The computerization of communications that has so enriched our capabilities has also facilitated stealth and evasion by those seeking to avoid detection. [FN7] Would-be targets of surveillance are communicating in ways that stress or evade the FISA system. [FN8] Because of the pervasiveness of U.S. telecom switching technology, collection inside the United States is now often the best or only way to acquire even foreign-to-foreign communications that were originally left unregulated by FISA. [FN9] Meanwhile, powerful computers and data-mining techniques now permit intelligence officials to select potential surveillance targets from electronic databases of previously unimaginable size. [FN10] The wholesale quality of this expansive computer collection and data mining is incompatible with the retail scope of the original FISA process. [FN11] Instead of building toward an individual FISA application by developing leads on individuals with some connection to an international terrorist organization, for example, officials now develop algorithms that search thousands or even millions of collected e-mail messages and telephone calls for indications of suspicious activities. [FN12]

At the same time, more Americans than ever are engaged in international communications, and there is far greater intelligence interest in communications to and from Americans. [FN13] Both circumstances increase the likelihood that the government will be intercepting communications of innocent Americans, raising as many questions about the adequacy of FISA safeguards as they do about the adaptability of FISA architecture. This tension forms the context for a series of post-9/11 developments, culminating in the FISA Amendments Act of 2008 (FAA). [FN14]
The FAA codified a procedure to permit broad, programmatic surveillance focused on patterns of suspicious activities and not on a specific individual or the contents of their communications through changes in FISA that overcame the case-specific orientation of the original statute. [FN15] As a result, the FAA also codifies, until December 31, 2012, potentially intrusive electronic surveillance unaccompanied by safeguards to protect personal privacy and free expression. [FN16] The amended FISA also institutionalizes operations that are prone to inaccuracy and chronic overcollection. [FN17] A 2008 decision by the FISA Court of Review (FISCR), [FN18] which upheld the government's implementation of the programmatic procedures of earlier but similar temporary legislation [FN19] by relying on procedures drawn from sources outside FISA, underscores the slapdash development and still-incomplete legal architecture that attends the broad-based programmatic orders. [FN20]

From its beginnings, the overarching FISA question has been how to evaluate and weigh the basic values of security and individual liberties when intrusive electronic surveillance is used to collect foreign intelligence. Modern communications and surveillance technologies have so complicated policy discussions, however, that the values debate has dawned in a sea of misapprehension about the means to implement the policies. [FN21] Meanwhile, FISA has become so complex that the law further occludes informed policy choices. [FN22] The basic architecture of FISA should be recast.

The Constitution continues to provide a baseline. The Fourth Amendment Warrant Clause applies to electronic surveillance conducted for foreign intelligence purposes within the United States if the surveillance involves U.S. persons who do not have a connection to a foreign power. [FN23] FISA now permits such electronic surveillance as the inevitable byproduct of surveillance of unprotected targets, but the Act does little to insulate U.S. persons from the effects of the surveillance. (It is not clear whether the Fourth Amendment Warrant Clause applies to such surveillance when a U.S. person is connected to a foreign power, or when the surveillance of U.S. persons occurs wholly outside the United States. The reasonableness component of the Fourth Amendment does apply in these instances.) [FN24] Historically, our laws have rejected granting discretion for government to undertake intrusive surveillance of individuals without some showing of suspicious activities. [FN25] If the combination of terrorism threats and computerization demands a more nimble capacity to conduct suspicionless electronic surveillance to combat terrorism, the discretion that is necessarily part of that system should be more carefully controlled, either at the point of collection or when the information is maintained or used by the government. Absent such controls, FISA as amended now threatens longstanding Fourth Amendment principles. Apart from its potential constitutional shortcomings, the programmatic surveillance that the FAA permits should be repaired to improve its efficacy. Making the program more efficacious will help make it lawful.

Even before programmatic surveillance was stitched onto FISA, the Act labored under continuing controversies over lowering the wall that separated intelligence from law enforcement investigations [FN26] and the inconsistency of requiring probable cause of foreign agency for targets while permitting surveillance of lone wolves. [FN27] Programmatic surveillance adds considerably to complexity, has already produced implementation problems, and casts doubt on the lawfulness and efficacy of FISA's techniques.

In Part I and Part II of this Article, I will review the FISA model for authorizing surveillance for foreign intelligence purposes and how the combination of evolving technologies and emerging terrorism threats caused FISA to become too unwieldy and inflexible to accommodate the needs for speedy and agile surveillance. In Part III, I will describe how the Bush Administration's Terrorist Surveillance Program (TSP) led to the temporary Protect America Act (PAA), and then to the FAA and the codification of programmatic surveillance. After reviewing a FISCR decision upholding the temporary version of programmatic FISA procedures and taking note of some implementation problems with the FAA in Part IV, in Part V I will suggest some benchmarks for re-
building FISA from the ground up.

The programmatic features are likely here to stay. For legal and policy reasons, these features should be improved. The thirty-year linchpin of FISA targeting—the location, identity, or both, of the target—should be abandoned where it is not known. Instead, applications for programmatic surveillance under FISA should be based on showing that the proposed electronic surveillance is material to an ongoing investigation of international terrorism or clandestine intelligence activities, that alternative investigative techniques are not capable of collecting the information, and that it is likely that conducting the surveillance will provide the information sought.

A second set of reforms should focus on the retention and dissemination of what is collected. Congress should create a standardized system for authorized use of collected information across the Executive Branch. Building on an authorized-use platform, the Department of Justice and the Office of the Director of National Intelligence should develop guidelines that account specifically for the unique dynamics of protecting personal information about U.S. persons that is collected, even inadvertently, in programmatic collection. In addition, where programmatic surveillance is requested, the FISA Court (FISC) should, before and periodically during implementation, review and approve minimization procedures that are tailored to assess the efficacy and impact on privacy, free expression, and security of the mega-collection and data-mining techniques employed. In the aggregate, a combination of administrative safeguards and judicial and congressional oversight that is more robust than what is now required should be built into the programmatic surveillance portion of FISA.

I. The Original Architecture

Until the FAA, FISA governed the electronic surveillance and physical searches only of persons in the United States and only for the purpose of collecting foreign intelligence. [FN28] (FISA did not apply to surveillance or searches conducted outside the United States or to foreign-to-foreign telephone communications intercepted within the United States.) [FN29] "Probable cause" required that a target of the surveillance be a "foreign power," [FN30] an "agent of a foreign power," [FN31] or, since 2004, a "lone wolf" terrorism suspect. [FN32] Applications to the FISC for approval of a search or surveillance had to specify "facilities" where the surveillance would be directed [FN33] and procedures to "minimize" the acquisition, retention, and dissemination of information not relevant to an investigation. [FN34] A special court, the FISC, which meets in secret, was created to hear requests for orders to conduct the surveillance. [FN35]

For a long time the process worked well as a mechanism to regulate surveillance of known intelligence targets. [FN36] The FISA process and its eventual orders have always been limited, however. FISA was concerned with acquisition, not with the uses government might have for what is collected. FISA also assumed that officials know where the target is and what facilities the target will use for his communications. [FN37] Knowing this much enabled the government to demonstrate the required probable cause to believe that the target was an agent of a foreign power or a lone wolf. [FN38] FISA did not authorize intelligence collection for the purpose of identifying the targets of surveillance, or of collecting aggregate communications traffic and then identifying the surveillance target. [FN39] In other words, FISA envisioned case-specific surveillance, not a generic surveillance operation, and its approval architecture was accordingly geared to specific, narrowly targeted applications. [FN40] FISA was also based on the recognition that persons lawfully in the United States have constitutional privacy and free expression rights that stand in the way of unfettered government surveillance. [FN41]

Although the volume of FISA applications increased gradually through the 1990s, [FN42] after 9/11 the pace of electronic intelligence collection quickened, and Bush Administration officials argued that traditional FISA
procedures interfere with necessary “speed and agility.” [FN43] As the pre-9/11 FISA applications doubled to more than 2,000 a few years later, [FN44] the Director of National Intelligence (DNI) complained that more than “200 man hours” are required to prepare an application “for one [phone] number.” [FN45] The system was, it seemed, grinding along, but it was carrying a lot of weight.

II. Technological Stresses on FISA

Meanwhile, with the revolution in digital communications, the idea of a geographic border has become an increasingly less viable marker for legal authorities and their limits. Using the Internet, packets of data that constitute messages travel in disparate ways through networks, many of which come through or end up in the United States. [FN46] Those packets and countless Skype calls and instant messages originate from the United States in growing numbers, and the sender may be in the United States or abroad. [FN47] Likewise, it may or may not be possible to identify the sender or recipient by the e-mail addresses or phone numbers used to communicate. [FN48]

Nor do we think of our international communications as being in any way less private than our domestic calls. Congress apparently exempted from FISA international surveillance conducted abroad because, when FISA was enacted, electronic communications by Americans did not typically cross offshore or international wires. [FN49] Now, of course, we do communicate internationally and our message packets may travel a long distance, even if we are corresponding by e-mail with a friend in the United States who is in the same city. [FN50] The location or identity of the communicants is simply not a useful marker in Internet communications. As former CIA Director General Michael Hayden said, “[t]here are no area codes on the World Wide Web.” [FN51]

Because FISA was written to apply to broadly defined forms of “electronic surveillance” [FN52] acquired inside the United States, digital technologies brought the interception of previously unregulated communications inside the FISA scheme. [FN53] In particular, digitization brought e-mail communications within the FISA scheme. [FN54] Because of the definition of “electronic surveillance,” even a foreign-to-foreign e-mail message could not be acquired from electronic storage on a server inside the United States except through FISA procedures. [FN55] While foreign-to-foreign telephone surveillance was expressly left unregulated by Congress, coverage of e-mail by FISA created an anomalous situation for investigators.

Even an exemption carved out of FISA for foreign-to-foreign e-mail would be problematic because it is often not possible to verify the location of the parties to a communication. [FN56] A broader authorization for e-mail surveillance would inevitably include U.S. person senders or recipients and even wholly domestic e-mail. A foreign-to-foreign e-mail exemption would effectively leave in place the requirement of individual FISA applications for overseas targets using e-mail that rely on an ISP in the United States because government could neither ferret out incoming or outgoing U.S. messages in real time nor ignore those messages. [FN57]

Changing technologies have also turned the traditional sequence of FISA processes on its head. We discovered after 9/11 that investigators could enter transactional data about potential terrorists and come up with a list that included four of the hijackers [FN58]—a sort of reverse of the typical FISA-supported investigation. Now our intelligence agencies see the potential benefits of data mining [FN59]—the application of algorithms or other database techniques to reveal hidden characteristics of the data and infer predictive patterns or relationships [FN60]—as a means of developing the potential suspects that could be targets in the traditional FISA framework. In order to collect the foreign intelligence data, officials claim that they need to access the telecom
switches inside the United States so that they can conduct surveillance of e-mails residing on servers in the United States. [FN61] The mined data would necessarily include data of U.S. persons. [FN62]

III. Programmatic Electronic Surveillance

A. The Terrorist Surveillance Program

After 9/11, President George W. Bush ordered an expanded program of electronic surveillance by the National Security Agency (NSA) that simply ignored FISA requirements. [FN63] In December 2005, the New York Times reported that President Bush secretly authorized the NSA to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without obtaining orders from the FISC. [FN64] Although the details of what came to be called the Terrorist Surveillance Program (TSP) have not been made public, NSA apparently monitored the telephone and e-mail communications of thousands of persons inside the United States where one end of the communication was outside the United States and where there were reasonable grounds to believe that a party to the international communication was affiliated with al Qaeda or a related organization. [FN65]

From subsequent accounts and statements by Bush Administration officials it appears that the TSP operated in stages. [FN66] With the cooperation of the telecommunications companies, the NSA first engaged in wholesale collection of all the traffic entering the United States at switching stations—so-called vacuum cleaner surveillance. [FN67] Second, those transactional data—addressing information, subject lines, and perhaps some message content—were computer mined for indications of terrorist activity. [FN68] Third, as patterns or indications of terrorist activity were uncovered, intelligence officials at NSA reviewed the collected data to ferret out potential threats, at the direction of NSA supervisors. [FN69] Finally, the targets selected as potential threats were referred to the FBI for further investigation, pursuant to FISA, and the human surveillance ended for the others. [FN70]

At first the Bush Administration defended the legality of the TSP vigorously, but it was an uphill struggle. [FN71] In the face of mounting criticism and litigation challenging TSP, the Administration persuaded the FISC to take over supervision of the program. [FN72] Presumably within the statutory parameters of FISA. When the FISC took over administration of the TSP program in January 2007, Attorney General Alberto Gonzales advised that a FISC judge “issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization.” [FN73] According to the Attorney General, all surveillance that had been occurring under the TSP would now be conducted with the approval of the FISC. [FN74]

Although the legal basis for fitting TSP inside FISA during this period has not been disclosed, the government must have persuaded at least one FISC judge to treat the international telecom switches as FISA “facilities.” [FN75] Because it could reasonably be argued that al Qaeda was using the switches for communications entering and leaving the United States, a few FISC orders gave the government access to nearly all of the international telecom traffic entering and leaving the United States. [FN76] The fact that the rest of us were using those switches at the same time was, presumably, dealt with through some version of FISA minimization procedures, where Executive Branch personnel would call what looked like al Qaeda communications from the
mass of data. [FN77]

B. The Protect America Act of 2007

A different FISC judge decided in April 2007 not to continue approval of what had been the TSP under FISC supervision, and apparently determined that at least some of the foreign communications acquired in the United States pursuant to the program are subject to individualized FISA processes. [FN78] After a backlog of FISA applications developed, the Bush Administration successfully persuaded Congress to pass statutory authorization for programmatic surveillance outside the case-specific FISA processes. [FN79]

The Administration emphasized the need to amend FISA to account for changes in technology and thus enable it to conduct surveillance of foreign digital communications from within the United States. [FN80] Yet providing statutory access to U.S. digital telecommunications switches would enable NSA to access e-mail traffic traveling to or from U.S. servers, thus opening up a vast swath of U.S. person communications for government scrutiny. [FN81]

As enacted in August 2007, the Protect America Act determined that the definition of “electronic surveillance” in FISA would not apply to surveillance of a person reasonably believed to be outside the United States. [FN82] The PAA also permitted the Director of National Intelligence and the Attorney General to authorize collection of foreign intelligence from within the United States “directed at” persons reasonably believed to be outside the United States, without obtaining an order from the FISC, even if one party to the communication was a U.S. citizen inside the United States. [FN83] Because a FISA “person” may include groups or foreign powers, [FN84] surveillance “directed at” al Qaeda permitted warrantless surveillance of the telephones and e-mail accounts of any U.S. person if the government was persuaded that the surveillance was directed at al Qaeda. [FN85]

The PAA thus made less onerous the determination that the target is known to be abroad. Comparing the PAA to the TSP (as characterized by Attorney General Gonzales), the main differences were that the TSP allowed surveillance of targets inside the United States, and the predicate for collection authority under the PAA was the location of the target, not his status in relation to a foreign power or terrorist organization (as it was under the TSP). [FN86]

C. The FISA Amendments Act of 2008

The PAA expired by its own terms in February 2008 after Congress and the Administration failed to agree on a set of provisions that would grant broad, retroactive immunity to telecommunications firms that participated in the TSP. [FN87] The FISA Amendments Act of 2008, enacted in July 2008, conferred the immunity sought by the Administration and the telecommunications industry. [FN88] and it authorized until December 31, 2012, sweeping and suspicionless programmatic surveillance from inside the United States. [FN89]

In essence, the FAA codified the PAA—with some additional wrinkles. The core of the new subtitle of FISA retains the broad-based authorization for the Attorney General and DNI to authorize, jointly, for a period up to one year, the “targeting” of non-U.S. persons “reasonably believed to be located outside the United States to acquire foreign intelligence information.” [FN90] The FISC does not review individualized surveillance applications, and it does not supervise implementation of the program. [FN91] The FAA does prohibit the government
from "intentionally target[ing] any person known at the time of acquisition to be located in the United States." [FN92] However, the government cannot reliably know a target's location, nor often the target's identity. [FN93] These uncertainties, combined with the fact that the targeted person may communicate with an innocent U.S. person, mean that the authorized collection may include the international or even domestic communications of U.S. citizens and lawful residents.

Under the FAA, the Attorney General submits procedures to the FISC by which the government will determine that acquisitions conducted under the program meet the program targeting objectives and satisfy traditional FISA minimization procedures. [FN94] Although the procedures are classified, we know that they are designed to limit the acquisition, retention, and dissemination of private information acquired during an investigation. [FN95] The application to the FISC must also contain a certification and supporting affidavit, [FN96] and “targeting procedures” designed to ensure that collection is limited to non-U.S. persons reasonably believed to be outside the United States and to prevent the intentional acquisition of communications where the sender and all known recipients are known at the time to be located in the United States. [FN97] The certification and supporting affidavit must state that the Attorney General has adopted “guidelines” to ensure that statutory procedures have been complied with, that the targeting and minimization procedures and guidelines are consistent with the Fourth Amendment, and that a significant purpose of the collection is to obtain foreign intelligence information. [FN98]

As with the PAA and the TSP, the FAA does not limit the government to surveillance of particular, known persons reasonably believed to be outside the United States, but instead authorizes so-called “basket warrants” for surveillance and eventual data mining. In addition, non-U.S. person targets do not have to be suspected of being an agent of a foreign power nor, for that matter, do they have to be suspected of terrorism or any national security or other criminal offense, so long as the collection of foreign intelligence is a significant purpose of the surveillance. [FN99] Potential targets could include, for example, a non-governmental organization, a media group, or a geographic region. That the targets may be communicating with innocent persons inside the United States is not a barrier to surveillance. [FN100]

For the first time, surveillance intentionally targeting a U.S. citizen reasonably believed to be abroad is subject to FISA procedures. [FN101] As a practical matter, this increased protection for Americans may be illusory. The government may not target a particular U.S. person's international communications pursuant to its programmatic authorizations, whether the person is in the United States or abroad. [FN102] Yet officials could authorize broad surveillance, for example, of all international communications of the residents of Detroit on the rationale that they were targeting foreign terrorists who may be communicating with persons in a city with a large Muslim population.

Unlike traditional FISA applications, the government is not required to identify the facilities, telephone lines, e-mail addresses, places, or property where the programmatic surveillance will be directed. [FN103] Under the FAA, targeting might be directed at a terrorist organization, a set of telephone numbers or e-mail addresses, or perhaps at an entire ISP or area code. [FN104] After a FISC judge approves the program features, [FN105] Executive Branch officials authorize the surveillance and issue directives requesting (or, through an additional court order, compelling) communications carriers to assist. [FN106] Although details of the implementation of the program authorized by the FAA are not known, a best guess is the government uses a broad vacuum-cleaner-like first stage of collection, focusing on transactional data, where wholesale interception occurs following the development and implementation of filtering criteria. Then NSA engages in a more particularized collection of content after analyzing mined data. [FN107]
Incidental acquisition of the communications of U.S. persons inside the United States inevitably occurs due to the difficulty of ascertaining a target's location and because targets abroad may communicate with innocent U.S. persons. [FN108] The FAA does nothing to assure U.S. persons whose communications are incidentally acquired that the collected information will not be retained by the government.

Historically, minimization has been conducted during law enforcement investigations to protect against the acquisition of private information unrelated to the purpose of the criminal investigation. [FN109] The protection of civil liberties through minimization during law enforcement surveillance occurs up front rather than during retention or dissemination in part because electronic surveillance during traditional law enforcement investigations is episodic and short term. Even with traditional FISA electronic surveillance, the authorization is broader and allows for continuous and longer term monitoring, with the understanding that information irrelevant to the investigation will be collected. [FN110] Thus, according to a 2002 opinion of the FISC, [FN111] the government conducts FISA minimization after processing (including transcription, translation, and analysis), and the retained foreign intelligence enters an indexed storage system for retrieval. [FN112] In explaining the minimization challenges inherent in foreign intelligence surveillance, the FISC opined in 2002, "[g]iven the targets of FISA surveillance, it will often be the case that intercepted communications will be in code or a foreign language for which there is no contemporaneously available translator, and the activities of foreign agents will involve multiple actors and complex plots." [FN113] In addition, unlike the targets of FISA surveillance, Title III targets eventually receive notice that they have been subject to surveillance. They may sue for Fourth Amendment violations, seek to suppress the evidence in a prosecution, or both. [FN114] Traditional FISA minimization protects only nonpublic information concerning U.S. persons who have not consented to acquisition, retention, or dissemination of their personal information, [FN115] and FISA permits the government to retain all information that could be considered foreign intelligence. [FN116]

The generic FISA minimization requirements were not modified in the FAA to accommodate the surveillance of individual targets through programmatic surveillance. [FN117] The FAA requires that the Attorney General and the DNI certify that minimization procedures have been or will be submitted for approval to the FISC prior to, or within seven days following, implementation. [FN118] However, the FISC does not review the implementation of minimization procedures or practices for the programmatic surveillance it approves, and FISA permits the government to retain and disseminate information relating to U.S. persons so long as the government determines that it is "foreign intelligence information." [FN119] By implication, the government may compile databases containing foreign intelligence information from or about U.S. persons, retain the information indefinitely, and then search the databases for information about specific U.S. persons.

Viewing minimization as it evolved from Title III to traditional FISA and to the FAA, the original objective—preventing the collection, retention, or dissemination of private information—has been seriously compromised, or so it seems from the public record. The combination of allowing the government to use the foreign intelligence trump card to hold or disseminate information and the lack of judicial oversight of how private communications are filtered out leaves the minimization mechanism short of meeting its goals for programmatic FISA surveillance. Because FISA minimization is already focused on retention and dissemination and not on acquisition, it should be relatively easy to reform FAA minimization to insert controls on executive discretion and assign a monitoring function to the FISC.

The FISC has described its role in authorizing and reviewing surveillance conducted under the FAA as "narrowly circumscribed." [FN120] The FISC must approve an order for programmatic surveillance if it finds that the government's certification "contains all the required elements," [FN121] that the targeting procedures
are “reasonably designed” to target non-U.S. persons, [FN122] and that the targeting and minimization procedures are consistent with the FAA and the Fourth Amendment. [FN123] The FISC does not supervise the implementation of the targeting and thus does not review the efficacy of specific surveillance targets.

Long-term congressional authorization for programmatic surveillance marks a stark change in FISA. The FAA permits collection without any showing of individualized suspicion (except for U.S. persons targeted abroad) even where collection of U.S. citizens' communications is the foreseeable consequence of the program orders. [FN124] It may be that individualized FISA applications and their foreign agency or lone-wolf probable-cause determinations are relics of the pre-digital age. Congress and the Executive Branch should confront the realities of digital surveillance and develop approval procedures, minimization safeguards, and judicial and legislative oversight mechanisms to govern the use of data mining and related surveillance techniques to better insure that programmatic surveillance protects our security and our liberties.

IV. Implementation of Programmatic Surveillance

A. The Directives Decision

On January 15, 2009, the FISCR made public portions of its August 22, 2008, decision, In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act. [FN125] In Directives, the FISCR upheld the constitutionality of directives in pursuit of programmatic surveillance issued to an unnamed telecommunications company pursuant to the temporary Protect America Act. [FN126] Because the FAA follows the basic thrust of the PAA, the opinion foreshadows the court's view of the now-codified procedures for programmatic surveillance. The telecom followed a statutory provision and challenged orders compelling it to assist with the acquisition of foreign intelligence where the target was a U.S. person reasonably believed to be outside the United States. [FN127] The orders were made following a joint determination by the DNI and the Attorney General that the acquisition satisfied a series of criteria, including minimization procedures. [FN128]

In its heavily redacted opinion--only the second one publicly issued in its thirty year history--the FISCR held that there is a foreign intelligence exception to the Fourth Amendment warrant requirement, based on the “special needs” doctrine, at least in the “defined context” of cooperation directives to a telecom company. [FN129] The exception is available for the programmatic purpose of the surveillance because the acquisition goes “beyond ordinary crime control” and foreign intelligence surveillance about “overseas foreign agents” is “particularly intense.” [FN130] Fourth Amendment reasonableness was met in this case through a variety of safeguards found outside the statute. The telecom argued that the collection activities would inevitably lead to incidental collection from nontargeted U.S. persons, but, without further explanation or support, the FISCR characterized the concern as “overblown.” [FN131] If incidental, said the court, the collections do not violate the Fourth Amendment. [FN132]

Relying on the FISCR’s own 2002 In re Sealed Case decision, [FN133] the telecom argued that the procedural protections provided by the FAA were insufficiently analogous to protections found in the earlier version of FISA, including a particularity requirement, prior judicial review for probable cause of foreign agency, and proxies for any omitted protections. [FN134] Despite the absence of these protections, in its 2008 decision the FISCR supported the government’s contention that Fourth Amendment reasonableness could be constructed from:
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. [FN135]

The FISCR concluded that the telecom presented no evidence of harm in this instance. According to the court, particularity and prior judicial-review concerns are "defeated by the way in which the statute has been applied." [FN136] According to the court, classified procedures approved by the Attorney General, when "combined with the PAA's other protections," and those provided in the Executive Order "are constitutionally sufficient compensation for any encroachments." [FN137] The next two subsections evaluate the court's Fourth Amendment analysis.

1. Special Needs.--The special-needs doctrine is a limited exception to the Fourth Amendment warrant requirement. It grew out of searches or surveillance as part of programs that were developed for purposes other than enforcing the criminal laws--searches for drugs in school lockers or immigration checkpoints at our nation's borders, for example. [FN138] To invoke the doctrine, the government must show that the primary purpose of its surveillance is something other than law enforcement and that following the warrant and probable cause requirements is impracticable. [FN139] If the special needs are accepted, the result is to exempt searches or surveillance authorized by the program from the warrant requirement, leaving reasonableness alone as the more general Fourth Amendment measure.

Following the USA PATRIOT Act amendments to FISA in 2001, the FISCR relied in part on the special-needs doctrine to uphold Department of Justice guidelines that permitted criminal investigators to assume lead roles in FISA-authorized surveillance so long as "a significant purpose" of the investigation included collecting foreign intelligence. [FN140] Arguably the special-needs doctrine should not have been applied in the traditional FISA setting to justify individually targeted electronic surveillance after the "significant purpose" amendment in 2001. [FN141] Although intelligence and law enforcement investigations often overlap in pursuit of national-security or counterterrorism targets, law enforcement officials may exploit the more government-friendly FISA processes and avoid traditional law enforcement rules for securing a warrant when they, and not intelligence investigators, are in charge of an investigation and, from the beginning, are working to build a case for prosecution. [FN142]

In any case, following the 2002 In re Sealed Case FISCR decision, the amended statute has been construed to permit the government to engage in "special needs" surveillance when the overriding objective of the surveillance is to gather evidence for prosecution. [FN143] The "significant purpose" qualifier applies to programmatic surveillance authorized under the FAA. [FN144] The use of programmatic surveillance to build a criminal case, such as a large criminal conspiracy, is at least as likely in these instances as in individual FISA applications. Although I continue to doubt the wisdom and lawfulness of the "significant purpose" standard, in the last section of the Article, I propose to accept programmatic surveillance for foreign intelligence as a "special needs" category so long as a series of safeguards are embedded in the system, including a review to assess the importance of the foreign intelligence objective of the surveillance.

2. Reasonableness.--The substitutions of individualized FISC review of applications for a traditional warrant and a specialized foreign intelligence related probable cause standard have been construed by nearly every court that has considered their constitutionality as adequate for Fourth Amendment purposes. [FN145] The programmatic orders are so dramatically different from the thirty-year FISA experience, however, that their suspicionless targeting procedures may not be reasonable in Fourth Amendment terms.
In the circumstances of foreign intelligence surveillance designed to counter threats of terrorism and to protect the national security, it is no longer realistic to argue that the Warrant Clause and its traditional law enforcement warrants and the criminal law version of probable cause should apply in the foreign intelligence context, at least where the government demonstrates that the foreign intelligence sought is important to an ongoing counterterrorism investigation and that it is impractical to seek a warrant. As such, the FISCR holding in Directives that there is a foreign intelligence exception to the Warrant Clause is not particularly important. Yet the wooden and pasted-together quality of the court’s reasonableness analysis is unfortunate, particularly since reasonableness is the only remaining Fourth Amendment criterion for assessing the programmatic surveillance.

The court purported to make a fact-based decision about reasonableness, as applied to the telecom and the directive it was issued. [FN146] Ironically, reasonableness was constructed by the court in part from minimization, but we have no idea what the minimization entailed. The facts are opaque due to classification and, whatever they reveal, are based on generic authorization for collection of personal information, on targeting procedures that may significantly overcollect U.S. person information, and are developed solely by the government without opportunity for adversarial testing. The FISCR must have recognized that it was working with especially limited statutory criteria for reasonableness. As a result, the FISCR reached outside the FAA to an executive order and an affidavit and relied on the assumed good faith of the implementers in deciding that there were adequate protections for the telecom. [FN147]

As an illustration that challenges to electronic surveillance in the foreign intelligence realm should not excuse a thorough reasonableness review, a panel of the Second Circuit affirmed several convictions in the Africa Embassies bombings prosecutions after a much more fulsome and thoughtful assessment of the Fourth Amendment. [FN148] While the Second Circuit panel began with similar “totality of the circumstances” and balancing quotes from landmark precedents cited by the FISCR, [FN149] its analysis carefully probed the factual record. Concerning the telephone surveillance conducted as part of the investigation of the bombings, the court found significant privacy invasions during the year-long surveillance, accompanied by limited efforts at minimization. [FN150] In balancing the intrusion against the government's need to conduct electronic surveillance, the court took into account: the difficulties of pinpointing surveillance of diffuse organizations like al Qaeda; the problems inherent in sorting through much irrelevant information in pursuit of foreign intelligence; the tendency of organizations such as al Qaeda to communicate in code; and the need to sift through foreign languages in finding relevant intelligence. [FN151] No similar fine-grained analysis accompanied the FISCR Directives decision.

The FAA enables the government to overhear Americans' most intimate conversations, for periods up to one year, and there is no judicial gatekeeper of administrative discretion—the agencies decide which communications to monitor. Where targeting and minimization requirements monitored by the FISC help show reasonableness in the traditional FISA setting, programmatic FISA surveillance leaves targeting and minimization so unbounded that the two features do little to assure Fourth Amendment reasonableness. Reasonableness requires a careful evaluation of the government's conduct, and neither the FAA nor the Directives opinion contain the necessary review.

One rejoinder to the Directives court's scattershot construction of reasonableness is that Congress improved the scheme in enacting the permanent FAA one year later by requiring probable cause of foreign agency for surveillance targeting U.S. persons abroad or intentional targeting of U.S. persons domestically. [FN152] Still, incidental collection of U.S. person communications inside the United States was not addressed by the FAA, and the Directives decision does not assess the reasonableness of such collection.
The FISCR conclusion that “incidental collections occurring as a result of constitutionally permissible ac-
quisions do not render those acquisitions unlawful” [FN153] faithfully parrots Fourth Amendment doctrine
[FN154] but fails to respond to the unique circumstances of programmatic FISA surveillance. Viewing the public
record in the Directives case, it is impossible to know to what extent the telecom had shown harmful effects
of incidental collections. In any case, the FISCR did not acknowledge just how significant an intrusion the “incidental”
collection could be.

B. Implementing the FAA

A lawsuit filed by the ACLU challenging the constitutionality of the FAA was dismissed on standing
grounds in August 2009. [FN155] Meanwhile, following a periodic review of the procedures and directives im-
plemented following enactment of the FAA, the Justice Department and DNI reported to the FISC in April 2009
that the NSA had been engaging in significant and systematic overcollection of the domestic e-mail messages of
Americans. [FN156] Though apparently inadvertent, the lapses were headline news and prompted congressional
investigations. [FN157] Unsurprisingly, as the NSA uses telecom switching stations and its satellites to intercept
millions of messages, one apparent cause of the overcollection of domestic e-mail messages is the ongoing diffic-
ulty of determining the location of the surveillance target. [FN158]

As investigations were launched, some members of Congress disputed the contention that the overcollection
was inadvertent. [FN159] Representative Rush Holt, D-N.J., Chair of the House Select Intelligence Oversight
Committee, worried that “the people making policy don’t understand the technicalities.” [FN160] Intelligence
officials told the New York Times that the NSA exceeded its statutory authorities in implementing eight to ten
separate orders issued by the FISC since enactment of the FAA. [FN161] Because each order could permit col-
clection of hundreds or thousands of phone numbers or e-mail addresses, millions of individual communications
could have been intercepted, some portion of which would have been domestic communications by U.S. per-
sons. [FN162]

V. Benchmarks for Reform

A. Revising Targeting

“If the government genuinely cannot determine a person’s location, it makes no sense to use geography as a
trigger for FISA’s warrant requirements.” [FN163]

One problematic feature of the FAA is, notwithstanding all the amendments to FISA over the years, that the
legislation follows the thirty-year FISA model of focusing on targets and their location for the purposes of au-
thorizing and conditioning surveillance and data collection. From the government’s perspective, the disadvant-
age of relying on the location of the target as a basis for conducting lawful surveillance was mitigated when the
FAA changes provided that the government had only to reasonably believe that the target is abroad. [FN164] How-
ever, one inevitable problem with the relaxed standard is that, given the unreliability of the location identi-
fier, more warrantless surveillance of persons inside the United States will occur.

The technical problems of knowing an individual’s location when an electronic communication is sent or re-
ceived may also be lessened when implementing FAA surveillance through an expansive interpretation of the

FISA definition of “person.” The term is broad enough to include diffuse non-state groups such as al Qaeda. [FN165] The “reasonably believe” standard presumably may be met because, at any one time, some persons affiliated with al Qaeda may be in the United States and some may be abroad; some may be U.S. persons and some may not.

In place of these workarounds, it is time to replace location of a target as a marker for regulation. Just as our national security interests and threats transcend borders, our personal liberties, including free expression and privacy, are expressed globally. If neither security nor personal freedoms are advanced by adhering to the traditional dividing line that prescribes authorities for warrantless electronic surveillance, it is time to find another approach.

One problem, of course, is that foreigners abroad are consumers of U.S. cyberspace. When corresponding with another foreigner, these persons are unprotected by the Fourth Amendment if they lack other ties with the United States. [FN166] There is no reason to limit our intelligence agencies in surveillance of those communications, and the FAA facilitates that collection. Yet if we unleash surveillance at U.S. switches, our laws and policies have not yet devised a way to prevent them from gaining access to the everyday communications of Americans, the dominant consumers of those switches.

I agree with Orin Kerr that much modern surveillance is “data-focused rather than person-focused.” [FN167] I also agree with Fred Cate that “[t]he absence of a legal regime governing data mining not only fuels privacy concerns, but also runs the risk of compromising the very objectives that data mining is designed to serve.” [FN168] Where location, identity, or both of a target are unknown, I, like Kerr, recommend a predicate for surveillance that focuses on the nature of the information sought. Whether the electronic surveillance technique consists of collection followed by data mining or collection accompanied by filtering, and whether the information collected is characterized as “terrorist intelligence information,” as Kerr labels it, [FN169] or foreign intelligence that bears directly on important national-security or counterterrorism objectives, [FN170] the government should be permitted to conduct warrantless electronic surveillance if it can demonstrate in advance to the FISC that the information cannot be obtained through a less intrusive means and that it likely will collect what is sought.

Another approach would provide a uniform standard for any collection technique that would require a Fourth Amendment warrant if undertaken for law enforcement purposes in the United States. [FN171] Following the current FAA, FISC approval would be required, subject to a probable cause showing that the surveillance will reveal the information sought, if a U.S. person is targeted for FISA surveillance anywhere, if a target is known to be in the United States, or if officials know in advance that a communication is wholly domestic. [FN172] All other categories of collection could be authorized by Executive Branch officials. Collection of non-content information, such as addressing information, would be permitted after administrative review to ascertain that the collection is material to an ongoing investigation of international terrorism or in pursuit of clandestine intelligence. Electronic surveillance of the contents of communication of other categories of targets could be administratively approved following a showing of probable cause that the collection is material to an ongoing investigation of international terrorism or in pursuit of clandestine intelligence, that the information cannot be obtained through a less intrusive means, and that it is likely that the surveillance technique proposed will collect the information. [FN173] These or similar reforms could eliminate the “agent of a foreign power” and “lone wolf” categories altogether.
B. What Happens with the Collected Data?—Minimization and Related Issues

We believe the retention and use by IC organizations of information collected under . . . FISA should be carefully monitored. [FN174]

While simplifying the basic targeting and presurveillance approval requirements will improve the overall FISA scheme, so much would be left to the discretion of unelected officials that FISA collection reforms should also focus on postcollection controls. The quotation above from the Inspectors General of DOD, DOJ, CIA, NSA, and ODNI is taken from the conclusions of their report on Bush Administration surveillance activities. [FN175] Following their lead, minimization should be enhanced for programmatic surveillance to make less likely the misuse of the massive collection of personal information about U.S. persons. Whether or not Fourth Amendment jurisprudence recognizes the collected information as part of our reasonable expectation of privacy, [FN176] Congress should impose limits on the retention, use, and dissemination of the information collected through FISA programmatic orders or directives.

Every FAA decision bearing on specific intelligence targets is made by Executive Branch officials and is not subject to review by the FISC or another judge. [FN177] Prior identification of targets to a judge protects innocent third parties from being swept up in the surveillance and enforces the hallmark predicate for government surveillance—individualized suspicion. [FN178] The breadth of FAA orders and determinations permits vacuum-cleaner-like collection from telecom switches, for example. [FN179] Once collected, executive officials cull through the data in pursuit of suspicious indicators that merit further investigation. [FN180] False positives are one inevitable result. Another is the potential for abuses of stored data. [FN181]

How do officials determine to look more closely at individualized pieces of the traffic? Apparently NSA uses algorithms that purport to identify terrorist suspects out of the vacuumed mass of data. [FN182] How exactly could such a data-driven process sort the innocuous call to me from my Muslim friend abroad from one that is worthy of further investigation? Is the limited, follow-on surveillance performed by humans then a minimal intrusion that we should be prepared to accept if we are assured that the brief surveillance will end and a traditional FISA application would follow if further electronic surveillance is deemed worthwhile? [FN183]

Under traditional, individualized FISA processes, “specific procedures” for minimization must be promulgated by the Attorney General and filed with the FISC for every individual target, “to minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning unconsenting U.S. persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.” [FN184] The case-specific procedures are classified. [FN185] In these cases, the minimization itself is supervised by the FISC during the course of surveillance, [FN186] and the court may modify the procedures and order that the modified procedures be followed if it finds that the proposed procedures do not satisfy the FISA definition. [FN187]

By focusing on what the collected information may be used for, FISA and the FISC, until the FAA, provided a useful, albeit opaque, mechanism to ensure the accountability of the collection scheme. To be sure, the government could use and disseminate information about a person who was not the target of the approved surveillance, but whose information was collected inadvertently. [FN188] In addition, the “consistent with” clause provides a hedge for the government to disclose to law enforcement officials or, presumably, to anyone else foreign intelligence information. [FN189] Indeed, in discussing the retention stage of minimization, the publicly released 2002 FISC opinion quotes the following standard from the Justice Department Standard Minimization Procedures for U.S. Person Agent of a Foreign Power: “communications of or concerning United States persons
that could not be foreign intelligence information or are not evidence of a crime . . . may not be logged or summarized." [FN190] Because minimization "is required only if the information 'could not be' foreign intelligence," [FN191] the standard is already extremely friendly to the government.

By its nature, the FAA shifts nearly all the burden of civil liberties protection to postcollection minimization, and there is no publicly known mechanism for tailoring minimization to these new conditions. Executive Branch personnel select which communications are retained and, thus, logged and indexed in some way for ease of retrieval, all without judicial supervision. [FN192] Relying on the default requirements, by following FAA minimization procedures the government could compile databases of collected information, maintain them, and search them later for information about U.S. persons. [FN193]

Minimization requirements should be reviewed alongside the predictive abilities of the data-mining methods employed in programmatic surveillance. [FN194] In 2008, a committee of the National Research Council found that "automated identification of terrorists through data mining is neither feasible as an objective nor desirable as a goal of technology development efforts." [FN195] Apart from the serious privacy intrusions that are an incident of data mining, the committee found that the questionable quality of the data in countering terrorism (in countering terrorism, much of the information collected is unreliable or has unclear meaning), [FN196] its propensity to lead to false positives, the vulnerability of data mining to countermeasures, and the paucity of scientific evidence supporting data mining argue that, at most, the techniques should be used as a "preliminary screening method for identifying individuals who merit additional follow-up investigation." [FN197] Employed only as a "preliminary screening method," [FN198] "any information-based counterterrorism program of the U.S. government should be subjected to robust, independent oversight." [FN199] For programmatic surveillance pursuant to FISA, their recommendation translates into rigorous minimization focused on retention and dissemination, supervised by the FISC.

The National Research Council acknowledged that traditional minimization "has been rendered largely irrelevant in recent years as technology and applications have evolved so that vast streams of data are recorded and stored, rather than just limited, relevant elements. . . . Even irrelevant data are routinely retained by the government indefinitely." [FN200] The Council recommends that "[w]henever practicable" personal identifying information should be "removed, encrypted, or otherwise obscured" [FN201] before retention or dissemination.

Whether or not required by the Fourth Amendment, minimization that protects against undue retention and dissemination would serve the particularity values that have long been central to Fourth Amendment reasonableness. Since 1976, the Supreme Court has held that there is no reasonable expectation of privacy in data held by a third party. [FN202] Courts haveReasoned that, by transferring the information to a third party, such as a bank, phone company, or ISP, the consumer has no reasonable expectation of privacy that prevents the company from sharing the information with the government. [FN203] The evolving third-party-records doctrine has, in turn, provided the legal basis for a variety of law enforcement and national security-related data-collection schemes by the government, including collection authorized by FISA. [FN204]

Because data mining and its techniques are employed after collection, the Fourth Amendment may not control what government does to use or store the collected information. [FN205] Although there are signs that some courts are beginning to question the efficacy of the third-party doctrine in the context of data mining for national-security and counterterrorism purposes, [FN206] a reversal of the Supreme Court rule is unlikely anytime soon. [FN207] Nor would a judicial reversal respond to the shortcomings in regulating data mining for foreign intelligence purposes. [FN208] Instead, Congress and investigating agencies should adopt controls on the use of
data mining for foreign intelligence purposes.

During the pre-enactment hearings on FISA more than thirty years ago, Congress recognized that there are “a number of means and techniques which the minimization procedures may require to achieve the purpose set out in the definition.” [FN209] The FISA practice of retaining foreign intelligence has relied on selective logging and indexing of information. [FN210] The FISC, in its 2002 In re All Matters opinion, closely examined the retention stage, and concluded that the critical determination is when “a reviewing official, usually an FBI case agent, makes an informed judgment as to whether the information seized is or might be foreign intelligence information related to clandestine intelligence activities or international terrorism.” [FN211] If the case agent decides that there is no foreign intelligence information in what is being reviewed, minimization would leave the recorded information off the indexing table: “if recorded[,] the information would not be indexed, and thus become non-retrievable[,] if in hard copy[,] from facsimile intercept or computer print-out[,] it should be discarded[,] if on re-recordable media[,] it could be erased[,] or if too bulky or too sensitive, it might be destroyed.” [FN212] Over time, criminal appeals where FISA surveillance was alleged to have been conducted unlawfully revealed that minimized information may nonetheless have been recorded and not destroyed and may remain in some electronic format available for retrieval. [FN213] In programmatic surveillance, NSA personnel likely substitute for the FBI case agent. [FN214] The magnitude of the minimization corpus has changed so much that guidelines for ferreting out material to be minimized and for administrative review of retention decisions should be promulgated.

In a September 2007 letter to the House Intelligence Committee, the Civil Liberties Protection Officer for the ODNI explained that minimization procedures then in place at NSA, while not identical to those used for the PAA or FAA, “provide[d] general guidance for the types of processes and requirements involved with minimization.” [FN215] Summarizing a declassified version of United States Signals Intelligence Directive 18 (USSID 18), the letter notes that U.S. person communications “may generally only be retained in raw form for a maximum of five years, unless there is a written finding that retention for a longer period is necessary to respond to a foreign intelligence requirement;” [FN216] identities of U.S. persons “are generally redacted . . . and replaced with generic terms”; [FN217] and U.S. person identities may be released if “necessary to understand foreign intelligence information or assess its importance.” [FN218] The letter emphasizes that, in addition to the ODNI office, internal oversight of minimization is provided by the National Security Division at DOJ and the Office of General Counsel at ODNI. [FN219]

In its PAA minimization procedures, discussed by NSA in answering questions from the Intelligence Committees and released following a FOIA request, NSA acknowledged that minimization is “not an exact science,” and yet “analysts over time develop an excellent working knowledge of their targets,” thus making mistakes in collecting foreign intelligence less likely. [FN220] Reading between the redactions in the declassified answers, it is impossible to obtain a clear picture of minimization practice. NSA does object to codifying minimization procedures “because it can be difficult to change a statute if the procedures need to be changed in order to meet operational needs,” and it notes that NSA “has established extensive compliance mechanisms” to meet PAA requirements, all of which are subject to oversight and review by the NSA SIGINT Directorate Office of Oversight and Compliance, the Office of Inspector General, and the Office of General Counsel, in addition to the ODNI and DOJ. [FN221] While the limited transparency afforded by the ODNI letter and NSA procedures and responses to the Intelligence Committees’ questions promises continuing oversight, these documents do not provide substantive administrative safeguards, much less legislative standards, which would more effectively protect civil liberties following programmatic surveillance.
The most facile means for minimization prior to dissemination pursuant to FISA has been simply to redact U.S. person names and identifiers. [FN222] In the few settings prior to the FAA where the Attorney General could authorize surveillance without advance FISC approval, there had to be “no substantial likelihood” that the acquisition would reach “the contents of any communication to which a United States person is a party.” [FN223] Because Congress recognized that U.S. person-communications collection could nonetheless occur in those situations, minimization required that none of the contents of such a communication could be disseminated “for any purpose or retained for longer than 72 hours” without a court order or an Attorney General determination that the information “indicates a threat of death or serious bodily harm to any person.” [FN224] Although these steps were contemplated for surveillance undertaken without any prior FISC involvement, the limited role that the court plays in approving programmatic surveillance suggests that requiring a court order for dissemination of information about U.S. persons within days of collection through programmatic surveillance may serve the minimization objectives.

In its third report on improving information sharing, [FN225] a Markle Foundation Task Force recommended responding to the problems of sharing too much or too little information with a government-wide authorized-use standard that “would improve the access, sharing, use, and protection of relevant information legally in the government’s possession while protecting privacy and civil liberties.” [FN226] In addition to recommending the use of anonymization technology to enable information analysis without disclosure of personal identifying information, the Task Force recognized the need to balance potentially competing gods to account for the sensitivities of U.S. persons, while permitting information sharing to occur in a timely fashion. [FN227] For information collected that is not about U.S. persons or is not personally identifiable, authorized use could be automatically generated by the digitized system. [FN228]

For such personal information about U.S. persons as is included in information proposed for use or dissemination, the requester would be required to “articulate a more specific authorized use to access that information . . . to meet a higher standard of care and need.” [FN229] In other words, permission to use the information would be based on the nature and timing of the threat or mission at issue in an investigation. The authorized-use system would be set up so that “the more sensitive the information, the higher the required authorized use, the stricter the audit, and potentially, the greater the need for an official to consider approval for deanonymization.” [FN230] Under authorized use, auditable records would be maintained for each dissemination, and audits and other forms of monitoring would be utilized to ensure enforcement of authorized use. [FN231]

New legislation would prescribe the framework for an authorized-use system, and the Executive Branch would develop agency-specific guidelines or regulations to implement authorized use subject to the agency requirements and to specific legal authorities that apply to the agency’s processes. [FN232] The process for creating the guidelines or regulations should be as transparent as possible and it should include privacy and civil liberties officers from the agencies, review by the Privacy and Civil Liberties Oversight Board, and then final approval by the President. [FN233] For programmatic FISA surveillance, the guidelines should formalize standards of care and need for the retention and use of U.S. person information inadvertently collected, and they should require FISC approval of the guidelines and of dissemination decisions where personally identifiable information about individual U.S. persons would be transferred. Anonymization of U.S. person information should be required wherever possible, consistent with lawful surveillance objectives. The guidelines should also specify audit procedures, and the procedures and audit reports should be reported to Congress.

VI. Conclusion
When I first became a student of FISA, more than twenty years ago, I struggled to understand when a friend who worked inside the FISA process told me that we should worry less about what is collected and how and more about how what is collected is used. Eventually I learned about the importance of the now-lowered wall that separated foreign intelligence from law enforcement and about how minimization could protect private information.

Meanwhile the digital revolution and our data-driven society resulted in private industry having access to personal identifying information about most Americans. The constitutional and statutory law grew up around the premise that our voluntary sharing of that personal information with our credit card companies, ISPs, and banks eliminated any reasonable expectation of privacy in that information. When the government more prominently and aggressively began collecting and then mining that stream of data, especially after September 11, only a few limits were set on its use. Yet, when the TSP was exposed based on the same techniques, there was widespread condemnation of the Bush Administration. Why?

Part of the reason is that Americans did not know that the government could be listening in on or viewing their international telecommunications traffic, incoming and outgoing, and we feared that our conversations and e-mails were being monitored by someone at NSA. Once we learned more about the program, we also feared that officials were continuing to monitor our communications without probable cause and without the approval of any judge.

As we learned more about TSP and its follow-on iterations, as authorized by the FISC and then Congress, it became clear that the more significant privacy intrusion occurs not at the initial stage of flagging our calls or e-mails, but at the point when someone, looking at aggregate data for patterns or suspicious activity, decides to personally review an individual's communications. In other words, we should be worried more about what the data is used for, not so much that it is collected.

Although information sharing has been a mantra in recent years, and curtailing the uses of collected data cuts against sharing, important reasons exist for imposing controls in the newest FISA program. Data mining is more than the "automation of traditional investigative skills." [FN234] The "automation" may have a greater impact on personal privacy because the mass of data mined will generate more false positives than traditional police work, and, absent controls, the data may be preserved indefinitely for any use, including human review. To defend data mining by arguing, as Judge Richard Posner has, that "[c]omputer searches do not invade privacy because search programs are not sentient beings" [FN235] is to ignore what happens to the data after it is mined.

Judge Posner concedes that programmatic surveillance

produces many false positives . . . But . . . the cost of false positives must be balanced against that of false negatives. . . . The intelligence services have no alternative to casting a wide net with a fine mesh if they are to have reasonable prospects of obtaining the clues that will enable future terrorist attacks on the United States to be prevented. [FN236] If we accept the utility and inevitability of programmatic collection, it does not undermine collection to insist on targeting criteria that focus on the nature of the information sought and fulsome protections against retaining and disseminating collected personal information.

[FN234]. Director, Institute for National Security and Counterterrorism; Board of Advisors Distinguished Professor, Syracuse University College of Law; Professor of Public Administration, Maxwell School of Citizenship

& Public Affairs, Syracuse University. The author thanks Spike Bowman, Stephen Dycus, Alexander Joel, Peter Raven-Hansen, Kim Taipale, and the participants in the Texas Law Review Symposium: Law at the Intersection of National Security, Privacy, and Technology, Feb. 4-6, 2010, for comments on a draft of this article. The author also thanks Andrea Masselli, Syracuse University College of Law, J.D. 2010, for excellent research assistance.


[FN2]. Id. § 105(a) (codified at 50 U.S.C. §1805(a)).


[FN5]. See FISA § 105(b)(2)(B) (requiring an order approving electronic surveillance to direct, at the applicant's request, a communication or other common carrier to assist an applicant in accomplishing the surveillance in a manner to protect its secrecy and minimize interference with the carrier's services); Id. §105(b)(1)(B) (requiring an application to identify the facilities where surveillance will be sought “if known”).


[FN7]. See William C. Banks, The Death of FISA, 91 Minn. L. Rev. 1209, 1275-76 (2007) (observing that, in the world of technological surveillance, evasion and logistical difficulties force the government to continually play “catch-up”).

[FN8]. Id.

[FN9]. See David S. Kris, Modernizing the Foreign Intelligence Surveillance Act: Progress to Date and Work Still to Come (noting that after FISA's enactment, the need to “conduct surveillance of international communications on wires inside the United States” developed, in part because of “the use, location, or accessibility of fiber optic cables”), in Legislating the War on Terror: An Agenda for Reform 217, 226 (Benjamin Wittes, ed., 2009).


[FN12]. See Shane Harris, FISA's Failings, Nat'l J., Apr. 8, 2006, at 59, 59 (“[T]he NSA's warrantless eavesdropping program also involves looking for suspicious patterns in a sea of communications.”).
[FN13]. See Leslie Cauley, NSA Has Massive Database of Americans’ Phone Calls, USA Today, May 11, 2006, http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm (“[T]he National Security Agency has been secretly collecting the phone call records of tens of millions of Americans. ... [T]he spy agency is using the data to analyze calling patterns in an effort to detect terrorist activity.”).


[FN15]. See id. § 702(a)-(e) (specifying the requirements for acquiring communications data and setting out targeting and minimization protocols).

[FN16]. See id. § 403 (indicating that the codification is to expire on December 31, 2012).

[FN17]. See infra notes 105-07 and accompanying text.

[FN18]. In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (FISA Ct. Rev. 2008).


[FN20]. See In re Directives, 551 F.3d at 1010 (recognizing the lack of an explicit foreign intelligence exception, but reasoning from the “special needs” cases that an exception to the warrant requirement was appropriate).

[FN21]. See Posner, Privacy, Surveillance, and Law, supra note 6, at 246-47 (discussing modern computer technology and its complication of the values debate shaping lawmaking in the field of electronic surveillance).

[FN22]. See Banks, supra note 7, at 1214-15 (arguing that the cumulative complexity of FISA has led to the loss of the policy compromise between enabling surveillance and using oversight mechanisms to safeguard individual privacy); Posner, A New Surveillance Act, supra note 6 (arguing that the “best, and probably the only, way” to clarify the government’s ability to conduct electronic surveillance is to “enact a new statute”).

[FN23]. See United States v. U.S. Dist. Court (Keith), 407 U.S. 297, 320-22 (1972) (holding that a warrant is required to conduct domestic surveillance, but limiting that holding to purely domestic threats to national security).

[FN24]. A lower federal court has upheld an exception to the Fourth Amendment Warrant Clause for searches conducted for foreign intelligence purposes outside the United States that involve U.S. persons acting as foreign agents, although in other respects a search still must be reasonable. See United States v. Bin Laden, 126 F. Supp. 2d 264, 277 (S.D.N.Y. 2000) (adopting a foreign intelligence exception to the warrant requirement for searches targeting foreign powers or their agents conducted abroad). The Supreme Court has not ruled on either set of questions.


[FN26]. Banks, supra note 7, at 1241-54.
[FN27]. See, e.g., id. at 1271-74 (discussing the debate surrounding the adoption of the 2004 Amendment that expanded FISA’s reach to unaffiliated persons).


[FN29]. See Banks, supra note 7, at 1230 (explaining that in 2008 the definition of electronic surveillance excluded surveillance taking place abroad).


[FN31]. Id.


[FN33]. FISA § 105(b)(1)(B).


[FN35]. FISA § 103.

[FN36]. See Banks, supra note 7, at 1233-40 (detailing the operation of FISA between 1978 and the early 1990s).

[FN37]. Banks, supra note 7, at 1231-32.

[FN38]. Id. at 1260.

[FN39]. Id. at 1276.

[FN40]. Id.


[FN42]. Banks, supra note 7, at 1233-34.


[FN46]. Banks, supra note 7, at 1294.

[FN47]. See Orin S. Kerr, Updating the Foreign Intelligence Surveillance Act, 75 U. Chi. L. Rev. 225, 234-35 (observing that due to “the dominant role of the United States in modern communications technology ... [c]ommunications service providers in the United States end up playing host to a great deal of traffic sent and received from individuals located abroad”).

[FN48]. Id. at 35.

[FN49]. See FISA for the 21st Century: Hearing Before the S. Comm. on the Judiciary, 109th Cong. 9 (2006) (testimony by Michael V. Hayden, Director, CIA, Office of the Director of National Intelligence), available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_senate_hearings&docid=f:43453.pdf (“When [FISA] was passed, almost all local calls were on a wire and almost all long haul communications were in the air.”).

[FN50]. Id.

[FN51]. Id. at 7.

[FN52]. FISA defines “electronic surveillance” as

(1) the acquisition by an electronic ... device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic ... device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States;

(3) the intentional acquisition by an electronic ... device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic ... device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.


[FN53]. See Kris, supra note 9, at 223 (noting that technological change from communications satellites to undersea fiber-optic cables has caused the scope of FISA to expand).

[FN54]. See Rebecca A. Copeland, War on Terrorism or War on Constitutional Rights? Blurring the Lines of Intelligence Gathering in Post-September11 America, 35 Tex. Tech. L. Rev. 1, 20 (2004) (noting that the USA PATRIOT Act essentially “puts email and internet communication within the purview of clandestine FISA surveillance”).

[FN55]. Kerr, supra note 47, at 230-32 (reporting that the provision was written to cover microphone bugs and closed-circuit television surveillance, but its original, unchanged terms apply to surveillance of foreign-to-foreign e-mail messages from inside the United States).


[FN57]. Kris, supra note 9, at 229.

[FN58]. Kristen Breitweiser, Enabling Danger (Part One), Huffington Post, Aug. 20, 2005, http://www.huffingtonpost.com/kristen-breitweiser/enabling-danger-part-one_b_5951.html. Media reports indicated that four of the hijackers had been in the summer of 2000 by a data-mining program called Able Danger, run by the Defense Intelligence Agency. Id.


[FN61]. See Tech. and Privacy Advisory Comm., supra note 59, at 27-28 (explaining that the USA PATRIOT covers “addressing and routing” Internet communications).

[FN62]. See id. at 33-41 (describing the implications of government data mining on U.S. persons).


[FN65]. President George W. Bush, Press Conference on the Post-September 11 Intelligence Gathering Program (Dec.19, 2005), available at http://www.whitehouse.gov/news/releases/2005/12/20051219-2.html; see also U.S. Dep't of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President 5 (2006) [hereinafter DOJ Whitepaper] (“The President has acknowledged that ... he has authorized the NSA to intercept international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations.”).
[FN66]. See Fine, supra note 63, at 15-16 (describing the layers of review that the PSP engaged in to target al Qaeda activity).


[FN68]. Id.

[FN69]. Id.

[FN70]. See Fine, supra note 63, at 17 (describing the FBI's role in the TSP as a recipient of the intelligence ultimately collected).

[FN71]. See id. at 11-14, 20 (outlining the arguments in favor of the legality of and presidential authority to authorize the TSP).

[FN72]. See Eric Lichtblau & David Johnston, Court to Overturn U.S. Wiretapping in Terror Cases, N.Y. Times, Jan.18, 2007, at A1 (reporting that the Bush Administration agreed to submit the NSA's wiretapping program to the supervision of the FISA Court).


[FN74]. See Fine, supra note 63, at 30 (“Certain activities that were originally authorized as part of the PSP have subsequently been authorized under orders issued by the Foreign Intelligence Surveillance Court (FISC). The activities transitioned in this manner included the ... ‘Terrorist Surveillance Program.’”).

[FN75]. Id. at 30-31.


[FN77]. See Kris, supra note 9, at 219, 230 (explaining the government is required to adhere to specific "minimization procedures" designed to balance the government's need to obtain intelligence against the privacy interests of Americans).


[FN79]. See Fine, supra note 63, at 9-13 (describing key features of the PAA and the scope of its coverage).

[FN80]. See id. at 5-7 ("FISA's definition of electronic surveillance, prior to the Protect America Act and as passed in 1978, has not kept pace with technology.").

[FN81]. See id. ("Thus, technological changes have brought within FISA's scope communications that the 1978 Congress did not intend to be covered.").

[FN83]. Id.


[FN85]. Kris, supra note 9, at 32-33.

[FN86]. See David Kris, A Guide to the New FISA Bill, Part II, June 25, 2008, available at http://balkin.blogspot.com/2008/06/guide-to-new-fisa-bill-part-ii.html (noting that the PAA “focuses only on the target’s location (or the government’s reasonable belief about his location) not his status or conduct as a terrorist or agent of a foreign power”).


[FN89]. Lichtblau, supra note 87; see also FISA Amendments Act §403 (indicating that the codification is to expire on December31, 2012).

[FN90]. FISA Amendments Act § 702.

[FN91]. See Kris, supra note 86 (“[T]here is no requirement that anyone--the FISA Court or the NSA--find probable cause that the target is a terrorist or a spy before (or after) commencing surveillance.”).

[FN92]. FISA Amendments Act § 702.

[FN93]. See supra notes 46-51 and accompanying text.


[FN95]. Id. § 101. The requirements for minimization are subject to the government’s need to “disseminate foreign intelligence information.” Id.

[FN96]. FISA Amendments Act § 404.

[FN97]. Id.

[FN98]. Id.

[FN100]. See Kris, supra note 86 (positing that the problem was solved, or “dealt with,” via “minimization”).

[FN101]. Compare FISA Amendments Act §703(a)(1), with id. §702(a).

[FN102]. See Kerr, supra note 47, at 230 (revealing that FISA, as enacted in 1978, prohibited the government from intentionally targeting the phone calls of “a particular, known United States person” from either outside the United States or within it).

[FN103]. FISA Amendments Act § 702.

[FN104]. See, e.g., Editorial, Compromising the Constitution, N.Y. Times, July 8, 2008, at A20 (criticizing the FAA in part because the federal government would be permitted to listen “to all calls to a particular area code in any other country”); Ryan Singel, Dems Agree to Expand Domestic Spying, Grant Telecoms Amnesty, Wired, June 19, 2008, http:// www.wired.com/threatlevel/2008/06/dems-agree-to-c/ (indicating that under the FAA, “the intelligence community will be able to issue broad orders to U.S. ISPs, phone companies and online communications services like Hotmail and Skype to turn over all communications that are reasonably believed to involve a non-American who is outside the country”); Ryan Singel, House Grants Telecom Amnesty, Expands Spying Powers, Wired, June 20, 2008, http:// www.wired.com/threatlevel/2008/06/house-grants-te/ (indicating that the FAA allows the NSA “to order phone companies, ISPs and online service providers to turn over all communications that have one foreigner as a party to the conversation”).

[FN105]. FISA Amendments Act § 702. FISC approval of a written certification from the Attorney General and DNI must occur prior to implementation of the authorization for surveillance, unless the same officials determine that time does not permit the prior review, in which case the authorization must be sought as soon as practicable, but not more than seven days after the determination is made. Id.

[FN106]. Id.

[FN107]. See Posner, Privacy, Surveillance, and Law, supra note 6, at 253 (describing the NSA process of “content filtering” and “traffic analysis”).

[FN108]. Id. at 252.

[FN109]. See Berger v. New York, 388 U.S. 41, 58-59 (1967) (striking down an electronic surveillance statute because it allowed acquisition of “the conversations of any and all persons coming into the area covered by the device ... indiscriminately and without regard to their connection with the crime under investigation”).

[FN110]. See In re Sealed Case, 310 F.3d 717, 740 (FISA Ct. Rev. 2002) (“[I]n practice FISA surveillance devices are normally left on continuously, and the minimization occurs in the process of indexing and logging the pertinent communications.”).

[FN111]. In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611 (FISA Ct. 2002), abrogated by In re Sealed Case, 310 F.3d at 717.

[FN112]. Id. at 617-18; see also In re Sealed Case 310 F.3d at 740 (“[I]n practice FISA surveillance devices are normally left on continuously, and the minimization occurs in the process of indexing and logging the pertinent communications.”).
[FN113]. In re Sealed Case, 310 F.3d at 741.


[FN115]. See FISA §101(h)(1) (defining minimization procedures to mean “specific procedures ... designed ... to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons”).


[FN118]. FISA Amendments Act § 702.

[FN119]. See FISA § 101(h)(2) (indicating that nonpublicly available information can be disseminated in a manner that identifies a U.S. person without their consent when such person’s identity “is necessary to understand foreign intelligence information or assess its importance”).


[FN121]. FISA Amendments Act § 702.

[FN122]. Id.

[FN123]. Id.

[FN124]. Id.

[FN125]. In re Directives to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1017-18 (FISA Ct. Rev. 2008).

[FN126]. Id. at 1011-12.

[FN127]. Id. at 1006.

[FN128]. Id. at 1007.

[FN129]. Id. at 1010-12.

[FN130]. Id. at 1011.

[FN131]. Id. at 1015.

[FN132]. Id.
[FN133]. In re Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).

[FN134]. In re Directives, 551 F.3d at 1013.

[FN135]. Id.

[FN136]. Id.

[FN137]. Id.

[FN138]. See, e.g., Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995) (approving warrantless searches that were designed to meet the government's "special needs, beyond the normal need for law enforcement" (quoting Griffin v. Wisconsin, 483 U.S. 868, 873 (1987))).

[FN139]. See Ferguson v. City of Charleston, 532 U.S. 67, 81-86 (2001) (declaring arrests made pursuant to hospital urine tests unconstitutional because of the policy's law enforcement purpose); City of Indianapolis v. Edmond, 531 U.S. 32, 41-47 (2000) (invalidating "drug checkpoints" because the program's primary purpose was to uncover evidence of ordinary criminal wrongdoing); Griffin, 483 U.S. at 880 (upholding the supervision of prisoners as a "special need" justifying departure from the warrant process).

[FN140]. In re Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).

[FN141]. See Banks, supra note 7, at 1282 (asserting that the application of the special-needs doctrine after the "significant purpose" amendment could allow the program to be used even when its sole purpose is the collection of evidence for prosecution without any version of a probable-cause requirement).

[FN142]. See id. at 1269?770 (noting that FISA should be unavailable if the purpose of the investigation is to prosecute because of FISA's requirements and the protections of the First, Fourth, and Sixth Amendments).

[FN143]. See Mayfield v. United States, 504 F. Supp. 2d 1023, 1032 (D. Or. 2007) (holding that "the government can conduct surveillance to gather evidence for use in a criminal case without a traditional warrant, as long as it presents a non-reviewable assertion that it also has a significant interest in the targeted person for foreign intelligence purposes"), rev'd, 588 F.3d 1252 (9th Cir. 2009) (declining to address the question of whether the challenged provisions of FISA, as amended by the USA PATRIOT Act, was unconstitutional).

[FN144]. Id.

[FN145]. See In re Sealed Case, 310 F.3d at 742 ("[A]ll the ... courts have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information."). But see Mayfield, 504 F. Supp. 2d at 1023.

[FN146]. See In re Sealed Case, 310 F.3d at 377?79.

[FN147]. In re Directives to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1014?15 (FISA Ct. Rev. 2008). In what the FISC calls a "parting shot," the telecom raised what the court called "a specific privacy concern." Id. at 1015. The court mentioned it only to task the Executive with notifying the telecom if that concern, whatever it is, arises, We cannot know whether the telecom was drawing attention to the inevitability of overcollection, either in general or specifically in this case. Id.

[FN149]. Id. at 172 (quoting Samson v. California, 547 U.S. 843, 848 (2006)).

[FN150]. Id. at 175.

[FN151]. Id. at 175-76.


[FN153]. In re Directives to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1014 (FISA Ct. Rev. 2008).

[FN154]. Id. at 1015 (citing, e.g., United States v. Kahn, 415 U.S. 143, 157-58 (1974)). In United States v. Butenko, 494 F.2d 593, 608 (1974), a review of warrantless surveillance for foreign intelligence purposes found that incidental collection that infringes privacy should be reviewed as part of Fourth Amendment reasonableness.


[FN158]. Id.

[FN159]. Id.

[FN160]. Id.

[FN161]. Id.


[FN163]. Kris, supra note 9, at 237.

[FN164]. See id. at 229 (noting that the amendments, pending at the time, only require the "government's reasonable belief about [a target's] location," as opposed to the more demanding requirement of the target's "status ... as a terrorist or agent of a foreign power").

[FN165]. See Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101(m), 92 Stat. 1783, 1786 (codified at 50 U.S.C. §1801(m) (2006)) (defining "person" as "any individual, including any officer or employee of the Federal government, or any group, entity, association, corporation, or foreign power").
[FN166]. See United States v. Verdugo-Urquidez, 494 U.S. 259, 274-75 (1990) (rejecting a Fourth Amendment claim based on the fact that the searched person had "no voluntary attachment to the United States").


[FN169]. Kerr, supra note 47, at 238.

[FN170]. Judge Posner would define the predicate for programmatic surveillance narrowly. "[T]he term national security" would include only "threats involving a potential for mass deaths or catastrophic damage to property or to the economy." Posner, Privacy, Surveillance, and Law, supra note 6, at 258.

[FN171]. See Kris, supra note 9, at 235-36 (suggesting changes to the FAA that would apply to communications between a sender and receivers all located in the United States).

[FN172]. Id.


[FN174]. Fine, supra note 63, at 38.

[FN175]. Id. at 3.

[FN176]. See Warshak v. United States, 490 F.3d 455, 473-76 (6th Cir. 2007) (finding that individuals have a "reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP" and thus that the government must provide notice and an opportunity to be heard before compelling the ISP to turn over the e-mails to the government), vacated, 532 F.3d 521 (6th Cir. 2008) (en banc); see also DanielJ. Steinbock, Data Matching, Data Mining, and Due Process, 40 Ga. L. Rev. 1, 82-83 (2005) (advocating due process protections in data mining).

[FN177]. The FISA Court only reviews targeting and minimization procedures to ensure that they meet the statutory requirements and the Fourth Amendment, and the court only reviews certifications as a matter of form, to ensure that they "contain[] all the required elements." Kris, supra note 86, at 230 (citing FISA Amendments Act, Pub. L. No. 110-261, §702, 122 Stat. 2436, 2444 (to be codified at 50 U.S.C. §1881a(ii)(3)(A)-(B))).

[FN178]. See, e.g., Cate, supra note 168, at 480, 487 (arguing that prior judicial authorization in data mining would help better balance security with privacy concerns).

[FN179]. See Mark Williams, The Total Information Awareness Project Lives On, Tech. Rev., Apr. 26, 2006, available at http://www.technologyreview.com/communications/16741 (explaining that when the NSA practices automated data mining, FISA requirements are inapplicable because it is not a search of a specific individual).

[FN180]. Cate, supra note 168, at 473-74.

[FN181]. Id. at 471-80.

[FN182]. See Williams, supra note 179 (stating that the NSA uses electronic analysis and content filtering to ap-
ply "highly sophisticated search algorithms and powerful statistical methods ... [to] search for particular words or language combinations that may indicate terrorist communications").


[FN185]. FISA § 106(f).


[FN187]. FISA § 105(a)(5); Intelligence Authorization Act §304(a)(5).

[FN188]. See supra notes 114-17 and accompanying text.

[FN189]. See supra note 184 and accompanying text.

[FN190]. In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 618 (FISA Ct. 2002), abrogated by In re Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).

[FN191]. Id.

[FN192]. It is, of course, also true that the failure of the government to log or index a communication that made that record practically inaccessible when FISA was enacted would not stand in way of retrieval of the record today if officials employed their search software. See DavidS. Kris & J.Douglas Wilson, National Security Investigations and Prosecutions 9-22 to -24 (2007) (describing "tensions" between retention and discovery in criminal cases, where useable files are disclosed to the defendant in compliance with Brady, including non-pertinent audio files that should have been destroyed or rendered useless following minimization). In other words, even information minimized following traditional FISA practices might still be accessible to the government. Id.

[FN193]. See supra notes 115-17 and accompanying text.


[FN196]. Cate, supra note 168, at 469-70.


[FN199]. Id. at 5.

[FN200]. Id. at 55.

[FN201]. Id.

[FN202]. See United States v. Miller, 425 U.S. 435, 442 (1976) (holding a bank customer had no expectation of privacy in checks and deposit slips held by a bank); see also Smith v. Maryland, 442 U.S. 735, 742 (1979) (holding there is no expectation of privacy when a pen register is installed on phone company property at the company's office because people do not reasonably believe there is an expectation of privacy when they "convey" a dialed phone number to the phone company).

[FN203]. See Miller, 425 U.S. at 442; Smith, 422 U.S. at 742 (both reasoning that the expectation of privacy vanishes when a person voluntarily submits data to a third party).

[FN204]. See Cate, supra note 168, at 454-60 (setting out the Court's decisions in Miller and Smith and applying that line of cases today).

[FN205]. Solove, supra note 194, at 356-57 (finding that the third-party doctrine severely limits Fourth Amendment protections where the government mines data voluntarily given to companies by their customers).

[FN206]. Cf. Warshak v. United States, 490 F.3d 455, 473, 482 (6th Cir. 2007) (finding Fourth Amendment protection against the government's warrantless subpoena of e-mails transmitted through a commercial ISP where the fact that it was not the ISP's normal practice to review e-mails supported users' reasonable expectation of privacy), vacated, 532 F.3d 521 (6th Cir. 2008).

[FN207]. Cate, supra note 168, at 460.

[FN208]. Id.


[FN210]. See In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 618 (FISA Ct. 2002) (outlining the principal steps in the minimization process), abrogated by In re Sealed Case, 310 F.3d 717, 736 (FISA Ct. Rev. 2002).

[FN211]. Id.

[FN212]. Id.
[FN213]. Kris & Wilson, supra note 192, at 9-23.


[FN216]. Id.

[FN217]. Id.

[FN218]. Id.

[FN219]. Id. at 7-8.


[FN221]. Id. at 000301, 000304.


[FN224]. FISA § 101.


[FN226]. Id. at 33.

[FN227]. Id. at 35-36.

[FN228]. Id. at 35.

[FN229]. Id.

[FN230]. Id. at 36.

[FN231]. Id. at 40. The Task Force also proposed that authorized use include a safe-harbor mechanism that would prohibit punitive action against any user of the system that used collected information following authorized-use guidelines. Id. at 40-41.

[FN232]. Id. at 34-35, 39.
[FN233]. Id. at 39.

[FN234]. Taipale & Carafano, supra note 6, at 21.


[FN236]. Id. at 252-53.

88 Tex. L. Rev. 1633

END OF DOCUMENT
Remarks by William C. Banks at the 35th Anniversary of the FISC, May 20, 2013

Virtually everyone in this room knows the basic story of how the Foreign Intelligence Surveillance Act (FISA) came about …

FISA was the product of a set of compromises unique to their time. The executive branch wanted a continuing discretion to employ wiretapping for foreign intelligence unfettered by judicial or congressional oversight. Because the Supreme Court’s Keith decision (United States vs. US District Court, 407 US 297 (1972)) concerned domestic security, the door was not shut. In addition, because Keith acknowledged a possibility that the rules might be different for foreign intelligence and the 1968 Crime Control Act disclaimed prescribing any rule for foreign intelligence gathering, it remained plausible to argue that the executive might make its own rules for collecting foreign intelligence.

Their hand was weakened considerably, however, by the effects of the Watergate scandal; lawsuits challenging warrantless surveillance; and the practical problem that telephone companies and government agencies were unwilling to approve electronic surveillance without a court order. There were, in addition, high profile investigations of illegal spying by intelligence agencies, including by the Senate Church Committee. The Church Committee reviewed nearly 40 years of domestic surveillance, learning that every president since Franklin D. Roosevelt had asserted and used the authority to authorize warrantless electronic surveillance and founding that “[t]oo many people have been spied upon by too many Government agencies and … Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power.” The Church Committee recommended a strict and careful separation of domestic and foreign intelligence gathering, although it recommended continued surveillance of “hostile foreign intelligence activity.”

Congress was thus emboldened to control executive overreaching in its use of surveillance. Civil liberties groups, such as ACLU, worried that if Congress set a wiretap standard too low, it could end up authorizing rather than curtailing intelligence agency excesses. In other words, would no legislation be better for civil liberties than bad legislation? At the same time, Congress recognized that “no United States citizen in the United States should be targeted for electronic surveillance by his government absent some showing that he at least may violate the laws of our society,” even though evidence of national security crimes could be collected during the electronic surveillance. After six years of hearings and discussion and through the stewardship of attorneys general Edward Levi and Griffin Bell, presidents Gerald Ford and Jimmy Carter, and several members of the House and Senate, FISA became law in 1978. In his signing statement, Carter said:

1 Available at http://bit.ly/1w3glwo.
The act helps to solidify the relationship of trust between the American people and their Government. It provides a basis for the trust of the American people in the fact that the activities of their intelligence agencies are both effective and lawful. It provides enough secrecy to ensure that intelligence relating to national security can be securely required, while permitting review by the courts and Congress to safeguard the rights of Americans and others.

Beginning in 1978, the FISA authorized the means for electronic collection of foreign intelligence that served the nation well for many years. The basic idea was simple. Government may conduct electronic surveillance of Americans or others lawfully in the United States without traditional probable cause to believe that they had committed a crime if it could demonstrate to a special Article III court that it had a different kind of probable cause: reason to believe that targets of surveillance are acting on behalf of foreign powers. Over time, FISA was amended several times to extend its procedures to conduct physical searches, monitor suspected lone-wolf terrorists, and accommodate evolving threats.

For a long time the process worked well as a mechanism to regulate surveillance of known intelligence targets. The FISA process and its eventual orders have always been limited, however. FISA was concerned with acquisition, not with the uses government might have for what is collected. FISA also assumed that officials know where the target is and what facilities the target will use for his communications. Knowing this much enabled the government to demonstrate the required probable cause to believe that the target was an agent of a foreign power or a lone wolf. Traditional FISA did not authorize intelligence collection for the purpose of identifying the targets of surveillance, or of collecting aggregate communications traffic and then identifying the surveillance target. In other words, FISA envisioned case-specific surveillance, not a generic surveillance operation, and its approval architecture was accordingly geared to specific, narrowly targeted applications. FISA was also based on the recognition that persons lawfully in the US have constitutional privacy and free expression rights that stand in the way of unfettered government surveillance.

Although the volume of FISA applications increased gradually through the 1990s, after the Sept. 11, 2001 terrorist attacks, the pace of electronic intelligence collection quickened, and Bush Administration officials argued that traditional FISA procedures interfere with necessary "speed and agility." FISA applications doubled to more than 2,000 a few years after 9/11. The system was, it seemed, grinding along, but it was carrying a lot of weight.

Over the last decade-plus, critics argued that the patchwork-like architecture of FISA has become too rigid, complicated, and unforgiving to enable effective intelligence responses to crises. The computerization of communications that has so enriched our capabilities has also facilitated stealth and evasion by those seeking to avoid detection. Would-be targets of surveillance began communicating in ways that stress or evade the FISA system. Because of the pervasiveness of US telecom switching technology, collection inside the United States is now often the best or only way to acquire even foreign-to-foreign communications that were originally left unregulated by FISA.
Changing technologies have also turned the traditional sequence of FISA processes on its head. We discovered after 9/11 that investigators could enter transactional data about potential terrorists and come up with a list that included four of the hijackers—a sort of reverse of the typical FISA-supported investigation. Powerful computers and data-mining techniques permitted intelligence officials to select potential surveillance targets from electronic databases of previously unimaginable size. The wholesale quality of this expansive computer collection and data mining is incompatible with the retail scope of the original FISA process. Instead of building toward an individual FISA application by developing leads on individuals with some connection to an international terrorist organization, the government could develop algorithms that search thousands or even millions of collected e-mail messages and telephone calls for indications of suspicious activities.

At the same time, more Americans than ever are engaged in international communications, and there is far greater intelligence interest in communications to and from Americans. Both circumstances increase the likelihood that the government will be intercepting communications of innocent Americans, raising as many questions about the adequacy of FISA safeguards as they do about the adaptability of FISA architecture. This tension formed the context for a series of post-9/11 developments, culminating in the FISA Amendments Act of 2008 (FAA). The FAA codified, now until Dec. 31, 2015, a procedure to permit broad, programmatic surveillance focused on patterns of suspicious activities and not on a specific individual or the contents of their communications through changes in FISA that overcame the case-specific orientation of the original statute.

The FISA architecture was changed to accomplish this neat trick in a simple way. The definition of electronic surveillance was amended so as not to apply to surveillance of a person reasonably believed to be outside the US. Under the new legislation, the DNI and the attorney general were authorized to collect foreign intelligence “directed at” persons reasonably believed to be outside the US, without obtaining an order from the Foreign Intelligence Surveillance Court (FISC), even if one party to the communication was a US citizen inside the US. The predicate for collection thus became the location of the target, not his status in relation to a foreign power or terrorist organization.

Under the FAA, the role of the FISC is narrowly circumscribed. The attorney general submits procedures to the FISC by which the government will determine that acquisitions conducted under the program meet the program targeting objectives and satisfy traditional FISA minimization procedures. After a FISC judge approves the program targeting procedures, executive branch officials authorize the surveillance of persons reasonably believed to be outside the US and issue directives compelling communications carriers to assist.

From its beginnings, the overarching FISA question has been how to evaluate and weigh the basic values of security and individual liberties when electronic surveillance is used to collect foreign intelligence. The Constitution continues to provide a baseline. The Fourth Amendment Warrant Clause applies to electronic surveillance conducted for foreign intelligence purposes within the US if the surveillance involves US persons who
do not have a connection to a foreign power. FISA now permits such electronic surveillance as the inevitable byproduct of surveillance of unprotected targets, but the Act does little to insulate US persons from the effects of the surveillance. If the combination of terrorism threats and computerization demands a more nimble capacity to conduct suspicion-less electronic surveillance to combat terrorism, the discretion that is necessarily part of that system should be carefully controlled, either at the point of collection or when the information is maintained or used by the government.

Programmatic surveillance adds considerably to FISA's complexity, and it has already produced implementation problems. For example, with the revolution in digital communications, the idea of a geographic border has become an increasingly less viable marker for legal authorities and their limits. Using the Internet, packets of data that constitute messages travel in disparate ways through networks, many of which come through or end up in the US. Those packets, and countless Skype calls and instant messages, originate from the US in growing numbers, and the sender may be in the US or abroad. Likewise, it may or may not be possible to identify the sender or recipient by the e-mail addresses or phone numbers used to communicate.

Nor do we think of our international communications as being in any way less private than our domestic calls. In 1978, Congress apparently exempted from FISA international surveillance conducted abroad because, when FISA was enacted, electronic communications by Americans did not typically cross offshore or international wires. Now, of course, we do communicate internationally and our message packets may travel a long distance, even if we are corresponding by e-mail with a friend in the US who is in the same city. The location or identity of the communicants is simply not a useful marker in Internet communications.

Conclusions

The FISC remains an especially successful court. It was created to do a job that traditional Article III judges were reluctant to do and that the executive branch preferred be left to them. At the same time, the FISC was created at a time when surveillance abuses cast a shadow over the integrity of these important foreign-intelligence activities. In the years between creation of the court and the 9/11 attacks, the FISC developed expertise in foreign intelligence surveillance and the court gained considerable respect from observers inside and outside government.

The combination of the criminalization of many terrorist activities and the digital revolution in communications and surveillance capabilities altered the role of the FISC and, following the 2008 amendments to FISA, strained its utility as an independent arbiter of lawful FISA surveillance. The programmatic surveillance now sanctioned by the FISC is a cause for concern because the special court has assumed more of an administrative function than a judicial role. There remain opportunities to revise minimization rules and to make government retention or dissemination of private information about innocent persons less likely. At the same time, if we must tolerate sweeping digital collection of our personal data, the FISC should have greater and more meaningful opportunities to oversee its collection—if not in advance, then after the fact.
In our legal system, we attach great importance to the value of fair processes. In national security law and policy, when secrecy has been an important operational requisite, we have developed review and oversight processes to help assure that unilateral power is not abused. So has it been with FISA. In the years since 9/11, those process safeguards have been compromised. If FISA is to have a meaningful role for the next 35 years, the role of the FISC as overseer of the system will have to be restored, one way or the other.

ENDNOTE: The Celebration of the 35th Anniversary of the US Foreign Intelligence Surveillance Court was sponsored by the American Bar Association Standing Committee on Law and National Security, Georgetown Law; the Center on National Security Law, University of Virginia School of Law; and the Institute for National Security and Counterterrorism.
8 Exceptional Courts in Counterterrorism

Lessons from the Foreign Intelligence Surveillance Act (FISA)

William C. Banks

The Foreign Intelligence Surveillance Court (FISC) is an exceptional court created by Congress to respond to a unique set of challenges related to foreign intelligence. On the one hand, U.S. presidents had on occasion authorized electronic surveillance and physical searches in pursuit of foreign intelligence without any prior judicial authorization, raising concerns that executive officials were violating the free expression and privacy rights of affected persons. On the other hand, many experts agreed that the need for speed and secrecy in collecting foreign intelligence in the face of threats of terrorism and espionage rendered traditional judicial warrant procedures ill-suited for foreign-intelligence surveillance. The FISC responded effectively to these challenges, but this exceptional court has also generated new problems. Because the factual predicate for gaining FISC approval to conduct surveillance or search is less demanding than what is required in traditional criminal cases, there has developed a considerable spillover effect, where criminal investigators and prosecutors rely on the exceptional FISC procedures to gather evidence for later use in criminal prosecutions. As a result, Fourth Amendment protections for the accused may be threatened by use of the exceptional procedures. At the same time, recent revisions to the FISC authorize the exceptional court to grant blanket approval to wholesale collection of foreign intelligence through issuance of directives to telecommunications companies and Internet service providers.
In this new role, the authorization for programmatic surveillance omits
the case-by-case review of applications for surveillance and converts the
FISC into an administrative clerk for executive officials.

This chapter first describes the history leading to the original cre-
ation of the FISC in 1978. Next, the role of this exceptional court in
implementing the special scheme for foreign-intelligence collection is
assessed, focusing on its overlap with law-enforcement objectives and
the challenges of keeping up with changing technologies of surveillance
and evasion. These challenges to the court’s role are evaluated, as is the
changing role of the FISC in the era of programmatic surveillance. In
the concluding section, reforms are suggested that could help shore up
the FISC in the face of the civil liberties threats posed by the continuing
operation of this special court.

1. The Original FISA Scheme

Following the Watergate scandal and collapse of the Nixon presidency,
congressional investigations discovered that, without seeking judicial
approval, the federal government had engaged in widespread domes-
tic surveillance for decades. The National Security Agency (NSA) had
collected millions of telegrams sent from the United States abroad, and
the Federal Bureau of Investigation (FBI) maintained watch lists of U.S.
citizens involved in political protests. In 1976, the Senate investigatory
Church Committee found that “too many people have been spied upon
by too many Government agencies and [too] much information has been
collected. The Government has often undertaken the secret surveillance
of citizens on the basis of their political beliefs, even when those beliefs
posed no threat of violence or illegal acts on behalf of a hostile foreign
dpower.”1

After the congressional investigators and media reports detailed the
surveillance abuses targeting innocent civil rights and antiwar protestors
in violation of their First and Fourth Amendment rights, members of

4 407 U.S. at 320, 323.
5 FISA § 105(a) (codified at 50 U.S.C. § 1805(a) (2010)).
of up to seven years. There are no special requirements that the judges have expertise in national security or counterterrorism; all district court judges are presumptively eligible. FISA also provides for designation by the Chief Justice of three district or court of appeals judges to sit as a special court of review to hear appeals by the government from denial of an application by one of the FISC judges. The government may then appeal to the Supreme Court.

Electronic surveillance can capture movements and conversations about plans to commit a terrorist act and thus allows the government to step in before the act occurs. At the same time, electronic surveillance imposes a heavy cost in threats to personal privacy and expressive freedoms if it reaches innocent persons. Threats to civil liberties are especially acute when national security reasons are invoked to monitor political activities, as the convergence of First and Fourth Amendment values is not present in cases of ordinary crime. The government may have strong interests because of the threat of terrorism, but those targeted also have important interests to be taken into account.

FISA governed the electronic surveillance only of persons in the United States and only for the purpose of collecting foreign intelligence. It did not apply to surveillance conducted outside the United States or to foreign-to-foreign telephone communications intercepted within the United States. "Probable cause" required that a target of the surveillance be a "foreign power," an "agent of a foreign power," or since 2004, a "lone wolf" terrorism suspect — a person believed to be preparing for terrorist activities who is not shown to be affiliated with a terrorist organization. Applications to the FISC for approval of a search or surveillance had to specify "facilities" where the surveillance would be directed and procedures to "minimize" the acquisition, retention, and dissemination of information not relevant to an investigation.\(^6\)

\(^6\) Id. § 105(b)(1)(B).

\(^7\) Id. § 101(b); see also Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103–359, sec. 807, § 301(4), 108 Stat. 3423, 3443–44 (codified at 50 U.S.C. § 1821(4) (2006)) (amending FISA to include a new definition for "minimization procedures").

Before the FISC issued an order approving electronic surveillance involving a U.S. person, a FISC judge had to find probable cause that the target was an agent of a foreign power, or on the basis of meeting one of four conditions: (1) the target knowingly engaged in clandestine intelligence activities on behalf of a foreign power, which "may involve" a criminal law violation; (2) the target knowingly engaged in other secret intelligence activities on behalf of a foreign power pursuant to the direction of an intelligence network, and those activities involved or were about to involve criminal law violations; (3) the target knowingly engaged in sabotage or international terrorism or was preparing for such activities; or (4) the target knowingly aided or abetted another who acted in one of the above ways.

The process undertaken by the government before going to the FISC (and before any wiretap is turned on) was elaborate and multilayered. FBI lawyers oversaw FBI agents who wanted to carry out the surveillance, and Department of Justice lawyers oversaw the FBI lawyers. Then, an application for FISA surveillance had to be approved by the Attorney General before presentation to the FISC. The department had to provide detailed information, including the identity of the target, a description of the information sought, and certifications that the information sought was believed to be foreign-intelligence information that could not reasonably be obtained by normal investigative techniques. The FISC may grant orders approving electronic surveillance anywhere within the United States.

However, what most of us think of as the judicial role in authorizing surveillance was limited by Congress in FISA in several important respects. From the beginning, FISA has allowed warrantless surveillance of non-U.S. persons for as long as one year, and another provision authorized electronic surveillance without judicial approval in an emergency situation. \(^8\) The special court's review of FISA applications is also limited. Unlike deciding the reasonableness of surveillance in a criminal case, or

\(^8\) 50 U.S.C. §§1822(a)(1); 1805(e) (2010).
compliance with probable cause standards, FISC judges simply certify that a purpose of the surveillance is to collect foreign intelligence. The FISC does not determine whether there is probable cause that the electronic surveillance will result in acquisition of foreign intelligence, even where the principal objective of government investigators is to build a case for prosecution. In essence, the FISC decides that the government’s paperwork is complete and in order. The legal standard requires only that the FISC find that the government certifications are not clearly erroneous.9

Once the statutory findings are made by the FISC, it must issue the surveillance order. The order must describe the target, the information sought, and the means of acquiring the information. The order must also determine that the government has set minimization procedures—mechanisms to assure that collected information is not stored or disseminated beyond the scope of what the FISC approved. The order must also set a period of time during which the surveillance may occur. The government may apply to renew the order on the same basis as the original application, and following the same procedures. More than 20,000 applications for surveillance or searches have been approved by the FISC since 1979. Less than 1 percent have been denied, and most of those denied applications were later approved after revision of the application.

To some observers, the FISC serves as a rubber stamp for executive branch officials who lack the traditional probable cause required by a magistrate in criminal cases. Some counter that the FISC is an unnecessary impediment as the executive branch strives to become nimble in collecting necessary intelligence. To others, the FISC has been a neutral arbiter necessary to ensure government accountability and legitimacy in furtherance of the narrow objectives for collecting foreign intelligence prescribed by FISA. At a minimum, the FISC provides assurances to Congress and the public that the government is meeting its statutory

---

9 Id. §1805(a).
United States have constitutional privacy and free expression rights that stand in the way of unfettered government surveillance.

Although the volume of FISA applications increased gradually through the 1990s, after 9/11 the pace of electronic intelligence collection quickened. Bush administration officials argued that traditional FISA procedures interfered with necessary “speed and agility.” As the pre-9/11 annual FISA applications doubled to more than 2,000 a few years later, the Director of National Intelligence (DNI) complained that more than “200 man hours” were required to prepare an application “for one [phone] number.” The system was, it seemed, grinding along, but it was carrying a lot of weight.

2. Challenges to the FISA System

In the years after 9/11, the FISA scheme and the role of the special court were stretched well beyond their case-specific focus on gathering foreign intelligence. Two developments placed special stresses on the FISC. Increasingly, terrorism-related activities had been criminalized, leading to frequent intersections of law enforcement and intelligence investigations. The FISC became the favored venue for seeking authorization to conduct surveillance in anticipation of prosecution in terrorism cases. As a result, the traditional law-enforcement warrant was often bypassed, and attendant Fourth Amendment interests of the targets and those on the other end of the phone line were compromised through incidental collection of communications. Second, digital communications technologies were at once exploited by foreign agents and suspected terrorists and relied on by government. The development of data-mining techniques for


EXCEPTIONAL COURTS IN COUNTERTERRORISM

use by the government enabled investigators to depersonalize electronic surveillance and focus on gathering massive quantities of communications data to mine for further indications of terrorist activities.

Meanwhile, the Bush Administration decided to obtain what it viewed as the necessary speed and agility by tasking the NSA to undertake a massive electronic surveillance program on its own, in secret, and without involvement of FISA processes or the FISC. Within weeks of 9/11, although not reported until the December 2005 publication of an article in The New York Times, the NSA began intercepting communications where one party was located outside the United States and the other party inside the United States. The collection occurred without gaining orders from the FISC. Instead of seeking new investigative authorities from Congress, the Bush administration simply ignored the requirements of FISA. The White House vigorously defended what it called the Terrorist Surveillance Program (TSP) after the story broke, but its legal arguments were weak and unpersuasive. Although details of the TSP remain secret, the NSA apparently would sweep up large quantities of data and then sift through it using data-mining processes. If the sifting produced information about specific individuals or groups that could be targeted for further surveillance, the NSA would then approach the FISC with a traditional FISA application.

Through statutory amendments to FISA since the September 11 attacks — in the 2001 USA Patriot Act, the 2007 Protect America Act, and the 2008 FISA Amendments Act (FAA) — the executive branch and Congress have tasked the FISC to endorse government efforts to build criminal prosecutions without following traditional Fourth Amendment rules, and to permit sweeping programmatic surveillance orders without review of the individual facts of potential targets. Even before the September 11 attacks, the United States moved to criminalize more terrorism-related activities. Although FISA and the FISC were designed

as preventives – to help the government forestall terrorism and espionage by learning about it in advance – increasingly, the investigations for foreign-intelligence and law-enforcement purposes had begun to blend and their objectives merge. Meanwhile, the FISA Court of Review approved executive branch practices that might sacrifice Fourth Amendment values and threaten the independence and legitimacy of the FISC. In the USA Patriot Act, Congress amended FISA to dismantle the wall between law enforcement and intelligence investigations by permitting the use of FISA procedures when there is “a significant” foreign-intelligence purpose to an investigation designed at the outset to build a criminal case. In other words, instead of coming to the FISC only when the primary purpose is collecting foreign intelligence, the government could launch its law-enforcement investigation with the FISC so long as some significant foreign intelligence could be collected. After the FISC objected to new Justice Department guidelines that dismantled the wall on the basis of the statutory change, the FISA Court of Review overturned the FISC and ruled that the Criminal Division of the Department of Justice could submit an application to the FISC so long as there was some significant foreign intelligence that could be collected. As a result, the role of the FISC diminished. The Court no longer questions the dominant prosecution objectives of government investigators who come before it, so long as there is some foreign-intelligence objective connected to the investigation. Similarly, its role in the new era of programmatic surveillance – to be described – is simply to approve and then occasionally monitor the suspicionless targeting procedures developed by the investigators.

3. Programmatic Surveillance and the Special Court

Under FISA as amended by the temporary Protect America Act in 2007 and the FAA in 2008, a significant portion of the FISC role has been transformed into performing a clerking function for the executive branch. Before Congress and in the context of the secret NSA surveillance program, the Bush administration successfully emphasized the need to amend FISA to account for changes in technology and thus enable it to conduct surveillance of foreign digital communications from within the United States. But providing statutory access to U.S. digital telecommunications switches would enable NSA to access e-mail traffic traveling to or from U.S. servers, opening up a vast swath of U.S. person communications for government scrutiny. In effect, the FAA authorized the TSP. The FISA architecture was changed to accomplish this neat trick in a simple way. The definition of electronic surveillance was amended so as not to apply to surveillance of a person reasonably believed to be outside the United States. Under the new legislation, the DNI and the Attorney General were authorized to collect foreign intelligence “directed at” persons reasonably believed to be outside the United States, without obtaining an order from the FISC, even if one party to the communication was a U.S. citizen inside the United States. The predicate for collection thus became the location of the target, not his status in relation to a foreign power or terrorist organization.

Under the FAA, the role of the FISC is narrowly circumscribed. The Attorney General submits procedures to the FISC by which the government will determine that acquisitions conducted under the program meet the program targeting objectives and satisfy traditional FISA minimization procedures. After a FISC judge approves the program targeting procedures, executive branch officials authorize the surveillance of persons reasonably believed to be outside the United States and issue directives compelling communications carriers to assist. Although details of the implementation of the program authorized by the FAA remain classified, a best guess is the government uses a broad vacuum cleaner-like first stage of collection focusing on transactional data in which wholesale interception occurs following the development and implementation of filtering criteria. Targeting might be directed at a terrorist organization or telephone number or e-mail address. Then NSA engages in a more particularized collection of content after analyzing mined data.
Although traditional FISA orders are still required for “intentional acquisition” of domestic communications, and they are also required for the first time for a U.S. person targeted as a foreign power or agent of a foreign power outside the United States, accidental or incidental acquisition of communications of U.S. persons inside the United States surely occurs, especially in light of the difficulty of ascertaining a target’s location. Following a periodic review of the directives issued after enactment of the FAA, the Justice Department and DNI reported to the FISC in April 2009 that the NSA had been engaging in significant and systematic over-collection of the domestic e-mail messages of Americans. After investigations had been launched, intelligence officials told The New York Times that the NSA exceeded its statutory authority in implementing eight to ten separate orders issued by the FISC since enactment of the FAA. Because each order could permit collection of hundreds or thousands of phone numbers or e-mail addresses, millions of individual communications could have been intercepted, including some by U.S. persons inside the United States. 13

The FISC must approve an order for programmatic surveillance if it finds that the government’s certification “contains all the required elements” and the targeting and minimization procedures are consistent with the act and the Fourth Amendment. If the FISC does not grant the government’s request for an order, it may appeal to the FISA Court of Review. Once the government’s request is approved, the FISC does not supervise implementation of the targeting. The FISC does conduct a semiannual review of the programmatic surveillance it has authorized.

Beyond the risks of incidental collection, many Americans feared what the government might do with the information it gathered. The FAA requires that the Attorney General and the DNI certify that minimization procedures have been or will be submitted for approval to the FISC

---


prior to, or within seven days following, implementation. 14 However, the generic FISA minimization requirements were not modified in the FAA to accommodate the surveillance of individual targets through programmatic surveillance. 15 The FISC does not review the implementation of minimization procedures or practices for the programmatic surveillance it approves. Nor do statutory minimization rules require the government to discard communications of U.S. persons incidentally collected when the government is targeting someone abroad. The amended FISA permits the government to retain and disseminate information relating to U.S. persons so long as the government determines that it is “foreign intelligence information.” 16 By implication, the government may compile databases containing foreign-intelligence information from or about U.S. persons, retain the information indefinitely, and then search the databases for information about specific U.S. persons. The combination of the government’s use of the foreign-intelligence trump card to hold or disseminate information and the lack of judicial oversight of how private communications are filtered out leaves the minimization mechanism short of meeting its goals for programmatic FISA surveillance.

Although traditional FISA applications and orders may not comply with the Warrant Clause or traditional probable cause requirements, the substitution of individualized FISC review of applications and a specialized foreign intelligence-related probable cause have been construed by nearly every court that has considered their constitutionality as adequate for Fourth Amendment purposes. The programmatic orders are so dramatically different from the thirty-year FISA experience, however, that their suspicionless targeting procedures deliver us nowhere near meeting warrant or probable cause standards. Nor are the procedures reasonable

---

15 Id.
16 50 U.S.C. § 1821(4)(B) (indicating that nonpublicly available information can be disseminated in a manner that identifies a U.S. person without their consent when such person’s identity “is necessary to understand such foreign intelligence information or assess its importance”).
in Fourth Amendment terms. Nor are any of the administrative officials required to find that the program targets are foreign agents, have or will engage in criminal activity, or are connected in any way with terrorism.

The programmatic title of FISA subordinates the FISC to the discretionary decisions of the Justice Department. Every FAA decision bearing on specific intelligence targets — except for the required FISC finding that a U.S. person outside the United States targeted for surveillance is a foreign power or agent of a foreign power — is made by executive branch officials and is not subject to review by the FISC or another judge. Prior identification of targets to a judge protects innocent third parties from being swept up in the surveillance and enforces the hallmark predicate for government surveillance — individualized suspicion. By focusing on what the collected information may be used for, FISA and the FISC (until the FAA) provided a useful, albeit opaque, mechanism to ensure the accountability of the collection scheme.

4. Shoring up the FISC as an Exceptional Court

The combined stresses of criminalizing terrorist activities and the digital revolution in communication and surveillance technologies have transformed the FISC from an effective model for an exceptional court that works into a clerk for executive branch investigators. Instead of doing what judges are good at — sifting facts and applying them to legal standards — the FISC spends much of its collective time on ministerial tasks. Unless reforms are made the special court may lose its independence and, over time, its legitimacy.

The original FISA procedure for reviewing applications for surveillance of foreign agents and lone wolves has served the nation well as a secondary, specialized system that serves discrete and important objectives. But the FISA experience shows in vivid ways the dangers that occur when a secondary system and its standards are mingled with those from the primary federal system, in this instance law enforcement and criminal prosecution in the federal courts. The byproduct of mingling the two is that the constitutional protections embedded in federal court prosecution are watered down and gradually eviscerated. Without FISA and the FISC, the federal courts would not have authorized electronic surveillance and physical searches absent probable cause of criminal activities or, in the event of exigent circumstances, on the basis of a finding of reasonableness. Employing the FISC, the government makes a less burdensome showing to the judge, and the target is never given notice of the application or the eventual surveillance. As ever more prosecutions related to terrorism are launched on the strength of FISA surveillance, the federal courts review the surveillance subject to permission already granted to the FISC by Congress. The courts do not undertake a de novo review of the surveillance application.

Because so many terrorism-related crimes now populate the criminal code in the United States it is unrealistic to expect any version of the wall that used to separate law enforcement and intelligence investigations to be rebuilt. The blending of the criminal and foreign-intelligence functions and personnel in the Justice Department, however, calls for reforms to protect the independence of the FISC and the integrity of the FISA process. One partial fix would be to create adversarial roles and processes. Both traditional FISA applications and certifications for programmatic surveillance orders are created, reviewed, critiqued, and presented entirely by Justice Department personnel, all with a singular objective to gain FISC approval of the applications and certifications. Congress or the FISC could create a straw adversary within the Justice Department to represent the interests of the described targets in an application or those likely affected by programmatic surveillance. The FISC could also be authorized by Congress to appoint cleared counsel to appear in connection with selected applications. Publicly released FISA Court of Review decisions demonstrate the shortcomings of insufficient procedures for those opposed to the government position to participate in the appeals process. Even where security concerns may require closing an argument or other session before the Court in part, an open session for cleared counsel to present arguments in opposition to the
government would assist the FISC or FISA Court of Review in weighing legal arguments and enhance the legitimacy of the otherwise secret process in the eyes of the public.

Congress did not modify the traditional minimization requirements in FISA when it approved programmatic surveillance, and it is surely possible that extensive personal communications of innocent Americans will be retained in government databases for the foreseeable future. It would be possible for the FISC to make rules detailing specific minimization procedures in connection with programmatic orders. With the wall down and basket warrants enabling government access to vast stores of personal records, new rules protecting against abuses in retaining and misusing personal information would help restore confidence in the FISA system. As an Article III court, the FISC likely has authority to so regulate on its own, analogous to the role courts have played in defining other federal judicial rules.

One persistent problem with exceptional courts concerns their expertise. Courts such as the FISC are created to manage a highly secretive and factually nuanced system of surveillance, but the Article III judges eligible for the FISC have no special training in national security surveillance. Although some of those appointed to the FISC have had relevant military experience or have written scholarly articles on electronic surveillance, the FISC judges are not typically expert on the questions they are asked to review. Moreover, FISA itself seriously truncates the judicial role throughout the FISA processes. By and large, the FISC signs off on certifications from the government that collection of foreign intelligence is a significant purpose of the action at issue. The judges find probable cause, but only regarding the target's status as a foreign power, a foreign power's agent, or a lone wolf, and that the facilities targeted are used by the target. The FISC does not assess in any respect whether the approved surveillance will result in acquisition of the foreign intelligence sought. In effect, the FISC is a record keeper – is the government's paper application in order? Under the act as amended for programmatic surveillance, the FISC does even less in measuring the government's application for surveillance to a factual predicate. Instead of probable cause of foreign agency, for example, the FISC only determines that the target is or targets are reasonably believed to be outside the United States.

In programmatic surveillance the FISC may reject a certification only if does not “contain all the required elements,” or the procedures “are not consistent with the requirements” of the act. The FAA does build in audits by inspectors general, and it provides for sharing some reporting information with congressional committees. The FISC, too, may review the programmatic surveillance procedures subject to “the need of the United States to obtain, produce, and disseminate foreign-intelligence information.”

Although the Supreme Court has not decided a FISA case – either on judicial review of a criminal conviction or a challenge to the FISC or its processes – all the lower courts that have heard challenges to the FISA architecture have upheld the scheme. The absence of adversarial proceedings and the use of ex parte processes do not violate the Article III case or controversy requirements, according to reviewing courts. Nor are challenges to FISA orders barred by the political question doctrine. As for substantive complaints, reviewing courts have found that FISA does not violate the Fourth Amendment, the Fifth Amendment's Confrontation Clause, or the First Amendment's free expression protections.

Conclusions

The FISC remains an especially successful exceptional court. It was created to do a job that traditional Article III judges were reluctant to do and that the executive branch preferred be left to them. At the same time, the FISC was created at a time when surveillance abuses cast a shadow over the integrity of these important foreign-intelligence activities. In the years between creation of the court and the 9/11 attacks, the FISC

---

17 Id. § 1821(a)(A) (2010).
18 But see Myers v. United States, 504 F. Supp. 2d 1023 (D. Or. 2007) (finding Fourth Amendment violation), rev'd, 588 F. 3d 1252 (9th Cir. 2009).
developed some expertise in foreign-intelligence surveillance and the court gained considerable respect from observers inside and outside government. Although the secrecy of the FISC and its processes produced a measure of skepticism about what the court actually did behind closed doors, reviewing courts and others that followed the surveillance activities closely were assured that the FISC approved electronic surveillance only when its primary purpose was the collection of foreign intelligence.

The combination of the criminalization of many terrorist activities and the digital revolution in communications and surveillance capabilities altered the role of the FISC and, following the 2008 amendments to FISA, strained its credibility as an independent arbiter of lawful FISA surveillance. The use of FISA processes to build criminal cases is regrettable, in my view, but the lowering of the wall between law enforcement and intelligence-gathering has been supported by the FISA Court of Review and there is considerable momentum behind the use of FISA in building criminal cases. The programmatic surveillance now sanctioned by the FISC is more problematic, however, because the special court has assumed more of a clerical function than a judicial role. There remain opportunities to revise minimization rules, either through new legislation or FISC rulemaking, and to make government retention or dissemination of private information about innocent persons less likely. At the same time, if we must tolerate sweeping digital collection of our personal data, the FISC should have greater and more meaningful opportunities to oversee its collection — if not in advance, then after the fact.
Article

The Death of FISA

William C. Banks

Introduction .................................................. 1209
I. The Origins of FISA ........................................ 1211
II. Foreign Intelligence Surveillance Act Practice Up to September 11 ........................................ 1211
A. The Collapse of the Foreign Intelligence Purpose Rule ........................................ 1211
B. Avoidance of FISA: The Terrorist Surveillance Program ........................................ 1211
C. Synthesizing the Post-September 11 Developments: The Death of FISA .................... 1211
   1. The Wall ........................................ 1211
   2. Statutory Obsolescence and Lone Wolf ........................................ 1211
III. The Post-September 11 Changes ................. 1211
A. The Collapse of the Foreign Intelligence Purpose Rule ........................................ 1211
B. Avoidance of FISA: The Terrorist Surveillance Program ........................................ 1211
C. Synthesizing the Post-September 11 Developments: The Death of FISA .................... 1211
   1. The Wall ........................................ 1211
   2. Statutory Obsolescence and Lone Wolf ........................................ 1211
IV. The Future Prospects ...................................... 1211
A. FISA and Modern Technology .......................... 1211
B. Is the TSP Lawful? ...................................... 1211
C. Proposals to Amend FISA ................................. 1211
D. Can FISA Be Saved? ..................................... 1211
   1. Minimization Reform? ................................ 1211
   2. An Exclusionary Rule for FISA? ...................... 1211
   3. Improved Oversight of FISA Activities .......... 1211
   4. Revisions to FISA to Accommodate the TSP ...... 1211
Conclusion .................................................. 1211

Blinded by dizaying technical advances in surveillance, and by the politics of the post-September 11 emergency, Congress

appears poised to grant the twenty-first century equivalent of eighteenth century general warrants—allowing the executive to conduct national security surveillance at will. Even if Congress does not grant such sweeping discretion by statute, arguably the modern general warrant is with us now, by order of the President. Just as English law permitted the searcher to "break into any shop or place suspected," the executive branch has invoked the specter of additional terrorist attacks against the United States to justify sweeping electronic surveillance of Americans, without judicial approval and outside the bounds of any statute. Within days of September 11, Attorney General John Ashcroft stated that the Department of Justice would thereafter be guided by a "paradigm of prevention," or preventive enforcement, where every resource would be devoted to early anticipation of potential terrorist plots. Over the last five years, the determination that the United States cannot wait until terrorist plots are fully developed and operational before they are stopped has become an established part of the counter-terrorism landscape, while the rise of preventive enforcement as a preferred counter-terrorism approach is a dominant theme in the Department of Justice strategy statements.

1. General warrants were given to agents of the Crown, permitting wholesale rummaging of the houses and businesses of political opponents. Following a history of such abuses under Charles I, the courts struck down general warrants as unconstitutional in Ex parte J. W. and J. K. (1817) and in Ex parte D. (1824).
4. See id.
THE DEATH OF FISA

One of the most useful tools available to the government to learn about terrorist plans before they mature has been the Foreign Intelligence Surveillance Act (FISA). Whether the strategy is to arrest the targets of surveillance early, or to continue monitoring in the hopes that more serious and sophisticated terrorists might enlist others as decoys or assets in a more concrete and more nearly operational plot, FISA permits the government to keep tabs on the targets without their ever knowing about the surveillance.6

Enacted in 1978, FISA resulted from an interbranch compromise. Until then, no president had ever conceded that the Congress could interpose any set of procedures to confine the constitutional discretion of the president to engage in electronic surveillance to protect the national security. However, beginning in the 1960s, the Supreme Court recognized an emerging constitutional right of privacy that is implicated when government conducts electronic surveillance, and courts began to limit warrantless electronic surveillance.8 Seen therefore, the Wa-
At the same time, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (Patriot Act) and rewritten FISA guidelines modernized FISA to account for new technologies and changing tactics in the never-ending leap-frog of the technologies of detection and evasion. Despite the Bush administration’s proclaimed satisfaction with the new tools, they secretly circumvented the updated FISA procedures in undertaking a new domestic surveillance program through the National Security Agency (NSA)—the Terrorist Surveillance Program (TSP). Although strong negative reactions followed the media release of the NSA story in December 2005, the administration has made legal arguments to justify not following

643

17. Part III.A infra, considers the effect of the change from “the purpose” to “a significant purpose” in FISA.
22. See discussion infra Part IV.A.
24. 1214 MINNESOTA LAW REVIEW [91.1209]

ing FISA while it supports amendments to the act that would eviscerate it. The administration has repeatedly stated that the TSP is limited to situations where one end of the communications captured is a known or reasonably suspected affiliate of al Qaeda, but those assurances are not subject to independent verification outside the executive branch. In any case, if the TSP can work around FISA for one programmatic purpose, it would be difficult to stop other such evasions of the FISA scheme. One way or the other, it looks like FISA is dead.

This Article is a requiem for FISA, and a plea for our government to restore the constitutional values that FISA wisely straddled—promoting national security while safeguarding civil liberties. FISA may have been doomed from the start because of its complex formulations regarding who the government may target, how the government must construct the applications, and how the government must minimize its dissemination of information collected. Still, its core set of requirements, and the judicial procedures to enforce them, remained in place until 2002. Even before September 11, and exponentially more so since then, a growing criminalization of terrorism-related activities has made the prosecutorial agenda a larger part of the sphere of electronic surveillance, and has accordingly further complicated the task of managing FISA implementation. With the long list of amendments enacted in the Patriot Act in 2001, and some others before and since then, the original deal from 1978 may have collapsed under its own weight. Whether from its cumulative complexity, the challenges of new technologies, or the efforts of the Bush administration after September 11 to curtail and circumvent its provisions, the
central premise of the FISA compromise—authorizing secret electronic surveillance for the purpose of collecting foreign intelligence, but subjecting applications to judicial scrutiny and the entire process to congressional oversight—has been lost.

The change in the purpose requirement and dismantling of the procedural wall in 2002 all but eliminated the protection against skirting Fourth Amendment requirements when misusing FISA to develop evidence for prosecution. FISA became something that it was never intended to be—an alternative to the traditional law enforcement procedures for building a criminal case against alleged terrorists that circumvents constitutional requirements. The TSF is, in some ways, even worse. Unless the executive branch has the constitutional authority to go around FISA, the TSF is a stark violation of limits on surveillance set by Congress. Instead of taking steps to resign in the NSA program, however, Congress is poised either to authorize open-ended and untargeted surveillance programs, or simply to make the FISA procedures optional. Even if Congress takes no action to authorize or regulate the TSF, it will be acquiescing in electronic surveillance activities that lack statutory authority.

Part I reviews the origins of FISA, the modern problems that demand secret surveillance capabilities, and the constitutional and political backdrop for the legislation. It also briefly sets out the statutory provisions and its structure. Part II examines the practice under FISA before September 11, particularly the developments that led to the erection of the wall between law enforcement and foreign intelligence. Part III reviews post-September 11 changes, focusing on the changes in the Patriot Act that led to the dismantling of the requirement

29. See Banker, supra note 16, at 1174-84.
30. See id.
31. See Bann & Laidler, supra note 28.
32. Part IV.C. discusses the congressional response to the NSA program.
34. See Banker & Brown, supra note 1, at 16-17.
38. See PATRICK BAHRING, FRONTIER DEPARTURES FROM THE SE-
THE DEATH OF FISA

2007] 1217

Now that terrorism has overtaken espionage as the domi-
nant investigative concern in protecting the national security, we have come to real-ize that terrorism presents difficult chal-}
go. Experience has shown that our criminal laws and traditional law enforcement methods cannot
provide sufficient protection against terrorism.\(^{39}\) Arrest and prosecution have proven successful in some instances, some-
times before and at other times after the planned terrorist\(^{40}\) but the risk that grave harms may occur from a terrorist
attack—another September 11, for example, or a biological weapons attack—forces us to look for other preventive tools.
Over time, these investigative techniques have anticipated and prevented many plots that would have harmed Americans.\(^{41}\)

Consider these examples:

In 1982, as part of an ongoing investigation of Armenian terrorist groups, FBI agents in Los Angeles monitored a court-
authorized electronic surveillance of a home in Santa Monica, trying to learn more about a suspected plot by an Armenian

group to bomb the Honorary Turkish Consulate in Philadel-
phia.\(^{42}\) During the course of the surveillance, the FBI learned
that the targets of the surveillance were building a bomb.\(^{43}\) Al-
though the plotters managed to transport dynamite inside
checked luggage on board a United States commercial
airliner, the suspects were arrested before the bomb was moved to its intended target.\(^{44}\) Criminal convictions were obtained,
and the evidence at trial included tape recordings and logs of the
electronic surveillance that had been undertaken for the purpose of
obtaining foreign intelligence.\(^{45}\)

In 1981, U.S. citizens affiliated with the Provisional Irish
Republican Army (PIRA) sought out a seller of surveillance and

39. See Banks & Newman, supra note 1, at 6-10 (noting that the goal of
national security—to prevent criminal activity before it occurs—is difficult to reconcile with criminal law's legal standards).
40. See Chomsky, supra note 17, at 26-27.
41. Hearing on U.S. Federal Efforts to Combat Terrorism Before the S.
Com. on Appropriations, Subcommittee on Commerce, Justice, State, the Hol-
gaggiement/09_09_01.htm.
42. United States v. Sarkesian, 841 F.2d 939, 961 (9th Cir. 1988).
43. Id.
44. Id. at 962.
45. Id. at 360-43.
2007] THE DEATH OF FISA 1219

From December 2001 until August 2003, Hemant Lakhani met several times in person and had telephone conversations with an FBI informant who posed as an arms dealer.\textsuperscript{54} In 2005, a New Jersey federal jury convicted Hemant Lakhani, an Indian-born United Kingdom national, for attempting to provide material support to terrorists and for his role in trying to sell an anti-aircraft missile to a man whom he believed represented a terrorist group intent on shooting down a United States commercial airliner.\textsuperscript{55} Recordings of the conversations and meetings became part of the evidence in the criminal case against Lakhani.\textsuperscript{56}

At its most effective, electronic surveillance captures conversations and movements about plans to commit a terrorist act and thus allows the government to step in before the crime occurs. Of course, electronic surveillance may also impose a heavy cost. An array of personal privacy and expressive freedom interests are threatened by electronic surveillance, especially surveillance that is undertaken on a long-term, 24/7 basis.\textsuperscript{57} Those who know or suspect the government of monitoring their conversations self-censor their conversations, inhibiting free-flowing expression.\textsuperscript{58} Individual interests in anonymity are compromised, as are self-determination choices and freedom of association.\textsuperscript{59} As the Supreme Court has noted, electronic surveillance for national security purposes may also implicate a "convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime," when it targets those whose activities are politically motivated.\textsuperscript{60} Government interests may be stronger in these areas, but there is also a greater risk of jeopardizing protected expression.\textsuperscript{61}

The use of traditional law enforcement techniques brings along with it traditional Fourth Amendment requirements, including the need to establish that a crime has been committed


\textsuperscript{55} This American Life: The Arms Dealer, supra note 55.


\textsuperscript{57} Id at 495.

\textsuperscript{58} See id at 491–99.


\textsuperscript{60} Id.

\textsuperscript{61} Id.

1220 MINNESOTA LAW REVIEW [91:1209

or is imminent before a judge will issue a warrant to conduct electronic surveillance.\textsuperscript{62} Because of the gravity of the threat of terrorism and the consequences of those acts, the government has sought the authority to undertake surveillance with something less than the criminal law standard.\textsuperscript{63} The grave danger of international terrorism arguably justifies the more permissive FISA regime, and the privacy intrusions are limited to the collection of information for foreign intelligence purposes. At the same time, foreign intelligence collection tends to be programmatic, focusing on nascent schemes and following up on ambiguous leads.\textsuperscript{64} In addition, terrorism in a loosely defined cell structure are hard to identify in general, and they are typically trained not to engage in criminal conduct that would justify the criminal warrant of electronic surveillance.\textsuperscript{65} Ordinary crimes electronic surveillance requires that an application for a warrant contain detailed information about the alleged criminal offense, the facilities and communication sought to be intercepted, the identity of the target (if known), the period of time sought for the surveillance, and an explanation of whether other investigative methods could achieve the objective.\textsuperscript{66}

The need for secrecy and the often more open-ended purpose of monitoring a target for foreign intelligence makes the ordinary crimes warrant procedures ill-suited for foreign intelligence gathering.\textsuperscript{67} Clearly, somewhat less than a completed act of international terrorism should be required before launching electronic surveillance in pursuit of foreign intelligence.\textsuperscript{68} However, deciding just how much evidence of a connection of a potential target to a terrorist group or to terrorist activities should be required is a nettlesome problem.\textsuperscript{69} Without suffi-


\textsuperscript{63} Hanso & Bowman, supra note 1, at 8–10 (discussing the difference in the legal standards for surveillance of terrorists and ordinary crimes (investigation)).

\textsuperscript{64} Hanso & Bowman, supra note 1, at 1145 (discussing new legislative tools to facilitate intelligence-gathering and analysis).


\textsuperscript{68} Id at 4, supra note 7, noting that national security investigations are bound by different probable cause standards than criminal investigations as a result of their unique objectives.

\textsuperscript{69} Id at 5–10.
cient controls, electronic surveillance is an especially ominous form of investigation because, in a digital world, it records and may store and retrieve forever not just the information that investigators seek but everything that the target communicates, no matter how unrelated to the purpose of the surveillance.71 The metaphor commonly associated with electronic surveillance is the net that captures everything.72 If not leavened with controls, electronic surveillance may become the contemporary equivalent of the eighteenth century English general warrant. The general warrant was abandoned in England, but English law did not recognize a right of privacy.73 As similar overreaching by Crown agents persisted in the colonies through the use of writs of assistance, colonists lacked a legal remedy.74 It was thus hardly a surprise that the Bill of Rights would include in the Fourth Amendment protection against the abuses of general warrants.75

Of course the Framers could not foresee the problems that would arise in adapting the Fourth Amendment to electronic surveillance. How should its two clauses— the protection against "unreasonable searches and seizures"76 and the warrant requirement77—apply to electronic surveillance? Must pursuit of foreign intelligence follow the Fourth Amendment rules at all, if undertaken inside the United States? If the Fourth Amendment does not offer clear guidance, may Congress legislate to implement and clarify its requirements for gathering information about international terrorists? Applied to the gathering of foreign intelligence, electronic surveillance offers those same advantages of being able to watch and listen without limitation and to learn about espionage or terrorist activities that may be only in the planning stages. As electronic surveillance became a common tool of law enforcement, as did it enter the world of intelligence investigations in the United States, first by the FBI and then later by the CIA and other intelligence agencies.78 As countering terrorism became a central national security challenge, the investigative community was faced with the reality that its purposes in investigating might simultaneously be gathering foreign intelligence and enforcing the criminal laws.79 While the rules for the two types of investigation look very much alike, they differ in some important respects, and they historically remained separate from one another, to protect the integrity of each one.80

Only in 1967 did the Supreme Court hold that the Fourth Amendment warrant clause applies to electronic surveillance.81 In Katz v. United States, the Court also held that warrantless searches "are per se unreasonable . . . subject only to a few specifically established and well-delineated exceptions."82 At the time, no foreign intelligence or national security exception had been so recognized, although the Katz Court expressly declined to extend its holding to cases "involving the national security."83 In 1969, Congress responded to Katz and enacted legislation creating procedures for judicial authorization of electronic surveillance in law enforcement investigations,84 but the legislation explicitly noted that Congress did not intend to set rules for national security investigations.85

In 1972, the Supreme Court addressed electronic surveillance in a national security setting for the first time. In United States v. United States District Court (Keith),86 defendants charged with conspiring to bomb a CIA office in Ann Arbor, Michigan, sought in pretrial proceedings electronic surveillance logs that the government had obtained without a warrant.87 The government admitted that a warrantless wiretap had in

72. Id. at 495 (noting that electronic surveillance also records behavior and social interaction).
73. Note & Newman, supra note 1, at 3.
75. U.S. CONST. amend. IV.
76. Id.
77. Id.
79. See, e.g., id at 9 (noting that terrorism is the exception to the general rule).
80. Id. at 8-9.
82. Id. at 108.
83. Id. at 108 n.33.
86. 407 U.S. 297 (1972). This case is typically known as the Keith decision, after Damon Keith, the district court judge who presided over the case.
87. Id. at 399-300.
intercepted conversations involving the defendants, but it defended the wiretaps on the basis of the Constitution and a disclaimer in the 1968 Crime Control Act.

The Court first rejected the statutory argument. The government argued that the provision of the 1968 Crime Control Act regulating electronic surveillance for domestic law enforcement purposes that excluded from its coverage surveillance carried out pursuant to the 'constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack . . . [and] to obtain foreign intelligence information deemed essential to the security of the United States' expressed an intention to allow unmonitored electronic surveillance for national security purposes. According to the Court, the disclaimer conferred no new authority and simply left presidential powers untouched.

The Court found authority in the oath clause for the power 'to protect our Government against those who would subvert or overthrow it by unlawful means.' However, the Court determined that the President must exercise the Article II authority consistently with the Bill of Rights. Although the Attorney General had personally approved the wiretaps and claimed that he had exercised the President's powers to protect the nation against the threat that domestic organizations would attack the government, the Court held that domestic national-security wiretaps required a warrant issued by a neutral magistrate. The Court relied on the 'broadest spirit' of the Fourth Amendment and found that the 'convergence of First and Fourth Amendment values' justified special warrants when the government undertakes national security wiretapping. In arriving at its holding, the Court balanced the 'duty of Government to protect the domestic security' against the potential danger posed by unreasonable surveillance to individual privacy and free expression.

Writing for the Court, Justice Powell concluded that waiving the Fourth Amendment prohibition requires a case-by-case examination and allowing 'unreviewed executive discretion' to be exercised could cause the executive to 'yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.'

Although the government cited the unique characteristics of ongoing national-security surveillance and its fear that leaks could undermine the sources and methods of intelligence collection, the Court refused to recognize an exception to Katz for national security surveillance. The Court took note of the potential for abuse of warrantless surveillance and it noted that courts had the capacity to manage sensitive information and could protect intelligence sources and methods through ex parte proceedings. At the same time, Justice Powell emphasized that the case involved domestic targets of surveillance and that the Court expressed no opinion on the executive discretion to conduct such surveillance when foreign powers or their agents are targeted. In addition, the Court expressly reserved the question whether similar rules should govern foreign intelligence surveillance and, after noting the 'different policy and practical considerations from the surveillance of ordinary crime' in investigating national security, the Court supplied a back-handed invitation for Congress to legislate a set of rules for what remained an uncertain term—national security investigations—for domestic and foreign intelligence.

Meanwhile, after Kiehl, two courts of appeals upheld the constitutional authority of the executive branch to conduct warrantless electronic surveillance in pursuit of foreign intelligence. However, the Court of Appeals for the District of Columbia decided a high-profile case at the edges of the post-Watergate prosecution of the White House—ordered break-in of

86. Id. at 308.
89. Id. at 307.
90. § 902, 82 Stat. at 214. The Kiehl Court interpreted the provision as having 'left presidential powers where it found them.' 407 U.S. at 303.
91. Id. at 308.
92. U.S. CONST. art. II § 1.
94. Id. at 312-13.
95. Id. at 300-01.
96. Id. at 325-26.
97. Id. at 312.
the Democratic Party headquarters, in United States v. Erhartman. Ehrlichman, the former Chief of Staff to President Nixon, argued that the activity he had authorized was a national security, counterintelligence operation, and therefore not illegal. Although the court held that Ehrlichman could not rely on such a defense because he "could not show presidential authorization... two of the three judges wrote a separate concurrence [to say that] no intelligence or counterintelligence exception to the Fourth Amendment existed." 110

FISA was the product of a set of compromises unique to their time. The executive branch wanted a continuing discretion to employ wiretapping for foreign intelligence, unchallenged by judicial or congressional oversight. Because Ehrlichman was a domestic security case, the door was not shut. In addition, because Ehrlichman acknowledged a possibility that the rules might be different for foreign intelligence and the 1968 Crime Control Act proclaimed prescribing any rule for foreign intelligence gathering, it remained plausible to argue that the executive might make its own rules for collecting foreign intelligence. The executive branch's position was weakened considerably, however, by the effects of the Watergate scandal, lawsuits challenging warrants surveillance, and the practical problem that telephone companies and government agencies were unwilling to approve electronic surveillance without a court order. There were, in addition, high profile investigations of illegal spying by intelligence agencies, including by the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities (the Church Committee). The Church Committee reviewed nearly forty years of domestic

110. Diane Carverly Pinto & Joseph Rodack, Parrying the "Historical Mind": The People and Events Behind the Passage of FISA and the Creation of the "Rota" 17 Stan. L. & Pol'y Rev. 431, 434 (2006).
111. 459 F.2d 754 (D.C. Cir. 1972).
113. See Banker & Bowman, supra note 1, at 50–52.
114. Pinto & Rodack, supra note 109, at 440; see also 427 U.S. at 272 in Amended the National Security Act of 1947 to Improve U.S. Counterintelligence Measures Hearing Before the Select Comm. on Intelligence of the Senate, S. 101st Cong. 136 (1990) (testimony of Harry Lebow, Counsel, Office of Intelligence Policy and Review, U.S. Department of Justice) (Electronic surveillance can only be done with Department of Justice approval). 115. 564 F.2d 835, 838 n. 1 (D.C. Cir. 1977) (unpublished) (describing the investigatory committee that reviewed intelligence activities).
2007] THE DEATH OF FISA 1227

- Intelligence files on more than 15,000 individuals and 
groups were created by the Internal Revenue Service be-
tween 1969 and 1972 and ten investigations were started 
on the basis of political rather than tax criteria.
- At least 20,000 individuals were at one point identified as 
an FBI list of people to be rounded up in the event of a "na-
tional emergency." 114

The Committee elaborates:
Sines the 1930s, intelligence agencies have frequently 
intercepted and tagged American citizens without the benefit of a judicial war-
rant. The application of vague and elastic standards for warrant-
generating and tagging has resulted in electronic surveillance which, by 
any objective measure, were improper and seriously infringed the 
Fourth Amendment Rights of both the targets and those with whom 
the targets communicated. The inherently intrusive nature of elec-
tronic surveillance, moreover, has enabled the Government to gener-
ate vast amounts of information—untethered to any legitimate 
official interest—about the personal and political lives of American 
citizens. ... Also formidable ... is the chilling effect which warr-
antless electronic surveillance may have on the constitutional rights 
of those who were not targets of the surveillance, but who perceived 
themselves, whether reasonably or unreasonably, as potential tar-
gets. 115

Watergate, the Church Committee and other investigative 
reports emboldened Congress to control executive overreaching 
in its use of surveillance. According to the Senate Judiciary 
Committee, the bill that became FISA was "designed ... to 
curb the practices by which the Executive Branch may conduct 
warrentless electronic surveillance on its own unilateral 
determination that national security justifies it," but to authorize 
the use of electronic surveillance to obtain foreign intelligence 
information. 116 Civil liberty groups, such as the ACLU, wor-
ed that if Congress set a warrant standard too low, it could 
end up "authorizing rather than curtailing intelligence agency 
abuse." 117 In other words, would no legislation be better for 

114. Id. at 6-7.
116. Id. at 6-8.
Problems of Select Committee on Intelligence, Report, Vol. 12, p. 35 (1977). The idea 

MINNESOTA LAW REVIEW [91:1209

1228

civil liberties than bad legislation? At the same time, Congress 
recognized that "no person should be targeted for electronic 
surveillance unless the Government has evidence they are en-
gaging in criminal conduct which directly threatens national 
security." 118 Even though evidence of national security crimes 
could be collected during the electronic surveillance. While this 
suspicion of criminal activity was an essential part of what 
would become the FISA provisions that apply to United States 
citizens, Congress did not intend for FISA to authorize surveil-

118. Id. at 1.
119. Id. at 1.
120. Id. at 1.

After six years of hearings and discussion and through the 
steeredhip of Attorneys General Edward Levi and Griffin 
Bell, Presidents Gerald Ford and Jimmy Carter, and several 

members of the House and Senate, FISA became law in 
1978. 119 In his signing statement, President Carter said:

The bill represents, for the first time, a prior judicial warrant for 
electronic surveillance for foreign intelligence or counterintelligence 
uses and national security purposes in the United States in which communications of U.S. per-
sone might be intercepted. It clarifies the Executive's authority to 
retain foreign intelligence by electronic surveillance in the United 
States. It will require the courts to act as an independent safeguard, for 
the Executive Branch's activities that 

119. Id. at 1.

proponents and opponents of national security electronic surveillance legisla-
tion.

120. FISA Hearing, supra note 121, at 92.
121. See supra notes and text, at 1190.
122. Senate Select Comm. on Intelligence, The Foreign 
123. Id. at 1.
FISA's authorization of electronic surveillance of "foreign powers" and their agents, terms taken from the Supreme Court in Aziz v. United Nations reflects the Act's focus on foreign intelligence. From the beginning, the definition of "foreign power" has included "a group engaged in international terrorism or activities in preparation thereof." An "agent of a foreign power" included a person who "knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power." The term "foreign intelligence information" was defined 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 or international terrorism by a foreign power or an agent of a foreign power;
(c) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power;
(d) information 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.

Non-United States persons (someone not a citizen or permanent resident, among others) could be an "agent of a foreign power" by being an officer or employee of a foreign power, or a member of an international terrorist organization. The government could target United States persons as agents only if they knowingly engaged in certain activities, including international terrorism which "involve or may involve a violation of the criminal statutes of the United States." The FISA process authorizes "electronic surveillance," which is broadly defined and must fall within one of four categories:

(3) the acquisition by an electronic, mechanical, or other surveill-
put in place a much more government-friendly process. Instead of a neutral magistrate finding probable cause to believe that a particular crime has been, is being, or is about to be committed and then issuing a warrant that is later noticed to the target,\(^{117}\) FISA authorizes a special court, the Foreign Intelligence Surveillance Court (FISC), that meets in secret, ex parte.\(^ {118}\) To permit electronic surveillance without the target ever learning that she was a target, based on a showing that pursuit of foreign intelligence is a significant purpose of the surveillance, and that there is probable cause to believe that the target is a foreign power or agent of a foreign power.\(^ {119}\)

The target may eventually learn of the FISA targeting only if the FISA surveillance is used by the government in a criminal or other proceeding against him before its use against the target.\(^ {120}\) Only the judge reviewing the lawfulness of the surveillance sees the surveillance logs, in person.\(^ {144}\) Applications to the FISC must pass through layers of review inside the Justice Department and obtain the approval of the Attorney General.\(^ {145}\) The order must describe in some detail the targets of surveillance and the places where surveillance will occur.\(^ {146}\) Time limits are set for the surveillance, although there are opportunities to extend the time.\(^ {147}\) Also, once the statutory findings are made by the FISC, the judge “shall” issue the surveillance order.\(^ {148}\)

To reduce the chance that FISA surveillance could interfere with the rights of U.S. persons, FISA requires “minimization procedures” that the Attorney General must adopt in order to curtail acquisition and retention and prohibit dissemination of nonpublic information about U.S. persons.\(^ {149}\) In essence, FISA forbids disclosing information obtained from FISA surveillance except as provided in the minimization procedures.\(^ {150}\) Although “information that is evidence of a crime which has been, is being, or is about to be committed can be retained or disseminated for law enforcement purposes.”\(^ {151}\)

To underscore that Congress intended this new scheme to replace entirely the previously unregulated electronic surveillance practices of the executive branch, federal law includes a provision stating that its procedures, along with those prescribing rules for law enforcement surveillance, provide the “exclusive means” of engaging in electronic surveillance.\(^ {152}\) The provision also clarified that the exclusivity provision does not cover other foreign electronic surveillance conducted abroad, including any such surveillance that targets U.S. persons.\(^ {153}\) Another FISA provision makes it a crime to conduct electronic surveillance “except as authorized by statute.”\(^ {154}\)

FISA also includes authorization for surveillance outside the FISA process for up to one year when directed solely at ‘communications transmitted by means of communications used exclusively between or among foreign powers’ and there is ‘no substantial likelihood’ that communication involving a U.S. person will be acquired.\(^ {155}\) However, this is a narrow exception.
to the default FISA process. Because this exception for programmatic surveillance is allowed only for direct foreign government communications, it does not allow surveillance outside the FISA process when foreign powers use public communication networks. Congress built into law two other exceptions to the exclusivity of the FISA process gathering for foreign intelligence. One section permits surveillance outside FISA for up to fifteen days following a declaration of war, and the other permits the Attorney General to certify that "an emergency situation exists" that requires electronic surveillance before an order from the FISC could be obtained. The emergency authority may be exercised for up to seventy-two hours from the time authorization is made by the Attorney General, until the information sought is obtained, or until the FISC denies the application for surveillance, whichever is earlier. The emergency procedures still demand an application to a judge, but it is not required until seventy-two hours after the emergency authorization.

Although the scheme was complex, the compromise struck a fundamental balance. Those most worried about the abuses of past presidents and their subordinates took comfort in the regulation of foreign intelligence surveillance that included Article III judges, albeit to a limited extent. The secrecy, ex parte proceedings, and corresponding lack of notice to the targets was troubling, but at least the procedures were prescribed by law. From the executive branch and intelligence investigators' perspectives, what was done in the past on the basis of supposed inherent constitutional authority was now subject to rules imposed by Congress, but once learned and followed, the rules felt legitimacy to secret surveillance.

II. THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: PRACTICE UP TO SEPTEMBER 11

Between 1978 and the early 1990's, FISA operated to the satisfaction of the primarily involved institutions, and it changed only incrementally. FISA applications grew in number during this period, although the growth was modest until 1995 (following the first World Trade Center and Oklahoma City

154. Id. (emphasis added).
155. Id. § 1805(e).
156. Id.
develop inside the Department. Their office sought to make FISA applications detailed and complete.194 When OIPR delivered applications to the FISC, the department could represent that it sought electronic surveillance in pursuit of a "foreign intelligence" purpose, not to spy on political enemies or to end-run the magistrate in building a criminal case.195

As the federal courts admitted FISA-obtained evidence in criminal prosecutions after finding that the primary purpose of the investigation was to collect foreign intelligence, OIPR performed its gatekeeping role to assure that the Department of Justice followed FISA procedures. Under OIPR head Mary Lawton, who ran OIPR from 1992 until her sudden death in 1999, OIPR operated without written guidelines.196 Although Lawton believed that some things were better "left undefined," she and OIPR made sure that the intelligence and law enforcement personnel regularly consulted one another.197 The 9/11 Commission Report and an Inspector General's report on the FBI and intelligence related to the September 11 attacks concluded that, from the inception of FISA through the early 1990's, "prosecutors had informal arrangements for obtaining information gathered in the FISA process,"198 and that "prosecutors within the Department's Criminal Division . . . had to be consulted in connection with intelligence investigations in which federal criminal activity was uncovered, or when legal advice was needed to avoid investigative steps that might inadvertently jeopardize the collection of information obtained from the intelligence investigation."199

Gradually, the insistence of OIPR and the FISC on fulsome FISA applications resulted in more elaborate procedures, including those that separated law enforcement and intelligence agents and activities.200 Although implementation of the FISA purpose requirement was to some extent responsible for develop-

agency/index/index.html (last visited Apr. 12, 2007).
195. Id.
196. See Pinna & Blake, supra note 100, at 489-502.
197. Id at 451-52.
200. Id at 25-27.

913: 1209

MINNESOTA LAW REVIEW

opposing what evolved into a "wall," to a large degree the barriers between successful intelligence and law enforcement cooperation and sharing were due to a perennially cumbersome FBI bureaucracy, an equally bad FBI computer system, and a culture inside the Criminal Division and intelligence units of the FBI that simply nurtured separation.201

For several years, the OIPR role in managing the FISA process evolved without major incidents.202 However, during the Aldrich Ames espionage prosecution in 1994, back-channel cooperation between the CIA and FBI prompted OIPR to advise the Attorney General that the close CIA/FBI collaboration in the Ames investigation could provide Ames' lawyers with an argument that the FISA warrants were missing.203 Ames accepted a plea bargain, so no test of the OIPR concern was presented to a judge.204 Still, the Justice Department was put on notice that back-channel consultations between its intelligence and law enforcement officials could be problematic.

Inside the Justice Department, Deputy Attorney General Jamie Gorelick convened a working group to reconcile emerging differences of opinion between OIPR, the Criminal Division, and FBI over "wall" issues.205 The working group sought an opinion from the Office of Legal Counsel (OLC) on the question of whether the FISC could approve a search under FISA only when the collection of foreign intelligence was the "primary purpose" of the search, or whether it sufficed that such collection was one of the purposes.206 In February 1996, the OLC "concluded that "courts are more likely to adopt the 'primary purpose' test than any less stringent formulation.'"207 Based on

170. Schulhofer, supra note 103, at 523-26 (FISA's "purpose requirement" was a "wall" from which "intelligence-driven shares developed. For the resulting problems were not inescapable, even under the law as it stood before 9/11); most of the difficulties could have been avoided with better training and more common sense, and more willingness to tolerate ambiguity and decentralized discretion.")
171. See 9/11 COMMISSION REPORT, supra note 107, at 78.
172. Id.
174. See 9/11 COMMISSION REPORT, supra note 107, at 78.
the FISA case law. OLC determined that "the greater the invol-
volve of prosecutors in the planning and execution of FISA
searches, the greater is the chance that the government could
not assert in good faith that the 'primary purpose' was the col-
lection of foreign intelligence." OLC thus recommended that
"an appropriate internal process" should be established "that
FISA certifications are consistent with the 'primary purpose'
test."116

Meanwhile, to assure that misuse of FISA did not occur,
OIPR began imposing information-sharing controls on its own
initiative.117 The working group made recommendations to
Deputy Attorney General Gorelick, who in turn submitted them
to Attorney General Reno.118 In March 1993,119 Gorelick wrote
a memorandum prescribing special "wall" procedures for two
pending cases, including the 1993 World Trade Center bombing
prosecution.120 The memorandum instructed that the intel-
ligence investigation in the New York case would go forward
"without any direction or control"121 by the U.S. Attorney's
office or the Criminal Division, and it required FBI headquarters
or OIPR approval to share some portions of intelligence inves-
tigative memoranda with law enforcement agents.122 In addi-
tion to these "wall" procedures, the March memorandum
also encouraged cooperation and coordination between the intel-
ligence and law enforcement personnel in a few particular
ways.123 According to a 2004 Office of the Inspector General re-
port, the March memorandum from Gorelick was somewhat
misconstrued and its "wall" procedures were applied through-
out the FBI for all FISA applications by 1997.124 Notably, the
restrictive procedures in the Gorelick memorandum exceeded
any requirements imposed by FISA or case law.125

The, in July 1993, Attorney General Janet Reno issued a
set of secret internal guidelines to prescribe procedures for con-
tacts among the Justice Department's Criminal Division, the
FBI, and OIPR.126 Contacts between the prosecutors and their
investigators and intelligence officials were limited, logged, and
noted to the OIPR.127 Those entities could exchange
consultations and advice, but the contacts should "not inadver-
tently result in either the fact or the appearance of the Crimi-
nal Division's directing or controlling" an investigation.128 The
guidelines were not written to affect contacts and informa-
tion-sharing between investigating agents—internal to the Criminal
Division or between criminal and intelligence investiga-
tors—but instead were intended to apply only between investigators
and prosecutors.129

According to a later Office of the Inspector General Report,
the OIPR lawyers almost immediately misconstrued and mis-
interpreted the 1993 guidelines as containing the special pro-
cedures imposed in New York by the March Gorelick memoran-
dum, thus interpreting FISA as essentially prohibiting contact
between the law enforcement and intelligence sides of an inves-
tigation.130 Coordination between law enforcement and intelli-
gence officials that had occurred before 1993 fell off after issu-
ance of the guidelines, and such contacts that did occur came so

117. See Gorelick Memos, supra note 182, at 2 (explaining that the re-
mended procedures "go beyond what is legally required").
118. See Memorandum from Janet Reno, Attorney Gen., to Assistant At-
torney Gen., Criminal Div., et al. (July 13, 1993) (regarding "Procedures for Contacts Between the FBI and the Criminal Division Concerning Foreign In-
telligence and Foreign Counterintelligence (intelligence investigations)"); available at http://
119. See id.
120. Id. at 18.
121. 9/11 COMMISSION REPORT, supra note 167, at 79; see also LAWRENCE
WEINER, THE LOOKING TOWARD AL-QADA: AND THE ROAD TO 9/11, at 343
(D2005) ("The Justice Department promulgated a new policy in 1995 designed
to regulate the exchange of information between agents and criminal prosecu-
itors, but not among the agents themselves").
122. 9/11 COMMISSION REPORT, supra note 167, at 79 ("[T]he procedures
were almost immediately misconstrued and misapplied"); 2004 OIG REPORT,
 supra note 108, at 93; WAGG, supra note 194, at 249 ("Provisional condi-
tions and criteria allowed the policy to gradually choke off the flow of essential
information . . . .").

128. See id. at 2-3.
late in the process as to be practically useless.\textsuperscript{103} Although not required by FISA, a metaphorical "wall" between law enforcement and intelligence gathering was thus put in place whenever an intelligence investigation suggested some indication of criminal activity.\textsuperscript{104} The FBI then developed a parallel system of "dirty" teams for gathering intelligence and "clean" teams for criminal law enforcement.\textsuperscript{105} The teams could investigate the same target at the same time, but they rarely talked with one another.\textsuperscript{106}

OIPR maintained its gatekeeper role throughout this period—only through it would information pass to the Criminal Division. According to the 9/11 Commission, OIPR sustained its position in part by maintaining it reflected the concerns of the chief judge of the FISC, and that "if it could not regulate the flow of information to criminal prosecutors, it would no longer present the FBI's warrant requests to the FISA Court."\textsuperscript{107} Although the OIPR FISA procedures were revised between 2005 and 2002 to permit consultation between the intelligence and prosecution sides of the FBI "aimed at preserving the option of criminal prosecution," the Criminal Division was not allowed to "direct or control the FISA investigation."\textsuperscript{108} During this period, the FISC approved the OIPR procedures and issued case-specific information screening, which varied with the complexity of the investigation, and sometimes saw the FISC serving as the "wall" between the two sides.\textsuperscript{109} In 1999, a badly managed espionage investigation of Los Alamos

\begin{itemize}
\item See hearing, supra note 75, at 49.
\item See WICHT. supra note 91, at 343 (characterizing the FISC as the "affair of what information could be shared—known as the Wall").
\item Id.; see also Hearing, supra note 15, at 49-50 (describing the problem as leading to decreased coordination on intelligence issues). U.S. Gen. Accounting Office, FBI Intelligence Investigations: Coordination Within, JUSTICE ON CONFRONTATION INTELIGENCE CRIMINAL MATTERS IS LIMITED 4 (2001) [\textsuperscript{110} (The implementation and interpretation of the procedures, led to a significant decline in coordination between the FBI and the Criminal Division.).]
\item 9/11 COMMISSION REPORT, supra note 167, at 79.
\item In re Sealed Case, 310 F.3d 717, 729; In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 319 F. Supp. 651, 610 (FISA Ct. 2000), intraduced by In re Sealed Case, 310 F.3d 717.
\item 9/11 COMMISSION REPORT, supra note 167, at 500 n.83.
\item See id.
\end{itemize}
2007] THE DEATH OF FISA

1241

Patriot Act describing and explaining any fundamental rethinking
of the basic terms of the FISA compromise of interests.207
Two developments merit special attention because, taken
together, they portend the death of FISA—one section of the
Patriot Act208 with its implementation by the FISA Court of
Review and the NSA Terrorist Surveillance Program (TSP).

A. THE COLLAPSE OF THE FOREIGN INTELLIGENCE PURPOSE
ROLE

Until amended by the Patriot Act, FISA required that an
application to the FISC for electronic surveillance had to in-
clude a certification that "the purpose of the surveillance is to
obtain foreign intelligence information."209 As interpreted by
the federal courts between FISA’s implementation and 2001, in
practice the rule was that the "primary purpose" of the FISA
surveillance must be to obtain foreign intelligence.210 If and
when a law enforcement purpose became dominant in an inves-
tigation, FISA required that traditional criminal investigative
rules be followed in order to continue the surveillance.211
In enacting FISA, Congress understood that, in many
situations, intelligence and law enforcement investigators work
side-by-side and that information collected in intelligence gath-
ering becomes evidence in an eventual criminal proceeding.212
In the aggregate, however, foreign intelligence gathering is
programmatic rather than targeting specific individuals for
known or anticipated crimes.213 Intelligence investigations
often continue long after a completed criminal act has been
prosecuted.214 In addition, the product of foreign intelligence
investigations may, at any point in time, appear fragmented

ports accompanied the Patriot Act).
210. See Banks supra note 16, at 1156.
211. See United States v. Truong Dinh Hung, 629 F.2d 998, 915 (6th Cir. 1980).
212. Banks & Bowman, supra note 1, at 6.
213. See Banks, supra note 16, at 1152.
214. Id.
and hard to evaluate to someone in law enforcement.215 The
culture of criminal investigations, including the legal standards
of particularity, criminality, and eventual notice to the target,
has no parallel in the world of foreign intelligence gathering.216
The intelligence gathering and law enforcement spheres
overlapped in 1978, and they overlap to a greater extent now.217
Intelligence investigations turn up leads that provide the
criminal investigators what they need to make a case.218 The
criminal enforcement team may gain intelligence during the
course of their surveillance or in an interrogation.219 However,
as counter-terrorism officials recognized the value of collabora-
tion between intelligence and law enforcement investigators,
they also confronted formidable institutional—not legal—
resistance.220 The tension between the need for secrecy and the
demand to share information is inevitable, long-standing, and
entrenched.221 From the intelligence side, leaks are anathema,
and compromised sources have no value.222 Criminal investiga-
tors and prosecutors work assiduously to avoid tainting prose-
cution evidence through contact with intelligence officials
whose knowledge could render critical evidence inadmissible.223
The law requires the use of law enforcement investigative pro-
cedures if the sole purpose of surveillance is prosecution, and it
permits FISA procedures if the purpose of the investigation is
the collection of foreign intelligence.224 To some extent, the
"wars" procedures grew out of concerns for preserving these base-
line rules.225 By and large, however, the separate institutional
responsible for the separate divi-

215. Id.
216. Id.
217. See infra note 291-299 and accompanying text.
218. See Banks & Bowman, supra note 1, at 6.
219. 9/11 COMMISSION REPORT, supra note 187, at 424.
220. See id at 79 (describing the barriers to information-sharing as the "wall").
221. See Mark J. Lowenthal, INTELLIGENCE FROM SECRETS TO POLICY 18-24 (2002).
223. See id.; WIGGINS, supra note 101, at 205 ("[FIS] personnel tended to be close-mouthed and unfriendly, treating all intelligence or potential evidences

224. See 9/11 COMMISSION REPORT, supra note 187, at 79.
225. See id at 79 (describing the "wall" as an accumulation of "institutional beliefs and practices").
sions for criminal and national security investigations inside the FBI, and they show that the "wall" is much more grounded in cultural or institutional matters than it is in legal concerns. The institutional differences, rivalries, and bureaucracies transcode the FBI and include the CIA and NSA, before and after September 11.

When the failures in information-sharing and cooperation surrounding the September 11 hijackers came to light, the Bush administration determined to lower the supposed barriers and turn loose all the investigative resources available in a paradigm of prevention to complement prosecution and other means of combating terrorism. Initially, the Justice Department proposed an amendment that would have replaced FISA's certification requirement that "the purpose" of surveillance was to obtain foreign intelligence with "a" purpose. According to the Department, the change would eliminate the current need continually to evaluate the relative weight of criminal and intelligence purposes, and would facilitate information sharing between law enforcement and foreign intelligence authorities. Even in the short time given to consider the proposal, members objected that the "a" purpose" standard would open the door for virtually unlimited use of FISA in criminal investigations, where foreign intelligence is only remotely connected.

326. See WEISZ, supra note 1, at 242 ("The two men must have been responsible for putting a stop to the hijackers and al-Qaeda — and each other (approximately) from the start, the response of American intelligence to the challenge presented by al-Qaeda was hampered by the disarray personal relationships and institutional warfare that these men compiled.").

327. Id. at 281 (citing the IC3's inability to share information on the hijackers' cell phone calls with the FBI, CIA, and White House counter-terrorism office).

328. See 50 U.S.C. § 1802(a) (pertaining to "intelligence agents of the Government.")

329. See 50 U.S.C. § 1802(a) (pertaining to "intelligence agents of the Government.").

330. See 50 U.S.C. § 1802(a) (pertaining to "intelligence agents of the Government.").

331. See WEISZ, supra note 1, at 242 ("The two men must have been responsible for putting a stop to the hijackers and al-Qaeda — and each other (approximately) from the start, the response of American intelligence to the challenge presented by al-Qaeda was hampered by the disarray personal relationships and institutional warfare that these men compiled.").

332. Id. at 281 (citing the IC3's inability to share information on the hijackers' cell phone calls with the FBI, CIA, and White House counter-terrorism office).

333. See 50 U.S.C. § 1802(a) (pertaining to "intelligence agents of the Government.")

334. See 50 U.S.C. § 1802(a) (pertaining to "intelligence agents of the Government.").

335. See 50 U.S.C. § 1802(a) (pertaining to "intelligence agents of the Government.").

336. See WEISZ, supra note 1, at 242 ("The two men must have been responsible for putting a stop to the hijackers and al-Qaeda — and each other (approximately) from the start, the response of American intelligence to the challenge presented by al-Qaeda was hampered by the disarray personal relationships and institutional warfare that these men compiled.").
THE DEATH OF FISA

though the administration stated that it would provide a legal analysis in support of the proposed change, at a Senate Judiciary Committee hearing, Senator Diane Feinstein urged Attorney General Ashcroft to consider an alternative formulation of the purpose requirement, to "substantial or significant purpose" rather than to "a purpose." The Attorney General agreed to support a slight change in the proposal, and the eventual Patriot Act amended FISA to provide that obtaining foreign intelligence must be "a significant purpose" of the surveillance.

During the floor debate Senate Judiciary Committee Chairman Patrick Leahy acknowledged that "protection against these foreign-based threats by any lawful means is within the scope of the definition of 'foreign intelligence information,' and the use of FISA to gather evidence for the enforcement of these laws was contemplated in the enactment of FISA." Senator Diane Feinstein also opined that the objective of the change in the purpose language in the Patriot Act was to make it easier to collect foreign intelligence information.

[...]

rather than forcing law enforcement to decide which purpose is primary, this bill strikes a new balance. It will now require that a "significant purpose" of the investigation must be foreign intelligence gathering in pursuit of surveillance under FISA.

The effect of this provision will be to make it easier for law enforcement to...[use FISA]...where the subject of the surveillance is both a potential source of valuable intelligence and the potential target of a criminal investigation.

These comments were embraced later by the Foreign Intelligence Surveillance Court of Review (FISC) as supporting its interpretation of the change in the purpose language as it...


MINNESOTA LAW REVIEW

practically eliminate any requirement that the government show a foreign intelligence purpose in its FISA applications.

However, the Leahy and Feinstein statements do not fairly reflect an intention, on their part or on the part of Congress as a whole, to change the overarching requirement of FISA that its processes be employed in pursuit of foreign intelligence. Senator Leahy simply acknowledged that it had been understood from the beginning of FISA that information collected under it could be used in prosecution, and Senator Feinstein noted that the statutory amendment will make it "easier" to use FISA in criminal cases, not that the foreign intelligence core of FISA was eliminated.

The limited attention to this issue during floor debates and the lack of committee reports is unfortunate. In the determination to enact the new measures quickly after September 11, the details and complexities of FISA and careful consideration of the effects of its amendments were mostly lost on the reformers. From the beginnings of FISA in 1976, however, national security crimes provided a fuzzy point between foreign intelligence collection and law enforcement. The wall between the two types of surveillance thus had an open portal of sorts early on, and the Patriot Act change in the purpose language eased its use. In other words, the adjective "significant" has significant meaning in the amended FISA. There was movement of the standard, but not to such an extent that "a purpose" to collect foreign intelligence would suffice.

As part of a bundle of what some viewed as significant and controversial changes to existing legislation that the Bush administration effectively rushed through Congress, Congress enacted the purpose amendment and several others subject to a five-year sunset provision. After enactment of the Patriot Act, the FISC responded to the first FISA applications filed under the revised Act by incorporating the augmented case-by-case 1995 "OIPR procedures as formal minimization procedures that would apply to all future applications to the FISC." Undaunted by the FISC's order, the Justice Department immediately changed its guidelines to suspend the "chaperone" re-
requirement that OIPR be present during any contacts between Criminal Division and FBI investigators concerning FISA matters.\footnote{In re All Motions Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d at 619.} Instead, OIPR and the FISC would thereafter receive briefings about such meetings.\footnote{In re Sealed Case: 310 F.3d at 723.} More concrete changes came in March 2002, when new Intelligence Sharing Procedures were approved by Attorney General Ashcroft.\footnote{In re All Motions Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d at 619.} The new guidelines removed the information screening procedures and lifted the restriction that had been formally in place since 1995 on prosecutors or other law enforcement officials "directing or controlling" the use of FISA surveillance.\footnote{In re Sealed Case: 310 F.3d at 733-34.} In addition, the new procedures encouraged complete sharing of information and advice and emphasized that "[t]he overriding need to protect the national security from foreign threats compels a full and free exchange of information and ideas."\footnote{Memorandum from John Ashcroft, Attorney Gen. of the United States, Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI to Dir. of the FBI, Assistant Attorney Gen. for the Criminal Div., Counsel for Intelligence Policy, and United States Attorneys (Mar. 6, 2002), available at http://www.fbi.gov/spo/agency/ashcroftiisp0203.html (hereinafter March 2002 procedures).} Prosecutors are expected to have access to all information developed by the FBI in field intelligence investigations undertaken pursuant to FISA and prosecutors may advise the FBI about "all issues."\footnote{Id.} Although the Criminal Division, FBI, and OIPR are expected to meet and consult, OIPR is not required to be present when the other two meet.\footnote{See id.}

The new guidelines effectively dismantled the system that OIPR had in place since 1995. Although the 1995 procedures had erected information barriers that were not required by FISA, they assumed that FISA was being used for its intended purpose and protected against newly emerging criminal cases with evidence obtained for the purpose of collecting foreign intelligence. The Ashcroft guidelines are, like their 1995 predecessor, for the most part not required by FISA, as amended by the Patriot Act.\footnote{Id. at 624.} The new information sharing provision in the Patriot Act did provide a statutory basis to remove barriers that had existed because of the previous procedures, including elimination of the OIPR as chaperone.\footnote{See supra Part III, notes 204-28 and accompanying text.} Although the legislative history surrounding the Patriot Act amendment to the purpose language does not clearly illuminate its purpose, the apparent aim was to facilitate information sharing between intelligence and law enforcement personnel after information is collected and, to a lesser extent, eliminate the incorrect but widespread belief that the use of FISA processes could undermine a subsequent or even contemporaneous prosecution.\footnote{In re All Motions Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d at 619.}

The change in the purpose language was really a change in emphasis only; it did not provide the basis for the elimination of the "direction or control" restriction on the Criminal Division. That single change in the procedures could be read to open up just the sort of misuse of FISA that was feared by the en banc FISC in its 2002 opinion.\footnote{In re Sealed Case: 310 F.3d at 723-24.} Prosecutors that did not have grounds for a Title III warrant could urge intelligence investigators to expand their FISA surveillance parameters in pursuit of a criminal charge.\footnote{In re All Motions Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d at 619-20.} With such surveillance in place, FISA orders permit longer periods of surveillance, easier renewals, and less oversight than Title III.\footnote{See supra Part III, notes 204-28 and accompanying text.} The "direction or control" change was not required by the Patriot Act, and it apparently reflected the Attorney General's determination to move vigorously forward with the policy of prevention. After the Attorney General approved the March 2002 procedures, the Department of Justice submitted a new application for FISA surveillance and, as part of the application, moved that the FISC vacate its minimization and wall procedures to the extent they are inconsistent with the new OIPR procedures.\footnote{Cf. supra Part III, notes 204-28 and accompanying text.} In May 2002, the FISC issued a decision, joined by all seven judges of the court, that agreed with the request.
for the most part, but that rejected a portion of the new Justice Department guidelines and ordered new procedures to ensure the integrity of the underlying foreign intelligence purpose of FISA investigations.\textsuperscript{204} The FISC opined that the new Justice Department procedures "appear to be designed to amend the law and subvert the FISA for [criminal law enforcement] electronic surveillances."\textsuperscript{205} As the FISC interpreted FISA, the Justice Department procedures would gut the minimization requirements—designed to minimize the gathering of information about United States persons and to prevent its dissemination—if the Criminal Division could so easily use FISA-obtained electronic surveillance, and the Patriot Act did not affect those minimization requirements.\textsuperscript{206} Instead of using minimization to determine the "need of the United States to obtain, produce, and disseminate foreign intelligence information,"\textsuperscript{207} the new OIPR procedures would have the FISC balance the use of FISA materials against the government's need to obtain and use evidence for criminal prosecution.\textsuperscript{208}

According to the FISC, the limits it set on the OIPR procedures seek to avoid FISA activities where "criminal prosecutors direct both the intelligence and criminal investigations . . . [and] coordination becomes subordination of both investigations or interests to law enforcement objectives."\textsuperscript{209} The Court summed up the implications of the new procedures:

"Criminal prosecutors will tell the FBI when to use FISA (perhaps when they lack probable cause for a Title III electronic surveillance). What techniques to use, what information to look for, what information to keep as evidence and when use of FISA can cause because there is enough evidence to arrest and prosecute.\textsuperscript{210}

The court feared that under the proposed procedures, prosecutors would have "every legal advantage conceived by Congress to be used by U.S. intelligence agencies to collect foreign intelligence information," including the lower probable cause standard and "use of the most highly advanced and highly intrusive techniques for intelligence gathering."\textsuperscript{211} The

\textsuperscript{204} Id. at 926–27.

\textsuperscript{205} Id. at 925.

\textsuperscript{206} Id. at 925–26.

\textsuperscript{207} Id. at 926.

\textsuperscript{208} Id. at 926 (emphasis omitted).

\textsuperscript{209} Id. at 926–27 (emphasis omitted).

\textsuperscript{210} Id. at 926–27 (emphasis omitted).

\textsuperscript{211} Id. at 926–27 (emphasis omitted).

\textsuperscript{212} Id. at 925 (emphasis omitted).

\textsuperscript{213} Id. at 926–27 (emphasis omitted).

\textsuperscript{214} Id. at 925 (emphasis omitted).

\textsuperscript{215} In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 219 F. Supp. 2d at 624.

\textsuperscript{216} Id. at 623–24 (emphasis omitted).

\textsuperscript{217} Id. at 624.

\textsuperscript{218} Id.

\textsuperscript{219} Id. at 625.

\textsuperscript{220} Id. at 625 (emphasis omitted) (internal quotation marks omitted).

\textsuperscript{221} In re Sealed Case, 310 F.3d 717, 720–724 (FISA Ct. Rev. 2002).

\textsuperscript{222} Id. at 721.

\textsuperscript{223} Id. at 725, 725–726.

\textsuperscript{224} Id. at 726–727.

\textsuperscript{225} Id. at 726–727.

\textsuperscript{226} Id. at 726–727.

\textsuperscript{227} Id. at 726–727.

\textsuperscript{228} Id. at 726–727.
date the FISA activities. If the gathering of foreign intelligence is a significant purpose of the surveillance, the later use of FISA-derived information in a criminal prosecution will not taint the evidence.278 In short, the FISCRC conflated what FISA information is used for with the purpose for using FISA.279

During the 1980s and early 1990s, some of the criminal convictions and appeals where FISA-derived evidence formed part of the basis for the prosecution upheld the use of the FISA evidence after finding that the surveillance was not "directed towards criminal investigation or the institution of a criminal prosecution."280 Indeed, a court of appeal that reviewed FISA-related criminal convictions during this period, only the Sarabian court "refus[ed] to draw too fine a distinction" between criminal and intelligence investigations.281 The others endorsed the "primary purpose" test and, in doing so, presumed that a "wall" between the law enforcement and intelligence sides of an investigation existed.282 However, none of these courts suppressed evidence and none contradict that in OIPR and the Justice Department during that period a robust coordination between intelligence and law enforcement officials was ongoing.283 In short, the purpose requirement existed from the beginning, but the wall, misapprehended by the FISCRC, came later.

After the sudden death of OIPR head Mary Lawton in 1993, Attorney General Janet Reno turned to her Florida colleague and Assistant U.S. Attorney in Miami, Richard Scruggs, to head OIPR.284 Scruggs became concerned that there were no written guidelines governing contacts between the Criminal

278. See supra note 209 (criticizing decisions upholding the use of FISA procedures and FISA-derived evidence in criminal prosecutions).
279. See H.R. REP. NO. 95-1283, at 69 (1978) ("How this information may be used to protect against clandestine intelligence activities is not prescribed by the definition of foreign intelligence information. . . . Obviously, use of [foreign intelligence] as evidence in a criminal trial is one way the government can lawfully protect against . . . international terrorism.").
281. United States v. Sarabian, 851 F.2d 910, 916 (9th Cir. 1988).
282. See United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991); United States v. Pollock, 835 F.2d 1097, 1075-76 (6th Cir. 1987); Duggan, 746 F.2d at 77.
284. See DOJ Memo, 8 DOJ ALERT 11 (May 2, 1994).
289. See Banks, supra note 16, at 1176 n.81.
must be sought. The FISC decision considerably weakened the foreign intelligence core of FISA.

When the FISC convened in 2002, it was undeniable that national security investigations often have multiple purposes. Moreover, because Congress has made many terrorist activities crimes, there is more than ever an overlap between foreign intelligence and law enforcement, even within the same investigation and targets. Criminal prosecution supported by effective intelligence investigations can be an effective counterterrorism tactic. Still, as interpreted by the Court of Review, FISA can permit the government to skirt the statutory and constitutional protections afforded those subject to law enforcement investigations. FISA was created as a system for surveillance for foreign intelligence, not for solving crimes. Outside that exceptional area of foreign intelligence, the Constitution before and after 1978 requires Fourth Amendment notice to targets. Sixth Amendment confrontation of evidence, and First Amendment freedom of expression without a chill from the specter of looming FBI surveillance.

So understood, the wall is an essential part of the larger context for managing and implementing FISA, whether or not the pre- or post-Patriot Act language literally requires such separation. If something like the wall procedures are not in place, FISC-approved surveillance may violate the Constitution when the FBI begins an investigation principally to build a criminal case.

---

212. See Banks, supra note 10, at 1177-81.
213. See Banks & Severe, supra note 1, at 9.
216. See id. at 1320-41 (discussing how the full protection of the American criminal justice system apply to targets of warrantless in ordinary law enforcement actions).
218. See id. at 134 (“The Bureau has a history of redefining criminal investigations as intelligence operations in order to use FISA warrants and NSA intercepts to obtain information for use in drug or other ordinary crime investigations.”).
219. See Swep, supra note 236, at 1361.
220. See infra notes 200-05 and accompanying text.
221. See Boston, supra note 24, at 17.
222. See id. in re All Matters Submitted to the Foreign Intelligence Surveillance Ct., No. 1296, 2016 U.S. Dist. LEXIS 180 (FISA Ct. Rev. 2016).
223. See id. at 25
224. See supra notes 200-05 and accompanying text.
225. See Stenger, supra note 24, at 17.
226. See id.
2007] THE DEATH OF FISA 1355

FISC, why would the administration not rely on a sure thing? How could the President have stated in 2004 that "any time you hear the United States government talking about wiretap, it requires . . . a court order. Nothing has changed. When we're talking about chasing down terrorists, we're talking about getting a court order before we do so."?

When critics pointed out the obvious—that secret electronic surveillance for foreign intelligence inside the United States is provided for by FISA—the administration defended the decision not to rely on the FISA process. Given the expansive nature of the definition of "electronic surveillance" in FISA, the "exclusivity" provisions of FISA and the companion criminal enforcement statute, and the criminal penalties for unauthorized electronic surveillance, the administration faced an uphill legal climb. FISA provides criminal penalties for anyone who engages in electronic surveillance "not authorized by statute." The administration has argued that the Authorization for the Use of Military Force (AUMF) constitutes the necessary authorization within the meaning of the FISA "authorized by statute" provision. The text and legislative history clearly reveal, however, that the purpose of the FISA provision is to provide security to intelligence personnel who act in accordance with FISA, not to immunize them if they violate the law. The "statute" referred to in section 1869 is FISA, or Title III. Similarly, the administration's claims of AUMF authority would make the exclusivity provision in FISA meaningless.

Attorney General Gonzales emphasized the need for "speed and agility" in making judgments about particular intercepts.

311. Id.
313. See generally NSA III: War Time Executive Power and the FISA Court Hearing Before the S. Commm. on the Judiciary, 106th Cong. 812 (2000) [herein-
315. Id.
316. Alberto R. Gonzalez, Adeclaration Remarks for Attorney General
318. Id.
321. Id.
322. Unconstitutional Territory, The Administration's New NSA Defense in Fact
respond to terrorist threats. Baker testified that the Justice Department would not support Senator DeWine’s proposal—because the probable cause standard was likely not an obstacle to effective use of FISA, and because the Department worried that the reasonable suspicion standard might be unconstitutional. The executive branch thus expressed concern that a lowered standard might be unconstitutional at the same time they were engaged in just that practice. Admittedly, the DeWine proposal would have loosened the predicate only for non-Unites States persons. The TSP does not distinguish United States persons from others, and it foregoes the PISC oversight that the lower standard would continue to provide.

Attorney General Gonzales also asserted that seeking legislative authority for the TSP would have tipped off the enemies and let them know what surveillance activities we were pursuing. Although Gonzales stated that the administration had been “advised that [it] would be difficult, if not impossible,” to obtain such an amendment to FISA, he apparently referred not to the political or legal difficulties such a proposal would face, but to the concern that such an amendment could not be obtained “without jeopardizing the existence of the program.” For example, once the administration admitted the program’s existence and cautioned that the program only intercepted international calls, in theory those who subject to the surveillance could evade the program through countermeasures, such as use of VoIP (Voice over Internet Protocol) phones with U.S. numbers but used abroad.

Putting to one side the possibility of legislation being considered in executive session, with classified information secured and sources and methods protected pursuant to House and Senate rules, and despite some briefings on the TSP to se-

320. Id. at 23 (statement of James A. Baker, Counsel for Intelligence Policy, Day of Details).
321. Id.
323. Id.
324. Id.
325. [Once telephone technology permits the user to mark his location because the telephone number that is dialed or transmitted can be used to identify location or wherever the call is placed, the National Security Agency is considering adding a Frequently Asked Questions. http://www.fas.org/vlc/oj/last updated Apr. 13, 2007].

327. Id. § 4136(d).
330. Id. § 4136(a).
331. See Press Briefing, Gonzales & Hayden, supra note 322.
332. Daniel Nadlerman et al., Public Statement: They Were Loyal Conversations.
2007] THE DEATH OF FISA 1259

fused to sign off on the program, a White House delegation, in-
ccluding then White House Counsel Gonzales, visited Achenroft in
the hospital to appeal Comey’s decision, with apparent suc-
cess.292 Vetted or not, administration admissions that wholly
domestic calls might have been monitored in the larger sweep
for terrorist activities contradict the claim that the only calls to
or from persons and locations overseas are monitored.293

Those who characterize the TSP as a complex and technolo-
gically advanced data mining program that simply cannot be
fitted inside the opaque structure of FISA take a different path.294
Apart from the Attorney General and the President fail-
ing back on the need for “speed and agility,” and stating that
the war we are fighting is “a different war,” many advocates of
the TSP say, quite simply, that the law has failed to keep up
with the technology.295 However, according to General Hayden,
who was head of NSA when the program was implemented,
TSP “is not a dragnet over Dearborn or Lackawanna or Free-
moor, grabbing conversations that we then sort out by these al-
leged keyword searches or data-mining tools. . . . This is tar-
geted and focused.”296 Hayden claimed the surveillance was
limited to “international calls and only those we have a reason-
able basis to believe involve al Qaeda or one of its affiliates.”297
Hayden was blant: “we’re not sucking up every call and then
using some of these magically alleged keyword searches—Did
he say that?”298 Instead, a shift supervisor at NSA substitutes
for a federal judge.299 She decides what part of the product
of the data-mining merits further targeted surveillance, and the

and Bush Administration. They fought a quixotic battle to
bring to the President’s
Power in the War on Terror. And They Paid a Price for It. A
Newsweek Investiga-
tion. NEWSPORT, Feb. 6, 2006, at 34, 39.
318. Id.
319. See Stewart M. Powell, White House Acknowledges Some Ties Wholly
320. Press Briefing Gonzales & Hayden, supra note 322.
322. General M. Powell, Principal Deputy Dir. Of Nat’l Intelligence: Ad-
.org/maps/20060123/Mayday/12306.html.
323. Id.
324. Id.
325. Id.
326. Id.

standard she employs in making these decisions is reasonable
suspicion instead of probable cause.340

The legality of the TSP was thus defended by the Adminis-
tration at the same time that it was admitted, in effect, that the
program does not comply with FISA. Nor did the Administra-
tion fulfill congressional reporting requirements for intelligence
collection activities. Whether officials substituted a “reasonable
suspicion” standard or some other criterion in deciding who to
target with TSP, the substitution of an NSA employee for a
federal judge as the gatekeeper is a startling departure from
the regularized procedures of FISA.

C. SYNTHESIZING THE POST-SEPTEMBER 11 DEVELOPMENTS:
THE DEATH OF FISA

The inter-branch compromise that produced FISA con-
tains a series of interlocking elements. FISA required a form of prior
judicial approval to intercept electronic communications inside
the United States, except in emergencies.329 The intercession
had to be targeted at particular persons or places related to
suspected terrorism or espionage.330 The predicate for issuing a
court order was a showing of probable cause of foreign agency
and that foreign intelligence will be acquired,331 and Congress
determined in 1978 that these parameters were the exclusive
means for covering our electronic surveillance for foreign intel-
ligence inside the United States.332 A fully informed Congress
was to oversee all of the above.333

Part B showed that amendments to the Act, judicial deci-
sions, or executive practice have already undercut some of
these elements of FISA. Others remained arguably intact until
the TSP emerged, and Congress prepared to bargain away the
important remaining pieces of FISA. The two sea-change devel-
lopments explored here—dismantling of the foreign intelligence
‘purpose’ screening requirements and the NSA Terrorist Sur-
veillance Program—should not be understood as the only
causes of the death of FISA. Larger institutional and societal
2007] THE DEATH OF FISA 1261

atmospheres, particularly in the last five years, place the demise of FISA in context.

An overriding aura of emergency has driven the post-
September 11 counter-terrorism programs, including the Patriot Act,\textsuperscript{347} the FISC decision,\textsuperscript{348} and the NSA program.\textsuperscript{349} The Bush administration effectively has sustained the emergency through its global war on terrorism and the war in Iraq, and Congress and the courts have altered their perspectives in light of it.\textsuperscript{350} One result is that the central lessons of the Keith case has been lost—that the societal interests in security and civil liberties must be balanced, with the participation of the federal courts.\textsuperscript{351} In a 2006 insider's account by Professor John
Yoo of his experiences inside the Justice Department in helping to shape the post-September 11 programs, Yoo maintained that FISA . . . was created specifically to hamstring the executive branch in favor of civil liberties.\textsuperscript{352} Professor Yoo's revisionist history is emblematic of the change in orientation of government after September 11, a change also expressed in the opinion of the FISA Court of Review. In rejecting the opinion signed by all of the FISC judges, the Court of Review essentially took the core out of FISA when it opined that the Justice Department would have free rein in deciding when to use the FISA procedures.\textsuperscript{353}

During the same period, Congress effectively ceded its role in leadership.\textsuperscript{354}The executive branch devised the policies it wished to follow after September 11, and it set in place the programs and enforcement activities to meet the policy objectives.

349. See Barton, supra note 300, at 47.
350. See Baren & Laitbrook, supra note 23, at A16 (discussing how the NSA program reflects a major shift in American intelligence gathering practices).
351. See id. at A1 (discussing the difficulty of identifying a line between national security interests and the rights of Americans against unjust search).
352. Yoo, supra note 305, at 72.
354. See Norman J. Ornstein & Thomas E. Mann, When Congress Checks Out: Foreign Policy, How Democracy Works (2004), at 87, 98 (the "recess contains congressional oversight of the executive . . . on foreign and national security policy . . . has virtually collapsed.").
2007] THE DEATH OF FISA

1263

When field agents sought the headquarters' approval for a FISA surveillance order, they were turned down, because there was insufficient information connecting Moussaoui to a foreign power.

However, the headquarters' agents only orally briefed the lawyers responsible for making the foreign agency recommendation. If the agents had searched FBI computer records relevant to the Moussaoui request, they would have had access to a July 2001 memorandum from a Phoenix agent that warned about the potential dangers of al Qaeda affiliates seeking training at U.S. flight schools. FBI personnel did not follow up on the memorandum, and no senior officials at the Bureau saw the memorandum before September 11.

In addition, the headquarters' staff lawyers apparently mistakenly advised the Minneapolis agents that foreign agency required a link to a terrorist organization on the State Department list of terrorist organizations.

At about the same time, the FBI received a classified cable from a French intelligence agency that warned the Moussaoui had "Islamic extremist beliefs." If the French intelligence had been coupled with the Phoenix memorandum, the fact-sensitive foreign agency inquiry might have produced a different outcome. But the two sources together would have only suggested that Moussaoui was affiliated with al Qaeda and thus had a connection to a foreign power.

The Minnesota agents did not open a criminal investigation that would have permitted a search of Moussaoui's laptop because FBI headquarters believed that the agents lacked sufficient probable cause of a crime.

A criminal case was opened and a FISA order was obtained, but only after the September 11 attacks.

359 Joint Inquiry Staff Memorandum, supra note 357, at 17.
360 See Shelby, supra note 15, at 20.
361 Id. at 23–26.
362 Id. at 53.
363 David Johnston & Philip Shenon, F.B.I. Cited Source of Moussaoui's Radio TXS to Attack, N.Y. TIMES, Oct. 6, 2001, at A1. Professor Yoo slightly alters the reported facts regarding Moussaoui and writes that Moussaoui "had connections to extremist Islamic groups." Yoo, supra note 355, at 80. It was precisely the lack of demonstrated ties to any foreign power that caused headquarters to decline to pursue a FISA application.


365 9/11 Commission Report, supra note 167, at 273. On September 12, the British government received and passed on to the United States intelligence that Moussaoui had attended an al Qaeda training camp in Afghanistan. Id. Obviously, if that information had been available in August, the predicate for FISA surveillance would have existed. Id. at 275.

366 Id. at 275.
367 Id. (stating that the connection between Moussaoui and al Qaeda was "just an easy trail to follow").
369 Yoo, supra note 355, at 82.
370 Id.
371 Id. at 80–81.
373 Id. at 439 (listing the witnesses who testified in front of the Commission).
THE DEATH OF FISA

2007

The death of FISA inevitably involved a great deal of work. The Senate Intelligence Committee, led by John Kerry (D-Mass.), held hearings on the topic. The committee's report was critical of FISA, calling for changes to the law.

FISA was enacted in 2001 as a response to the terrorist attacks of September 11, 2001. It was designed to provide legal authority for the government to conduct surveillance of Americans suspected of terrorist activity. However, the law has been controversial, with some critics arguing that it has been too easy for the government to obtain warrants to conduct surveillance.

The Senate Intelligence Committee report recommended changes to FISA, including requiring the government to provide more information to the court when applying for a warrant, and restricting the government's ability to collect data on associates of a target, such as their phone numbers.

The committee also recommended that FISA be reauthorized for another five years, with some changes to the law. However, it remains to be seen whether Congress will enact these changes.

---

669
2007] THE DEATH OF FISA 1267

purpose" language or to clarifying the reason for the "purpose" language. Instead, after compromises were made to revise the authorities for National Security Letters and business records,385 the sunset on the significant purpose provision and twelve of fourteen other Patriot Act authorities subject to sunset were simply repealed.386

The reauthorization and lifting of the sunset on "significant purpose" only underscores that the Patriot Act change was not legally necessary or sufficient to eliminate the wall. The amendment was not necessary because the obstacles to sharing information or integrating data are not the product of legal rules.387 A change would not have been sufficient to overcome the Fourth Amendment requirement that relaxed approval processes for electronic surveillance be reserved for when the purpose is collection of foreign intelligence.388 However, the Supreme

384. CONGRESSIONAL REPT., supra note 307, at 329 n.81 (stating that there was "no legal reason" why information could not be shared).

385. CONGRESSIONAL REPT., supra note 307, at 329 n.81 (stating that the sunset authority would not be included).

386. CONGRESSIONAL REPT., supra note 307, at 329 n.81 (stating that there was "no legal reason" why information could not be shared).

387. CONGRESSIONAL REPT., supra note 307, at 329 n.81 (stating that the sunset authority would not be included).

388. CONGRESSIONAL REPT., supra note 307, at 329 n.81 (stating that the sunset authority would not be included).


391. MINNESOTA LAW REVIEW [91:1209

2007

THE DEATH OF FISA 1260

To argue, as some did in the Patriot Act reauthorization debates, that the modern blending of crimes and foreign intelligence threats should be reason enough to eliminate the wall provisions.407 However, this fails to take into account that the purpose requirement focuses on the investigators’ reason for seeking a FISA order, not on what is done with the product of the surveillance.408 If the purpose of the investigation is to prosecute, FISA should be unavailable, given its requirements and protections of the Fourth, Sixth, and First Amendments.409 If the purpose is to monitor conversations toward understanding a terrorist threat, FISA may be used if its requirements are otherwise met. If both objectives are present, reasonable officials should weigh which purpose is dominant and use the appropriate path toward authorized surveillance. The 2001 amendment and its 2006 codification did not tear down the wall; nor did the 1978 purpose language build it. Nor could these phrases in FISA knock down a set of protections that the Constitution requires.

Within a few months of the FISCR decision,410 the Justice Department reported to the House Judiciary Committee that the procedures approved by the FISCR greatly improved the way that investigations are conducted, in terms of efficiency, order, and effectiveness.411 Approximately 4500 open intelligence files were shared with criminal prosecutors during that several-month period.412 In 2003, the FBI issued a directive, the Model Counterterrorism Investigations Strategy (MCIS), which requires law enforcement and intelligence investigators to work together as part of the same teams investigating terrorists.413

407. Kate Martin & Viet Dinh, Section 302: Authority to Share Criminal Investigative Information under PATRIOT (DEBATE: EXPERTS DEBATE THE USA PATRIOT ACT 12 (Stuart A. Baker & John W. Carlin eds., 2005) (“Even the most ardent opponents of the USA PATRIOT ACT would not want another terrorist attack to occur because law enforcement and intelligence communities were prevented from talking to each other.”). This rhetoric obscures the fact that FISA did not prevent such sharing of information. In re Sealed Case, 310 F.3d 717, 727 (FISA Ct. Rev. 2002).

408. See Banks, supra note 16, at 1156 (discussing the focus of the primary purpose provision).

409. See Banks, supra note 296, at 1361.

410. In re Sealed Case, 310 F.3d 717.


412. Id. at 16.


417. MINNESOTA LAW REVIEW [91:1209]

All terrorism investigations are "banded from the outset like an intelligence or espionage investigation," run out of the counter-terrorism division at the FBI, and investigators from the blended teams may use FISA processes.414 One aim of the new system is to deemphasize criminal prosecution in favor of longer term surveillance, although prosecutors that bring criminal charges will be able to use FISA surveillance at trial.415

In September 2005 testimony before the Senate Judiciary Committee, a senior FBI official stated that the Patriot Act, the Ashcroft information sharing procedures, and the FISCR decision "removed real and perceived barriers to coordination" among the FBI and other intelligence agencies.416 In a September 2006 release the Justice Department reported an increase of more than 122 percent in court-approved FISA applications between 2001 and 2005, with anticipated 10 percent growth for 2006.417 In addition, since 2004 the Department had reduced the backlog of pending FISA requests by about 60 percent, and reduced the number of days it takes to process FISA requests by 35 percent.418 The size of the lawyer staff at OFPR was tripled during the same period, and standardized pleadings and automated drafting have made FISA filings shorter and easier to produce.419

Former NSA General Counsel Stewart Baker maintained that the wall was born out of fear.420 Baker believed that agency professionals "were focused on the hypothetical risk to privacy if foreign intelligence and domestic law enforcement were allowed to mix" and on the chance "that years of successful collaboration would end in disaster if the result of a single collaboration could be painted as a privacy scandal."421 Whatever the motivation, Baker is surely correct that the wall was deeply embedded in the FISA culture when these decisions were made.

414. Id.

415. Id.


417. DEPT. JUST. FACT SHEET, supra note 6.

418. Id.

419. Id.


421. Id.
THE DEATH OF FISA 1271

were rendered in 2002.425 The FISC did not see the risk identified by Baker as hypothetical, and it had long experience in managing the FISA process.426 The FISC reflected on Baker, but it had never seen a FISA application before.427 If the FISC's decision is forming the basis for implementing FISA now, the FBI is not prepared to perform any of the primary functions of the FBI process for the primary purpose of investigating a crime even though there is no probable cause to suspect the commission of a crime.

2. Statutory Obsolescence and Lone Wolf

One by-product of the compromising that was necessary to produce FISA was a set of definitions and procedures that were difficult to understand and apply, even in the beginning.428 As sometimes happens with major legislation that is complicated at the outset, amendments are made and, over time, what was simple becomes hopelessly complex.

In addition, the investigative resources directed at countering terrorism have grown considerably, and their orientation has shifted. In the years since FISA was implemented, Congress has, often at the behest of the executive branch, criminalized more and more national security and terrorism-related conduct, adding hundreds of new offenses to the federal criminal code.429 As a result, in the universe of foreign intelligence surveillance, a law enforcement purpose for the surveillance inevitably occupies a larger portion of the whole than it once did. The challenges in sorting out what should be FISA surveillance and what should follow the law enforcement model are greater now than they were in 1978.

As terrorism overtook espionage as the dominant foreign intelligence collection challenge, the foreign power and agent of a foreign power concept did not align easily with targeting objectives.430 The growing criminalization of terrorism made the

427. See id. at 1173–74.
428. See Banks, supra note 16, at 1161–62 (describing early difficulties of restricting procedures, while, supra note 296, at 1150 (calling FISA a ‘great compromise’)).
430. See Banks, supra note 397, at 1298 (noting that FISA was created for gathering intelligence about foreign powers inside the United States).

1272 MINNESOTA LAW REVIEW [91:1209

minimization rubric for what was collected pursuant to FISA harder to sustain, while the growing need for cooperation and information sharing was not contemplated when FISA was enacted in 1978. Congress never took the initiative, nor did the executive branch, to step back and rewrite FISA from top to bottom. As a result, the issues that have plagued FISA have lingered, and new ones crop up. Amendments have been made piecemeal.

When Congress amended FISA in 2004 to provide authority to conduct FISA-ordered investigations of so-called “lone wolf” terrorist suspects,431 it was billed by many as “the Moutassem Act”—referring to the failure to find that Moutassem was an agent of a foreign power as defined by FISA because he had no apparent links to terrorist organizations.432 As amended, the “agent of a foreign power” may include any person, other than a United States person, who “engages in international terrorism or activities in preparation therefore.”433 In expanding FISA to reach these unaffiliated persons, or those for whom the foreign agency connection cannot be established by probable cause, Congress did not attempt to rework its 1978 formula for identifying targets, an approach that was derived from traditional concerns with espionage and counterintelligence.434 Logically, the foreign agency concept could not bear the weight of the lone wolf amendment in 2004. If an individual may be targeted for FISA surveillance without any showing of a connection to any other supposed terrorists, the idea of “agency” simply does not fit. Congress can call an unaffiliated person an agent, but the Act does not require any agency relationship.

Yet the lone wolf amendment is arguably among the most defensible changes to FISA since 1978. On the one hand, recent terrorist trends suggest that the lone wolf is the terrorist of our time, symbolized by the universal violent jihad rhetoric.435 In
THE DEATH OF FISA

individual terrorists are not a new phenomenon, and examples of the lone wolf trace back at least as far as European anarchism in the late nineteenth century. As Bob Chesney has explained, internet and encryption technologies have joined with the growing violent jihad movement and the partial success of efforts to curtail violent jihad organizations to facilitate the growth of unaffiliated terrorists and their causes. Conducting surveillance only of those who are foreign agents may miss some of the most important targets.

On the other hand, the extension of FISA processes to unaffiliated individuals does not solve the problem of coming up with sufficient information to meet the FISA probable cause requirement. Put differently, investigators still have to know something about the lone wolf target before they may begin FISA surveillance, and learning that modicum of information is made no easier by the lone wolf amendment.

At first blush, the lone wolf provision may appear to permit intrusive electronic surveillance pursuant to FISA of an especially broad array of individuals—from those who are suspected of buying or selling component materials for weapons of mass destruction to those who make donations to apparently humanitarian organizations in the Middle East. However, the lone wolf provision does not apply to U.S. persons and it requires pursuit of "foreign intelligence" and a connection to "international terrorism," offering protection against targeting domestic activity. Yet in the post-September 11 era, where supposed links to al Qaeda are legion, the tendency to rely on FISA to investigate even the most speculative suspicions of a connection to international terrorism by lone wolves could turn FISA surveillance into a quotidian occurrence.

Moreover, there may be a tendency to couple the discretion to conduct electronic surveillance of lone wolves with early arrest and prosecution. If an, cessation of surveillance may impose opportunity costs and a higher likelihood of acquittals than have been the case under the previous foreign agency criteria. With this potential risk in mind, the lone wolf change may be a practical statutory solace to an important policy challenge, while it shows that the original FISA framework for targeting electronic surveillance may not be workable now.

IV. THE FUTURE PROSPECTS

Now that the basic survival of FISA has been called into question, it is important to consider whether FISA can be restored to its useful role in maintaining the security and civil liberties balance. Changes in technology and the dimensions of the modern threat of international terrorism have combined to complicate finding the appropriate mechanisms that may or may not be accommodated inside the FISA scheme. This part of the Article will consider whether technological developments make it impossible for the TSP to be conducted with FISA procedures. Next, the Article will offer some tentative conclusions concerning the lawfulness of the TSP. Then it will evaluate proposed FISA amendments, although in the main they simply relegate FISA to an historic dust bin. Whether the TSP could be reshaped harmoniously with a still-relevant FISA is a hard question, one that I will address briefly in the final two subsections.

A. FISA AND MODERN TECHNOLOGY

When deliberating FISA in 1977, Congress was well aware that "NSA had engaged in its share of the abuses chronicled by the Church Committee and others." From 1945 until 1975, NSA received copies of millions of international telegram sent

[Links to sources and citations are not fully translated into natural text.]

© [2007] MINNESOTA LAW REVIEW
to, through, or from the United States.442 NSA intended Operation SHAMROCK to obtain telegrams of foreign targets for foreign intelligence purposes.443 With the assistance of commercial telegraph companies and without obtaining any kind of judicial warrant, NSA had access to as many as 150,000 telegrams per month, including those of U.S. citizens who were not in any way targeted for foreign intelligence and who reasonably expected their communications to be private.444 When considering FISA, however, Congress expressly declined to extend FISA procedures to NSA surveillance activities at least in part because of then-recent enhancements in oversight of NSA provided by presidential executive orders and through classified Attorney General procedures.445 In addition, Congress took note of the "particularly difficult conceptual and technical problems" in regulating NSA, and it opted to leave NSA untouched until separate legislation could be considered.446

The modern NSA story is in part about the supposed leapfrogging of technology. The story is familiar. The technologies of surveillance and its evasion change rapidly. The bad guys keep up with them, and the government lags behind, always playing catch up.447 "NSA does not "engage in wiretapping"; its electronic surveillance is referred to as "signals intelligence" or SIGINT."448 NSA intercepts "entire streams of electronic communications containing millions of calls and e-mails," and screens them through computers that search for key words or phrases, telephone numbers, or Internet addresses.449 Data that is identified as worthy of further investigation is generated by the computers, and then forwarded to NSA personnel.450 Of course, the immense volume of electronic communication in the world today is such that NSA can only process a small portion of it. Some of what is collected is in foreign languages, and some is encrypted, while technical issues limit the capabilities of NSA computers to find all the desired identified markers.451 Accordingly, NSA must establish priorities for its collection activities.

Is FISA an impediment to the government in the technology race? One part of the NSA program, first reported by the media in May 2006, apparently consists of collecting meta-data, information about communications, but not the contents of those communications.452 NSA collects the phone numbers or e-mail addresses and the time and day of communications between sets of numbers or addresses.453 Computers then sift through the billions of pieces of data and cross reference them with information databases in order to identify persons for further investigation.454

The FISA definition of "electronic surveillance" extends to some non-content information, and thus even the indiscriminate data mining program run by NSA may require a FISA application and order before it is performed, or, on an emergency basis, an application within seventy-two hours of approval) by the Attorney General.455 Attorney General Edward Levi testified in 1975 that FISA should include provisions for the approval of "program[s] of surveillance" for foreign intelligence when there are no "specifically predetermined targets" and where "the efficiency of a warrant requirement would be minimal."456 Of course, Congress enacted FISA without such a provision, and the compromise that became FISA included a considered judgment that only individualized consideration of applications for secret surveillance to collect foreign intelligence would be prescribed.

One additional problem with the TPP is that NSA computers do not know who placed the calls or sent the messages. How do they know the contents of those communications? How 451. See id. at 63 ("The NSA's office at Crypto City also houses the agency's largest collection of powerful computers, advanced mathematicians, and skilled language experts.").

452. Leslie Cockburn, NSA Has Master Key for Americans' Phone Calls, USA Today, May 11, 2006, at 1; John O'Neil, Back Says U.S. Spying Is Not Widespread, N.Y. Times, May 11, 2006, at A2 (describing the program and its descriptions by USA Today).

453. See O'Neil, supra note 452.

454. See Fleischer, supra note 309, at 48.


and based on what criteria does someone demonstrate probable cause or even reasonable suspicion to justify targeted surveillance that triggers FISA? Kim Taipale proposes "the electronic surveillance equivalent of a Terry step"—in this case "an authorized period for follow-up monitoring or investigation of initial suspicion derived from automated monitoring." Taipale's reasonable suspicion standard would form the basis for the judgment either to discontinue or continue the automated monitoring at this early stage. If the monitoring produces probable cause of foreign agency (or lone wolf, statute), a traditional FISA process could be launched by NSA and the Department of Justice. Taipale does not suggest that programmatic measures be used indiscriminately in search of terrorist activities. Instead, officials should direct these techniques "against known or reasonably suspected foreign terrorist communication sources," sources not subject to FISA or a traditional law enforcement warrant, and employ them to "automate the process of looking for connections, relationships, and patterns for further follow-up investigations." Taipale offers examples—Abu Musab Zulfiqar's cell phone number or a known al Qaeda communication network in Pakistan, Saudi Arabia, or Hamburg. In a similar vein, Judge Richard Posner lamented that, while FISA has value for monitoring known terrorists, "it is hopeless as a framework for detecting terrorists." Posner argues that the FISA requirement of probable cause of foreign agency before electronic surveillance may be approved as of no help "when the desperate need is to find out who is a terrorist," yet what kind of rule-based program could permit surveillance in the circumstances of concern to Taipale and Judge Posner that would consist of anything other than the unilateral discretion of executive officials and intelligence professionals who would determine what counts as a suspected foreign terrorist communication source for these purposes, and what criteria would be used to decide whether and how to continue follow-up investigations?

B. IS THE TSP LAWFUL?

At this writing, a few legal conclusions about the TSP may be at least tentatively drawn. First, the NSA has, by the public admissions of administration officials, conducted the foreign intelligence "electronic surveillance" that is subject to FISA, taking into account the changes in technology since 1978. Second, although the President may have had Commander-in-Chief Clause authority to engage in a range of surveillance activities incident to conducting a lawful war, in the absence of congressional legislation limiting such discretion, the Supreme Court has consistently upheld the authority of Congress to limit that authority. In this context, Congress intended to foreclose the authority the President might have previously had under the Constitution to conduct such surveillance without statutory authority. The same section of FISA also forecloses employing foreign intelligence electronic surveillance authority in any other statute—only a clear authorization in a statute subsequent to FISA could overcome the original preclusion.

The administration has argued that the Authorization for the Use of Military Force (AUMF) permits the NSA surveillance, extrapolating from the Supreme Court's determination that the AUMF authorized the use of military detention in Hamdi v. Rumsfeld. The AUMF argument could fail on the content distinctions between detention of those captured on a battlefield and electronic surveillance of Americans inside the United States. The distinctions matter less, however, than the stark history of the immediate post-September 11 period. At the same time that Congress passed the AUMF, it was considering versions of what later became the Patriot Act. Among the most

important features of the Patriot Act were those that amended FISA to provide greater tools for the government in the war on terrorism. It is difficult to conclude that the AUMF permitted electronic surveillance inside the United States beyond what Congress was simultaneously revising in FISA. Apart from its questionable application to electronic surveillance inside the United States, the AUMF should not be read to overcome the "exclusivity" provision of FISA. The comprehensiveness of FISA is reinforced by the section that permits electronic surveillance without approval by the FISC for fifteen days immediately following a declaration of war.

The stronger constitutional argument for the administration is that Article II permits the President to authorize warrantless surveillance of Americans inside the United States to gather information about terrorist activities. Two courts of appeal so held before FISA was enacted. Now, however, the constitutional question is whether FISA is unconstitutional in restricting the President's authority to warrantless surveillance. Congress enacted FISA pursuant to its Commerce Clause authority to regulate wire communications between states and between nations. FISA is also an exercise of the Necessary and Proper Clause, because it serves to "carry[] into execution" other national security powers of Congress and also because it reaches NAA (part of the Department of Defense) incident to its power "to make Rules for the Govern-

---

risation information sharing between law enforcement and intelligence agen-
rising electronic surveillance); §§ 201, 210, 212, 115 Stat. 273, 283-96 (amend-
ing 18 U.S.C. §§ 2518, 2702, 2710 (2000)) (allowing access to wire and elec-
thority and access to business records of United States persons); §§ 214, 115 Stat. 272, 291 (amending 50 U.S.C. § 1894 (2000)) (changes in the purpose,
standard).


472. See U.S. Const. art. II § 2, cl. 3.

473. United States v. Bates, 469 F.2d 550, 605-06 (D.C. Cir. 1974); United

474. See 1607 Congress of David R. Krietz, supra note 318 (implying the separa-
tion of powers by balancing and concluding that "a line must be drawn on the fact")

475. U.S. Const. art. I, § 8, cl. 3.
for electronic surveillance or search. To provide an explicit escape from FISA for the executive branch would likely curtail significantly the FISC oversight that emergency applications currently receive.

Despite General Hayden's claims that the TSP is narrowly focused on targets that are reasonably suspected of terrorist links and is not a dragnet or massive data mining program, proposals were made to amend FISA to authorize "programmatic approvals of cutting-edge technologies—including automated monitoring of suspected terrorist communications." Kim Taipale argues that FISA should be amended so that its definition of "electronic surveillance" can accommodate orders to capture the data and voice communications inside modern networks. He also acknowledges that the automated monitoring that Hayden favors could not be done under FISA as it now stands because the intercepts would not meet the probable cause standard, even if submitted retroactively under the emergency authority.

The administration-backed proposals to amend FISA would ratify the TSP by authorizing the FISC to approve "electronic surveillance programs" inside the United States, for up to ninety days, renewable by the FISC. Such a program would have as a "significant purpose the gathering of foreign intelligence information or protecting against international terrorism" where it is "not feasible" to name the targets or locations, where "flexibility" is required for "effective" surveillance, and where an "extended period" of surveillance is contemplated. The FISC could authorize a program for up to 90 days initially, and the court could reauthorize a program for any "reasonable" period. If the FISC denied an application, the Attorney General could reapply or appeal to the FISC. If, during an approved program of surveillance, the Attorney General determines that any target of the program could satisfy the criteria for individualized consideration under FISA, surveillance of that target must be discontinued unless an ap-

1281

1282

lication is made, either for continued programmatic surveillance or for an individual order of surveillance from the FISC.

So styled, this proposal is just as devastating to FISA as the repeal of the exclusivity provision. The "program" could be used when its sole purpose is the collection of evidence for prosecution, and, instead of any version of a probable cause requirement, the program has only to be "reasonably designed" to meet its objectives. The "electronic surveillance program" could become the contemporary general warrant, going beyond even what has been publicly described as the TSP.

The administration-backed proposals also expand the definition of "agent of a foreign power" to reach non-U.S. persons who possess, control, transmit, or receive significant foreign intelligence information while in the United States. This definition requires no connection of the target to a terrorist organization and no showing of a link to international terrorism. Both approaches end the collaborative roles of Congress and the judiciary in monitoring intrusive surveillance for foreign intelligence inside the United States, and both restore constitutional doubt to one of the administration's most important counters to the threat of terrorism.

One of the main choke points in FISA is the expansive definition of "electronic surveillance." Whether by present drafting or simple luck, the definition is broad enough to reach communications technologies, including many of the technologies that NSA uses. To avoid becoming ensnared in traditional FISA procedures, the 2006 bills the administration favors would narrow the previously expansive definition, enabling NSA electronic monitoring or data mining so long as the government is not intentionally targeting a United States person inside the United States. No order of the FISC would be required in these situations, including the vast vacuum cleaner-like operations of NSA. Warrantless surveillance would be expressly permitted under these bills, including any communication between a U.S. person and foreign power or agent of foreign power, so long as the target is one of the latter.
categories.696 Existing minimization requirements would also be eliminated, so that the contents of electronic communications of U.S. persons could be stored and disseminated without statutory restrictions.697

A more modest set of proposals seeks to retain the FISA compromise, update some provisions in light of changing technologies, and assure that the Justice Department has adequate resources and personnel to meet the challenges of the FISA processes.698 One bill would extend the FISA emergency period from seventy-two hours to seven days and allow the Attorney General to delegate the authority to approve FISA applications and to authorize emergency surveillances.699 This bill would also require development of improved management systems for facilitating the FISA application process and authorize hiring more staff to meet the demands of regular or emergency applications under FISA.700 While these measures may stand the least chance of enactment in the short term, their enactment could actually restore some elements of the FISA compromise.

As described by Attorney General Gonzales and General Hayden, the TSP targets communications involving those for whom there is reasonable suspicion of a link to al Qaeda or a group of affiliates of al Qaeda.701 Monitoring occurs then only if one end of the communication is abroad.702 Although this warrantless electronic surveillance itself violates FISA, the leading bills would ratify the TSP and then go farther and permit the twenty-first century equivalent of general warrants.703 Viewed in the aggregate, the bills would authorize NSA to listen in on the contents of phone conversations of U.S. citizens inside the United States without probable cause or even reasonable suspicion (i.e., the “program” must be “reasonably designed” to intercept the communications of suspected terrorists) that the person is connected in any way to terrorism—even where the conversation itself has nothing to do with terrorism (interruption permitted of a person who “is reasonably believed to have commu-
2007] THE DEATH OF FISA 1285

sketched using the roving wiretap provision,858 the enhanced pen register and trap and trace authorities,859 or the expansion of the national security letters and document production authorities to reach "any tangible thing."860

After a modest expansion of information sharing authority in FISA by the Homeland Security Act of 2002,861 the 2004 intelligence reform legislation significantly expanded FISA by adding the "lone wolf" amendment to "agent of a foreign power."862 As the sunsets loomed in 2008, Congress approved short-term extensions until enacting the USA PATRIOT Reauthorization Act of 2005 in March 2006.863 Fourteen of the sixteen provisions due to sunset were made permanent in the Act, while the roving wiretaps, "tangible thing," and "lone wolf" provisions were extended until the end of 2009.864

Even if Congress enacted none of the proposals to amend FISA being considered at the end of the 109th Congress, it is fair to say that the compromise collapsed with September 11. Perhaps the richest example of how the emergency atmosphere worked to undo the compromise that served well for more than two decades is the review of the Patriot Act purpose change by the FISC and the FISCR. At the time, that group of seven FISC judges probably understood FISA mechanics, processes, and the delicate balancing of interests it represented better than anyone. In the face of the emergency and the statutory change, the judges did their best to preserve the central purpose of FISA while respecting the changes made in the Patriot Act. The FISC opinion reached a fair accommodation of the competing interests, even though the court's emphasis on complying with the minimization requirements of FISA struck many readers, including the FISCR, as not responsive to the government's argument and not as central to their outcome as the original purposes of FISA and its reasonableness in light of the Fourth Amendment.

599. Patriot Act, § 206.
600. Id. § 214.
601. Id. §§ 215, 502, see Schillerhof supra note 192, at 844-45.
605. Id. § 103. 120 Stat. 195 (2000).

1286 MINNESOTA LAW REVIEW [91:1209

Minimization procedures are designed to protect U.S. persons from having what would typically be the inevitable by-product of indiscriminate electronic surveillance—communications intercepted that are not foreign intelligence—from being acquired, retained, or disseminated.865 As the FISC saw a FISA future under the proposed OIPR procedures, the amount of non-foreign intelligence information that would be collected would increase, and the possibility of direction and control of a FISA investigation meant that considerable non-foreign intelligence information would be collected, stored, and disseminated.866 In effect, the FISC worried that FISA would be used to enforce the criminal law, and that application of FISA surveillance would be inconsistent with the underlying purpose of minimization.867

Based on the long experience of the FISC judges in working with FISA and its implementation, their concern with the effects of the new procedures on minimization was understandable. Particularly since the 1995 procedures promulgated by Attorney General Reno heightened the sensitivities of FISC judges to inappropriate uses of FISA in criminal investigations, the court was especially wary of endorsing what could be seen as a way to work around the rigor of Title III warrants.868 Yet the FISC was, to some extent, a prisoner of its limited perspective and its symbiotic relationship with OIPR. Without meaningful oversight by Congress or other Article III courts, the FISC was "coached" by OIPR after 1995 to elevate the wall and information screening procedures beyond the statutory requirements.869 FISA failed to explain the prohibition on the Criminal Division directing or controlling FISA surveillance, but it did not justify the restrictive screening walls that stood in the way of effective cooperation and coordination. Thus, the 2002 FISC decision puzzled many observers. If the proposed OIPR procedures would enable prosecutors to use FISA when obtaining Title III warrants was too difficult, the more viable and concrete legal problem was that the purpose of the investigation was no

601. Id. at 406-07.
602. See 9/11 COMMISSION REPORT, supra note 107, at 78.
longer to collect foreign intelligence, or that the surveillance would be undertaken in violation of the Fourth Amendment. It was understandable for the FISC to rule that the FISA for basing their decision on the FISA minimization requirements, and for failing to respond directly to the Patriot Act arguments advanced by the government. As the FISC construed FISA, the minimization requirements allow the dissemination for law enforcement purposes of non-foreign intelligence information that is evidence of ordinary crimes.491 In addition, the FISC correctly noted that expanding foreign intelligence collection to include evidence of crimes is not the same as directing a FISA investigation for the purpose of building a criminal case.492 In addition, the "chaperone requirement" that the FISC fashioned and the FISC overturned,493 where OPR was to "be invited" to all meetings between the intelligence and criminal division staff, was cumbersome and not essential to the preservation of the foreign intelligence essence of FISA.

Still, it was not "quite pusillanimous," as the FISC proclaimed, that the pre-Patriot Act Justice Department read FISA "as limiting the Department's ability to obtain FISA orders if it intended to prosecute the targeted agents—even for foreign intelligence crimes."494 As noted above, the FISC confused what FISA surveillance is used for with the purpose for seeking FISA procedures. Even though the foreign agency definition is, as the FISC noted, "grounded on criminal conduct,"495 That OPR misconstrued the procedures and applied them in a skewed fashion to erect barriers to sharing information is highly unfortunate, but it is not a justification for eliminating the central protection against law enforcement direction and control of the FISA process. FISA requires a significant foreign intelligence purpose before surveillance may be approved by the FISC. It was that assurance that the FISC was understandably seeking to protect.

In any case, reversal of the FISC was an overreaction, and the rhetoric of crisis and fear appeared to outstrip calm reflection in its opinion. In their first ever consideration of a FISA matter, the three judges misunderstood the historical distinctions about primary purpose that FISA case law created.
the collateral crime—credit card fraud, for example—will be connected to the terrorist activities and will thus present an easy "significant purpose" determination in the FISA certification. If, however, the strategy at the time the FISA application is made is to find the evidence of crimes unrelated to the foreign intelligence—a suspected terrorist who consumes child pornography, for example—FISA should not be available for the surveillance because the law enforcement and foreign intelligence interests are not intertwined, and the enforcement procedures should be available for investigation and prosecution of the crimes. If some unrelated collateral crimes are discovered later, during FISC-approved foreign intelligence collection, then the criminal evidence should be available in a prosecution. Although a "significant" foreign intelligence purpose is present in both examples, the purpose of the FISA processes would be subverted if the unrelated collateral crimes strategy is allowed to direct and control FISA surveillance.

1. Minimization Reforms?

Consistent with the prevention strategy, it would be possible to amend the minimization requirements in FISA to permit more real time information sharing between foreign intelligence and law enforcement investigators. As FISA minimization is now prescribed, criminal evidence obtained through FISA procedures disseminated for law enforcement purposes as evidence of a crime "which has been, is being, or is about to be committed." Minimization thus requires that responsible officials make an a priori or contemporaneous decision that the collected information is evidence of a crime. (The Sorkiasian, Duggan, Hammod, and Lakhani examples in the introduction to this Article are model applications of permissible sharing of law enforcement information consistent with the minimization requirements.) In Sorkiasian, Duggan, and Lakhani, the collection of foreign intelligence led to the evidence of the crimes. Once the crimes were discovered, the FISA surveillance came to an end. In Hammod, the cigarette smuggling and support for Hashollahi investigations overlapped, but the FISA surveillance was reviewed by the courts and was found to

532. See supra text accompanying notes 42-55.
533. See supra text accompanying notes 42-55.
534. See supra text accompanying notes 42-55.
535. See supra text accompanying notes 42-55.
536. See supra text accompanying notes 42-55.
537. See supra text accompanying notes 42-55.
THE DEATH OF FISA

with the collected intelligence? Is the inevitable high rate of false positives and accompanying chilling of protected expression and individual privacy worth the gain in surveillance discretion?540

2. An Exclusionary Rule for FISA?

Alternatively, minimization could be better managed by the FISC if the federal courts were to enforce a species of exclusionary rule, where the government would be prevented from using FISA-obtained information as evidence in a prosecution of a target for a so-called collateral crime—one having nothing to do with terrorism or national security—if some of the evidence demonstrated that the criminal conduct had any connection to terrorism or national security.541 If this form of use limit were faithfully observed and enforced, the damage done to the purpose rule by the Patron Act and the FISC decision could be repaired, after the fact. Instead of the ex ante purpose rule, the use limit would accomplish the same end ex post.542 The potential for privacy invasions by investigators using FISA inappropriately would remain, but the check on the utility of the misuse would discourage the original invasion.543 Elsewhere I proposed the hypothesis of an international terrorist [who] is also a drug dealer—not to support terrorist activities but to support himself.544 If FISA surveillance is obtained and evidence of the drug dealing derived from the FISA surveillance is offered as evidence, it should be excluded under this approach, while the same material would be admissible if the target is charged with using his narcotics to energize a support network. In addition, a use limit would, unlike FISA minimization, be based on Fourth Amendment reasonableness and not on the terms of FISA, thus enabling the protections of the use limit to be enjoyed by targets who are not U.S. persons.545

540. A full consideration of these issues is beyond the scope of this Article. They are explored generally in MANNIX, supra note 37, pages. See also DANIEL J. SEBEN, Digital Detours and the Disruption of Fourth Amendment Privacy, 79 CHI. L. REV. 1969 (2002).


542. Id. at 103.

543. Id.

544. DAVIS, supra note 18, at 1178.

545. Hall, supra note 544, at 109.

MINNESOTA LAW REVIEW

If some sort of ex post use limit is employed to lessen the minimization task and shore up the weakened purpose requirement in FISA, would the cure be worse than the disease, i.e., would the use limit stand in the way of effective national security or counter-terrorism investigations that do not result in criminal prosecutions? For example, if FISA surveillance uncovers information ultimately insufficient to build a criminal case related to terrorism, but obtains enough information to deport the target for a visa overstay or to prosecute for an unrelated crime, the target might raise the use limit in an eventual deportation hearing or criminal proceeding through the ex parte, in camera hearing to suppress the evidence. Conceivably, the executive could be forced to expose intelligence sources and methods, or simply to alert the target to the nature of the FISA investigation. These are not trivial concerns, but their resolution, if a use limit were accepted and utilized, would likely parallel the outcomes of challenges by criminal defendants under the pre-Patriot Act primary purpose standard—the courts uniformly upheld the FISA surveillance with a high level of deference to the executive branch and the FISC.546

3. Improved Oversight of FISA Activities

Because Congress and the courts have not provided meaningful oversight of FISA activities, the FISC has served an important oversight capacity in addition to its responsibility to review applications for surveillance. In 2000, the FISC complained that several applications to the court contained factual inaccuracies.547 Thereafter, the FBI developed FISA verification procedures to better ensure the accuracy of the facts in each FISA application, particularly those concerning the probable cause determination, and the existence and nature of any parallel law enforcement processes or prior or ongoing asset relationship involving the target. The procedures require computer database searches and efforts to check the status of the target with other units of the FBI.548 When FOIA requests

546. Id. at 120.


2007] THE DEATH OF FISA 1293
turned up additional data two years later, the FBI detailed over
one hundred instances over two years where procedural re-
quirements of FISA may not have been met, such as conducting
wiretaps that were broader in scope and longer in duration
than approved by the FISC.549 This recent record reinforces the
importance that Congress should attach to oversight of the
FISA processes. Whether Congress provides greater oversight
itself or through the FISC, it should not be left to the discre-
tion of the Department of Justice to decide whether and how to use
the FISA processes.550

E. REVISIONS TO FISA TO ACCOMMODATE THE TSP

During a September 15, 2006 news conference, President
Bush commented on the bills in Congress that would amend
FISA to account for the NSA surveillance program. One ques-
tioner asked about the "eavesdropping program." The President
responded: "Yes, the illegal eavesdropping program you
wanted to call it... TFP, as opposed to TSP."551

To those who doubt that the technology-challenged Con-
gress is capable of legislating an effective system for surveil-
ance of would-be terrorists, recall that the Bush administra-
tion specifically stated in 2001 that the Patriot Act allowed
"surveillance of all communications used by terrorists," and
that the Act makes us able to "better meet the technological
challenges posed by this proliferation of communications tech-
nology."552 In March 2006, when the Patriot reauthorization
was completed and most of the sunsets repealed, the Justice
Department reiterated that the Patriot Act provisions "brought
the federal government's ability to investigate... into the
modern era—by modifying our investigative tools to reflect
modern technologies."553 So far as all but a handful of members

549. Eric Lichtblau, Justice Dept. Report Cites Intelligence-Rule Violations
by FBI, N.Y. TIMES, Mar. 9, 2006, at A21.
550. See Schulte, supra note 163, at 541-42 (arguing greater FISA over-
sight of individual cases by FISC judges as well as public and congressional
oversight).
551. President's News Conference 42 WEEKLY COMP. PRES. DOCS. 1617
(June 15, 2006).
552. Remarks on Signing of the USA PATRIOT ACT of 2001, 2 PRES. Pr.
PRES. 1307 (Oct. 28, 2001).
553. U.S. DEP'T OF JUSTICE, FAST FORGE: USA PATRIOT ACT IMPROVEMENTS

1294 MINNESOTA LAW REVIEW [91:1209

of Congress knew, it had not the technological demands of the
executive branch for effective surveillance authorities.

Nonetheless, some variant of the TSP program could be ac-
commodated after changes to FISA that would not rip apart the
fabric of the Act. First, FISA could be amended to permit sur-
veillance from "within the United States" of the electronic
communications of an agent of a foreign power abroad who is
talking to a U.S. person. Modern communications packets of
foreign-to-foreign calls or e-mails of non-U.S. persons may pass
through the United States as a function of the way that tech-
nology operates.554 The revelation that NSA has been doing just
that in the TSP, with the cooperation of telecommunications
providers, lets those who we might intercept know something
about U.S. capabilities that probably was not known—that
even wholly foreign communications may pass through massive
switches in the U.S. network. Even though the element of sur-
prise has been eliminated, the location of the switch where the
interception of electronic communication by an agent of a for-
793
eign power takes place should not affect its legality.

Second, in situations where the government is targeting
the foreign communications of a non-U.S. person abroad, FISA
does not apply, but if the target calls the United States, the
surveillance must be turned off. While amending FISA to ex-
clude from its coverage such surveillance when incident to an
ongoing electronic surveillance of a non-U.S. person abroad
means that an agency could listen in on innocent persons inside
the United States,555 such a risk might be small in return for the
gain to the overall foreign intelligence value.

Third, the FISA minimization requirements could be made
more flexible. The fact that the FISC and FISC could had funda-
mentally different conceptions of what minimization was de-
digned to accomplish in FISA may be reason enough to revisit
its objectives. More important, minimization should take into
account the contemporary reality that the information collected
cannot always be pigeonholed a priori in a binary world of for-
eign intelligence or criminal violation evidence. Assuming con-
tinued government interest in prosecuting terrorism conspira-
in situations where the government has "special needs" above and beyond ordinary law enforcement. As has been argued elsewhere, the special needs cases have sustained drunk-driving checkpoints and drug testing in schools, programs that are standardized and relatively non-intrusive. But the doctrine has never supported the highly discretionary and intrusive likes of the TSP. When the FISC relied on the "special needs" cases to support the Ashcroft procedures lowering the wall, the judges did so in the context of a system that is based on individualized suspicion and prior judicial approval. TSP contains neither protection.

In the first decision to reach the merits of the TSP, Judge Anna Diggs Taylor ruled that the TSP violated FISA, the separation of powers, and the First and Fourth Amendments. Although the analysis in Judge Taylor's opinion was sparse, and the case is on appeal, several other pending cases may eventually produce a Supreme Court decision on the TSP.

CONCLUSION

So much of the post-September 11 redirection of our counter-terrorism law and policy in the United States has been based on the impassioned rhetoric of the war on terrorism. Often foreclosing reasoned analysis, careful consideration of costs and benefits, and alternative courses of action, our post-September 11 laws and policies have been developed with a sort of bunker mentality, designed to anticipate worst case outcomes. Consider the statement of Vice President Richard Cheney, commenting in the wake of the revelations that a Paki-

558. See, e.g., Letter from Former Government Officials and Law Profes-
561. ACLU v. NSA, 437 F.3d 590, 591 (6th Cir. 2006) (granting motion for a stay pending appeal).
2007] THE DEATH OF FISA 1297

A scientific group with scientific expertise may wish to export nuclear technologies to Muslim nations:

If there’s a one percent chance that Pakistani scientists are helping al-Qaeda build a nuclear weapon, we have to treat it as a certainty in terms of our response. . . . It’s not about our analysis, or finding a preponderance of evidence . . . it’s about our response.\textsuperscript{563}

The prevention policy first announced by Attorney General Ashcroft shortly after September 11 is hardly the same as treating the one percent chance as certainty, but it is closer to policies that treat suspicion as probable cause. What are the marginal costs and benefits to our national security of laws and policies that base their operational terms on a "one percent chance," or even a reasonable suspicion of a horrific consequence? What values and legal safeguards are lost when traditional standards of proof and evidence are eschewed in favor of action based on suspicion or an indiscriminate data mining program? How does a program like TSF serve to disrupt or even expose al Qaeda or other would-be terrorists? And to what extent do secret surveillance initiatives like TSF corrode the democratic values and institutions that we seek to protect from terrorism? At a minimum, the unraveling of FISA and emergence of the TSF call into question the virtual disappearance of effective oversight of our national security surveillance. The Congress and federal courts have become observers of the system, not even participants, much less overseers.\textsuperscript{564}

The circumstances that led to the enactment of FISA nearly thirty years ago—a chastened executive, an awakened Congress, courts newly willing to protect privacy in electronic surveillance settings—may never recur. The imperfect system for national security surveillance that FISA codified worked reasonably well through the early 1990’s. As terrorism ascend in importance as a national security concern and Congress and the President worked to enact new laws criminaliniz-

\textsuperscript{563} Ron Sohnke, The One Percent Solution: Deep Inside America’s Pursuit of Its Enemies Rome II, at 62 (2001) (quoting Vice President Richard Cheney); see also id. at 67-69 (discussing the background of the Pakistani group and its objectives).

\textsuperscript{564} Jack Balkin & Sanford Levinson argue that an emerging "National Surveillance State" will be driven principally by technological advances and national security interests. The executive branch will, they say, make decisions to deploy the criminal justice system with security measures and to make other elements of our political system like the national security system. Jack M. Balkin & Sanford Levinson, The Promise of Constitutional Change From Foreign Intrusion to the National Surveillance State, 72 FOREIGN L. REV. 489, 522-23 (2006).

1298 MINNESOTA LAW REVIEW [91:1299

ing terrorist activities, pressures on the FISA process increased and its careful accommodation of foreign intelligence and law enforcement interests was eroded in bureaucratic confusion, institutional rivalries, and personal and inter-agency jealousies.\textsuperscript{565}

When the Patriot Act followed soon after September 11, the institutional and bureaucratic barriers to sharing intelligence information that contributed to the failure to anticipate the hijackers were misapplied and translated into a legal change to FISA that was showcased as breaking down the wall that kept us from preventing the attacks. The ensuing revision of Justice Department guidelines and their review by the FISC and FSCR struck a serious blow to the essential terms of the FISA arrangement—providing a mechanism for secret surveillance with reduced predicates for targeting, in return for a commitment that the special process would not be used by criminal prosecutors who simply could not meet the traditional warrant requirements. Now the fear expressed by the FISC in 2003—that abuses of FISA could increasingly occur—has been fulfilled.

David Kris has pointed out an argument that keeping the wall down may enhance civil liberties. Kris reasons that, with the wall out of the way, "more DOJ lawyers may become involved in national security investigations. . . . More lawyers mean more oversight, and lawyer oversight is how we protect[ ] civil liberties in intelligence." Second, Kris argued, using law enforcement to counter foreign threats is, considering alternative methods available to the government, "among the most benign. The wall channels government toward more extreme measures."\textsuperscript{566}

Kris correctly observes that the Church Committee Report concluded that retaining domestic security investigations to a legal framework under the supervision of the Attorney General was one of the fundamental corrective to the abuses uncovered.\textsuperscript{567} As FISA, FBI Guidelines, and executive orders were
THE DEATH OF FISA

example involved the Department's investigations of suspected Al Qaeda cell members in Lackawanna, New York, the so-called "Lackawanna Six." The investigation began in the summer of 2001, based on an anonymous tip delivered to the FBI that local Yemeni-Americans might be involved in drug crime and terrorist activities. Initially, FBI concluded that existing law required the creation of two separate investigations in order to retain the option of using FISA. As the Department, the Patriot Act made clear that information sharing between the two teams was allowed, which in turn let the criminal side know that an Al Qaeda agent was involved, leading to early criminal charges against the six. This Article has shown that neither the 1978 FISA nor the 2001 FISA, as amended by the Patriot Act, stood in the way of simultaneous investigations of the same target or targets, in parallel or as one team, so long as the purpose of the FISA investigation was the collection of foreign intelligence. The wall procedures that appeared in 1995 were not required by FISA and even those would have permitted the sharing that allegedly could not occur in the Lackawanna investigation, so long as the Criminal Division did not direct or control the FISA investigations. 571

Meanwhile, rapid and accelerating changes in technology and in particular the digitization of surveillance and communications presented Congress and the President with ongoing challenges to keep up with and exceed the communications and evasion capabilities of adversaries. While FISA was amended toward these ends to the apparent satisfaction of the executive branch, the administration approved NSA surveillance and the TSP. Consistent with the prevention paradigm, the TSP overflows probable cause and individualized suspicion and judicial

566. See supra note 560, at 527.

568. Kris v. supra note 560, at 527.

571. In addition to the Lackawanna investigation, the Justice Department filed seven other examples "made possible by the USA PATRIOT Act," 846 et seq. (July 2003), available at http://www.fbi.gov/leg/toptopics/patriot0704.pdf.
and congressional oversight and review, all hallmarks of FISA. The extent to which digital capabilities render these central legal instruments obsolete in a complex topic that could only briefly be considered in this Article. Whatever the answer to this digital revolution, however, it is clear that what remains of FISA has been ignored.

In our legal system, we attach great importance to the value of fair processes. In national security law and policy, where secrecy has been an important operational requisite, we have developed review and oversight processes to help assure that unilateral power is not abused. So has it been with FISA. In the five years since September 11, those process safeguards have largely been lost or overtaken. If FISA is to have any meaningful role for the next thirty years, its central terms will have to be restored, one way or the other.
The Basis for the NSA’s Call-Tracking Program Has Disappeared, If It Ever Existed [Updated]

By Jameel Jaffer
Thursday, November 7, 2013 at 9:00 AM

There’s a significant discrepancy, one that deserves more attention, between what the NSA told the Foreign Intelligence Surveillance Court five years ago about the call-tracking program and what the agency is telling ordinary federal courts about the program now. It told the FISC five years ago that the program was indispensable, but it’s saying something quite different today.

From recently released documents, we know that in 2008 the NSA asked the FISC to reauthorize the call-tracking program, a program the FISC had first authorized two years earlier. The FISC obliged, issuing an order that permitted the NSA to continue collecting information about essentially all telephone calls made or received on U.S. telephone networks, subject to “minimization requirements” restricting the government’s access to information collected under the program. In reauthorizing the program, the FISC relied on representations from the government about the program’s importance and the feasibility of tracking suspected terrorists’ associations through other, less intrusive means. We know about these representations because in his March 2009 opinion describing the NSA’s “frequent[] and systemic[ ]” violation of the minimization requirements, Judge Reggie Walton had this to say:

On December 12, 2008, the [FISC] re-authorized the government to acquire the tangible things sought by the government in its application in the above-captioned docket (“BR 08-13”). . . . The Court found reasonable grounds to believe that the tangible things sought are relevant to authorized investigations being conducted by the [FBI] to protect against international terrorism. . . . In making this finding, the Court relied on the assertion of the [NSA] that having access to the call detail records “is vital to NSA’s counterterrorism intelligence mission” because “[t]he only effective means by which NSA analysts are able continuously to keep track of all affiliates of one of the aforementioned entities [who are taking steps to disguise and obscure their communications and identities], is to obtain and maintain an archive of metadata that will permit these tactics to be uncovered.”
A few things about this passage are worth noting. First, it makes clear that the government represented to the FISC not simply that the call-tracking program was useful but that it was crucial—“vital”—to the NSA’s mission. Second, it makes clear that the government represented that there were no less-intrusive means of achieving its objectives. The call-tracking program, the NSA told the FISC, was “the only effective means” of “keep[ing] track” of suspected terrorists’ associations. Third, the passage makes clear that the FISC relied on the government’s representations. In other words, the FISC reauthorized the program because the government said that the program was indispensable.

It seems significant, then, even remarkable, that the government has not made similar representations in the Southern District of New York, where the ACLU’s challenge to the call-records program is pending before Judge William Pauley. In the declarations in which one might expect to find the phrases “only effective means” and “vital to the NSA’s counterterrorism mission,” here is the language one finds instead (with my italics):

The call-tracking program is “one method that the NSA has developed to accomplish the objective” of “[d]etecting threats by exploiting terrorist communications.” Declaration of FBI Acting Assistant Director Robert J. Holley at ¶5.

“[E]xperience has shown that NSA metadata analysis, in complement with other FBI investigatory and analytical capabilities, produces information pertinent to FBI counter-terrorism investigations, and can contribute to the prevention of terrorist attacks.” Declaration of FBI Acting Assistant Director Robert J. Holley at ¶9.

The call-tracking program is “[o]ne method that the NSA has developed” to “detect any terrorist threat inside the U.S.” Declaration of NSA Signals Intelligence Director Teresa H. Shea, National Security Agency at ¶7.

The call-tracking program is “[o]ne method that the NSA has developed” to “detect any terrorist threat inside the U.S.” Declaration of NSA Signals Intelligence Director Teresa H. Shea, National Security Agency at ¶7.

“Without the ability to obtain and analyze bulk metadata, the NSA would lose a tool for detecting communications chains that link to identifiers associated known and suspected terrorist operatives.” Declaration of NSA Signals Intelligence Director Teresa H. Shea, National Security Agency at ¶58.

The government’s response to the petition filed by the Electronic Privacy Information Center uses similarly weak language: Without the call-tracking program, the government writes, “it may not be feasible for the NSA to identify chains of communications that cross different telecommunications networks.”
It seems to me that there’s a lot of distance between the representations the government was willing to make to the FISC in 2008 and the representations it’s willing to make now. There’s a lot of distance, that is, between “the only effective means,” on the one hand, and “one method that the NSA has developed,” on the other. We could speculate about the reasons for the shift in the NSA’s language. Perhaps the government’s assessment of the program’s importance has changed since 2008. Perhaps the government was willing to say things in an ex parte proceeding that it’s not willing to say in an adversarial one. Or perhaps the fallout to DNI James Clapper’s “least untruthful statement” has led intelligence officials to take more care in making factual claims about the NSA’s surveillance activities.

Whatever the reason for the government’s shift, though, it’s a shift that utterly undermines the representations the government made to the FISC in 2008—representations that the FISC itself said it relied on in determining that the program should be reauthorized. If the government’s “only effective means” representation was crucial to the FISC’s reauthorization of the program in 2008, as Judge Walton’s opinion suggests it was, shouldn’t the government’s quiet retreat from that representation lead the FISC to withdraw its authorization for the program?

And if the government is no longer willing to say in court what it said in 2008, isn’t it fair to say that the government is asking Judge Pauley to hold something that the FISC has never held—namely, that the call-tracking program is lawful and reasonable under the First and Fourth Amendments even if it’s not “vital” to the NSA’s counterterrorism efforts, and even if there are less intrusive means that the NSA could employ to achieve the same ends?

And if the government is no longer willing to say to federal judges that the program is crucial and the least-intrusive means of accomplishing its counterterrorism objectives, isn’t it reasonable for us to ask why intelligence officials are still making those claims to the public?

ADDENDUM: As Marty Lederman observed in these two posts, although in its White Paper and its opening brief in ACLU v. Clapper the government embraced Judge Eagan’s argument that the collection satisfied section 215 because it is “necessary” for FBI counterterrorism investigations, the Solicitor General’s Office abandoned that argument in its Supreme Court filing in EPIC, perhaps because it realized that it would be very difficult to satisfy such a threshold (or because it was unable to find declarants who would attest to such a strong claim). The government is now arguing instead that the statute doesn’t require it to show that the call-tracking program is necessary or indispensable or “the only effective means”—only that the program “facilitate[s] the government’s use of investigative tools.” As Marty explains in the second of the two posts, and as we at the ACLU explain at
pages 11-12 of this brief, this new theory of the statute—apparently not the theory adopted by the FISA Court—proves far too much, because adopting it would allow the government to collect virtually any system of records. After all, access to virtually any such system would *facilitate* investigations.

FILED UNDER: *Civil Liberties, Courts, Featured*

**ABOUT THE AUTHOR**

*Jameel Jaffer* is Deputy Legal Director at the American Civil Liberties Union and Director of the ACLU’s Center for Democracy. Follow him on Twitter (@JameelJaffer).

SEND A LETTER TO THE EDITOR
Testimony of

Jameel Jaffer
Deputy Legal Director of the
American Civil Liberties Union Foundation

Laura W. Murphy
Director, Washington Legislative Office
American Civil Liberties Union

Before
The Senate Judiciary Committee

Strengthening Privacy Rights and National Security:
Oversight of FISA Surveillance Programs

July 31, 2013

On behalf of the American Civil Liberties Union (ACLU), its hundreds of thousands of members, and its fifty-three affiliates nationwide, thank you for inviting the ACLU to testify before the Committee.

Over the last two months it has become clear that the National Security Agency (NSA) is engaged in far-reaching, intrusive, and unlawful surveillance of Americans’ telephone calls and electronic communications. These unconstitutional surveillance programs are the product of defects both in the law itself and in the current oversight system. The Foreign Intelligence Surveillance Act (FISA) affords the government sweeping power to monitor the communications of innocent people. Excessive secrecy has made congressional oversight difficult and public oversight impossible. Intelligence officials have repeatedly misled the public, Congress, and the courts about the nature and scope of the government’s surveillance activities. Structural features of the Foreign Intelligence Surveillance Court (FISC) have prevented that court from serving as an effective guardian of individual rights. And the ordinary federal courts have improperly used procedural doctrines to place the NSA’s activities beyond the reach of the Constitution.

To say that the NSA’s activities present a grave danger to American democracy is no overstatement. Thirty-seven years ago, after conducting a comprehensive investigation into the intelligence abuses of the previous decades, the Church Committee warned that inadequate regulations on government surveillance “threaten[ed] to undermine our democratic society and fundamentally alter its nature.” This warning should have even more resonance today, because in recent decades the NSA’s resources have grown, statutory and constitutional limitations have been steadily eroded, and the technology of surveillance has become exponentially more powerful.

Because the problem Congress confronts today has many roots, there is no single solution to it. It is crucial, however, that Congress take certain steps immediately.

First, it should amend relevant provisions of FISA to prohibit suspicionless, “dragnet” monitoring or tracking of Americans’ communications. Amendments of this kind should be made to the FISA Amendments Act, to FISA’s so-called “business records” provision, and to the national security letter authorities.

Second, it should end the unnecessary and corrosive secrecy that has obstructed congressional and public oversight. It should require the publication of FISC opinions insofar as they evaluate the meaning, scope, or constitutionality of the foreign-intelligence laws. It should require the government to publish basic statistical information about the government’s use of foreign-intelligence authorities. And it should ensure that “gag orders” associated with national security letters and other surveillance directives are limited in scope and duration, and imposed only when necessary.

Third, it should ensure that the government’s surveillance activities are subject to meaningful judicial review. It should clarify by statute the circumstances in which individuals can challenge government surveillance in ordinary federal courts. It should provide for open and adversarial proceedings in the FISC when the government’s surveillance applications raise novel issues of statutory or constitutional interpretation. It should also pass legislation to ensure that the state secrets privilege is not used to place the government’s surveillance activities beyond the reach of the courts.

Thank you again for the invitation to testify. We appreciate the Committee’s attention to this set of issues.

I. Metadata surveillance under Section 215 of the Patriot Act

On June 5, 2013, The Guardian disclosed a previously secret FISC order that compels a Verizon subsidiary, Verizon Business Network Services (VBNS), to supply the government with records relating to every phone call placed on its network between
April 25, 2013 and July 19, 2013.\footnote{See Glenn Greenwald, NSA Collecting Phone Records of Millions of Verizon Customers Daily, Guardian, June 5, 2013, http://bit.ly/13judib.} The order directs VBNS to produce to the NSA "on an ongoing daily basis... all call detail records or ‘telephony metadata’ relating to its customers’ calls, including those ‘wholly within the United States.’\footnote{Secondary Order, In Re Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Bus. Network Servs., Inc. on Behalf of MCI Comm’ns Servs., Inc. d/b/a Verizon Bus Servs., No. BR 15-80 at 2 (FISA Ct. Apr. 25, 2013), available at http://bit.ly/11FY3J9.} As many have noted, the order is breathtaking in its scope. It is as if the government had seized every American’s address book—with annotations detailing which contacts she spoke to, when she spoke with them, for how long, and (possibly) from which locations.

News reports since the disclosure of the VBNS order indicate that the mass acquisition of Americans’ call details extends beyond customers of VBNS, encompassing the telephone records of essentially all Americans for at least seven years.\footnote{See Siobhan Gorman et al., U.S. Collects Vast Data Trove, Wall St. J., June 7, 2013, http://on.wsj.com/1luOfhe (“The arrangement with Verizon, AT&T and Sprint, the country’s three largest phone companies means, that every time the majority of Americans makes a call, NSA gets a record of the location, the number called, the time of the call and the length of the conversation, according to people familiar with the matter. ... AT&T has 107.3 million wireless customers and 31.2 million landline customers. Verizon has 98.9 million wireless customers and 22.2 million landline customers while Sprint has 55 million customers in total.”). Siobhan Gorman & Jennifer Valente-DeVries, Government Is Tracking Verizon Customers’ Records, Wall St. J., June 6, 2013, http://on.wsj.com/13mLt7c.}

Intelligence officials have said that the government does not “indiscriminately sift through” the phone-record database. Instead, it queries the database “only when there is reasonable suspicion, based on specific and articulated facts, that an insurer is associated with specific foreign terrorist organizations.”\footnote{See e.g., How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries: Hearing Before the H. Permanent Select Intelligence Comm., 113th Cong. (June 18, 2013)(testimony of NSA Deputy Director John C. Inglis), http://bit.ly/1SS2w6h.} According to a statement released by the government last month, “less than 300 unique identifiers met this standard and were queried” in 2012.\footnote{Dan Roberts & Spencer Ackerman, Senate Frustrated: NSA Phone Call Data Collection in Place Since 2006, Guardian, June 6, 2013, http://bit.ly/13rQ6du. id. (Senator Saxby Chambliss: “This has been going on for seven years.”).} But even if the government ran queries on only 300 unique identifiers in 2012, those searches implicated the privacy of millions of Americans. Intelligence officials have explained that analysts are permitted to examine the call records of all individuals within three “hops” of a specific target.\footnote{See e.g., Ellen Nakashima, Call Records of Fewer Than 300 People Were Searched in 2012, U.S. Says, Wash. Post, June 15, 2013, http://wapo.st/14rZ7Wm.} As a result, a query yields information not only about the individual thought to be “associated with [a] specific foreign terrorist organization[,]” but about all of those separated from that individual by one, two, or three degrees. Even if one assumes, conservatively, that each person has an average of 40 unique contacts, an analyst who accessed the records of everyone within three hops of an initial target would have accessed records concerning more than two million people.\footnote{For ease of reference, this testimony uses “business records provision” to refer to the current version of the law as well as to earlier versions, even though the current version of the law allows the FBI to compel the production of much more than business records, as discussed below.} Multiply that figure by the 350 phone numbers the NSA says that it searched in 2012, and by the seven years the program has apparently been in place, and one can quickly see how official efforts to characterize the extent and impact of this program are deeply misleading.

a. The metadata program is not authorized by statute

The metadata program has been implemented under Section 215 of the Patriot Act—sometimes referred to as FISA’s “business records” provision—but this provision does not permit the government to track all Americans’ phone calls, let alone over a period of seven years.

As originally enacted in 1998, FISA’s business records provision permitted the FBI to compel the production of certain business records in foreign intelligence or international terrorism investigations by making an application to the FISC. See 50 U.S.C. §§ 1861-62 (2000 ed.). Only four types of records could be sought under the statute: records from common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities. 50 U.S.C. § 1862 (2000 ed.). Moreover, the FISC could issue an order only if the application contained “specific and articulated facts giving reason to believe that the person to whom the records pertain[ed] was a foreign power or an agent of a foreign power.”\footnote{See Pete Yost, Congress Expresses Anger Over NSA Surveillance Program, Boston Globe, July 18, 2013, http://bostonglobe.com/17mqWU.}\

The business records power was considerably expanded by the Patriot Act.\footnote{Id.} Section 215 of that Act, now codified in 50 U.S.C. § 1861, permitted the FBI to make an application to the FISC for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities ....

No longer limited to four discrete categories of business records, the new law authorized the FBI to seek the production of "any tangible things." Id. It also authorized the FBI to obtain orders without demonstrating reason to believe that the target was a foreign power or agent of a foreign power. Instead, it permitted the government to obtain orders where tangible things were "sought for" an authorized investigation. P.L. 107-56, § 215. This language was further amended by the USA PATRIOT Improvement and Reauthorization Act of 2005, P.L. 109-177, § 106(b). Under the current version of the business records provision, the FBI must provide "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant" to a foreign intelligence, international terrorism, or espionage investigation. 50 U.S.C. § 1861(b)(2)(A) (emphasis added).

While the Patriot Act considerably expanded the government’s surveillance authority, Section 215 does not authorize the metadata program. First, whatever "relevance" might allow, it does not permit the government to cast a seven-year dragnet over the records of every phone call made or received by any American. Indeed, to say that Section 215 authorizes this surveillance is to deprive the word "relevance" of any meaning. The government’s theory appears to be that some of the information swept up in the dragnet might become relevant to "an authorized investigation" at some point in the future. The statute, however, does not permit the government to collect information on this basis. Cf. Jim Sensenbrenner, This Abuse of the Patriot Act Must End, Guardian, June 9, 2013, http://bit.ly/18sDA3x ("[B]ased on the scope of the released order, both the administration and the FISA court are relying on an unbounded interpretation of the act that Congress never intended."). The statute requires the government to show a connection between the records it seeks and some specific, existing investigation.

Indeed, the changes that Congress made to the statute in 2006 were meant to ensure that the government did not exploit ambiguity in the statute’s language to justify the collection of sensitive information not actually connected to some authorized investigation. As Senator Jon Kyl put it in 2006, "We all know the term ‘relevance.’ It is a term that every court uses. The relevance standard is exactly the standard employed for the issuance of discovery orders in civil litigation, grand jury subpoenas in a criminal investigation."10

As Congress recognized in 2006, relevance is a familiar standard in our legal system. It has never been afforded the limitless scope that the executive branch is

affording it now. Indeed, in the past, courts have carefully policed the outer perimeter of "relevance" to ensure that demands for information are not unbounded fishing expeditions. See, e.g., In re Horowitz, 482 F.2d 72, 79 (2d Cir. 1973) ("What is more troubling is the matter of relevance. The [grand jury] subpoena requires production of all documents contained in the files, without any attempt to define classes of potentially relevant documents or any limitations as to subject matter or time period.").11 The information collected by the government under the metadata program goes far beyond anything a court has ever allowed under the rubric of "relevance."12

b. The metadata program is unconstitutional

President Obama and intelligence officials have been at pains to emphasize that the government is collecting metadata, not content. The suggestion that metadata is somehow beyond the reach of the Constitution, however, is not correct. For Fourth Amendment purposes, the crucial question is not whether the government is collecting content or metadata but whether it is invading reasonable expectations of privacy. In the case of bulk collection of Americans’ phone records, it clearly is.

The Supreme Court’s recent decision in United States v. Jones, 132 S. Ct. 945 (2012), is instructive. In that case, a unanimous Court held that long-term surveillance of an individual’s location constituted a search under the Fourth Amendment. The Justices reached this conclusion for different reasons, but at least five Justices were of the view that the surveillance infringed on a reasonable expectation of privacy. Justice Sotomayor observed that tracking an individual’s movements over an extended period allows the government to generate a "precise, comprehensive record" that reflects "a wealth of detail about her familial, political, professional, religious, and sexual associations." Id. (Sotomayor, J., concurring).

The same can be said of the tracking now taking place under Section 215. Call records can reveal personal relationships, medical issues, and political and religious affiliations. Internet metadata may be even more revealing, allowing the government to learn which websites a person visits, precisely which articles the reads, whom she corresponds with, and whom those people correspond with.

The long-term surveillance of metadata constitutes a search for the same reasons that the long-term surveillance of location was found to constitute a search in Jones. In fact, the surveillance held unconstitutional in Jones was narrower and shallower than the surveillance now taking place under Section 215. The location tracking in Jones was meant to further a specific criminal investigation into a specific crime, and the

---

10 Records are presumptively relevant if they pertain to (1) a foreign power or an agent of a foreign power; (2) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or (3) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation. This relaxed standard is a significant departure from the original threshold, which, as noted above, required an individualized inquiry.


12 See also Hale v. Henkel, 201 U.S. 43, 76-77 (1906).

13 The metadata program also violates Section 215 because the statute does not authorize the prospective acquisition of business records. The text of the statute contemplates "release of "tangible things" that can be "fairly identified," and "allow[s] a reasonable time" for providers to "assemble" those things. 50 U.S.C. § 1861(c)(1)(T). These terms suggest that Section 215 reaches only business records already in existence.
government collected information about one person's location over a period of less than a month. What the government has implemented under Section 215 is an indiscriminate program that has already swept up the communications of millions of people over a period of seven years. Some have defended the metadata program by reference to the Supreme Court's decision in Smith v. Maryland, 442 U.S. 735 (1979), which upheld the installation of a pen register in a criminal investigation. The pen register in Smith, however, was very primitive—it tracked the numbers being dialed, but it didn't indicate which calls were completed, let alone the duration of the calls. Moreover, the surveillance was directed at a single criminal suspect over a period of less than two days. The police were not casting a net over the whole country.

Another argument that has been offered in defense of the metadata program is that, though the NSA collects an immense amount of information, it examines only a tiny fraction of it. But the Fourth Amendment is triggered by the collection of information, not simply by the querying of it. The NSA cannot insulate this program from Fourth Amendment scrutiny simply by promising that Americans' private information will be safe in its hands. The Fourth Amendment exists to prevent the government from acquiring Americans' private papers and communications in the first place.

Because the metadata program vacuums up sensitive information about associational and expressive activity, it is also unconstitutional under the First Amendment. The Supreme Court has recognized that the government's surveillance and investigatory activities have an acute potential to stifle association and expression protected by the First Amendment. See, e.g., United States v. U.S. District Court, 407 U.S. 297 (1972). As a result of this danger, courts have subjected investigatory practices to "exact[ing] scrutiny" where they substantially burden First Amendment rights. See, e.g., Clark v. Library of Congress, 750 F.2d 89, 94 (D.C. Cir. 1984) (FBI field investigation), In re Grand Jury Proceedings, 776 F.2d 1099, 1102-03 (2nd Cir. 1985) (grand jury subpoena). The metadata program cannot survive this scrutiny. This is particularly so because all available evidence suggests that the program is far broader than necessary to achieve the government's legitimate goals. See, e.g., Press Release, Wyden, Udall Question the Value and Efficacy of Phone Records Collection in Stopping Attacks, June 7, 2013, http://1.usa.gov/19Q1NiR ("As far as we can see, all of the useful information that it has provided appears to have also been available through other collection methods that do not violate the privacy of law-abiding Americans in the way that the Patriot Act collection does.")

c. Congress should amend Section 215 to prohibit suspicionless, dragnet collection of "tangible things"

As explained above, the metadata program is neither authorized by statute nor constitutional. As the government and FISC have apparently found to the contrary, however, the best way for Congress to protect Americans' privacy is to narrow the statute's scope. The ACLU urges Congress to amend Section 215 to provide that the government may compel the production of records under the provision only where there is a close connection between the records sought and a foreign power or agent of a foreign power. Several bipartisan bills now in the House and Senate should be considered by this Committee and Congress at large. The LIBERT-E Act, H.R. 2399, 113th Cong. (2013), sponsored by Rep. Conyers, Rep. Justin Amash, and forty others, would tighten the relevance requirement, mandating that the government supply "specific and articulable facts showing that there are reasonable grounds to believe that the tangible things sought are relevant and material," and that the records sought "pertains only to an individual that is the subject of such investigation." A bill sponsored by Senators Udall and Wyden, and another sponsored by Senator Leahy, would also tighten the required connection between the government's demand for records and a foreign power or agent of a foreign power. Congress could also consider simply restoring some of the language that was deleted by the Patriot Act—in particular, the language that required the government to show "specific and articulable facts giving reason to believe that the person to whom the records pertain[s] is a foreign power or an agent of a foreign power."

II. Electronic surveillance under Section 702 of FISA

The metadata program is only one part of the NSA's domestic surveillance activities. Recent disclosures show that the NSA is also engaged in large-scale monitoring of Americans' electronic communications under Section 702 of FISA, which codifies the FISA Amendments Act of 2008. Under this program, labeled "PRISM" in NSA documents, the government collects emails, audio and video chats, photographs, and other Internet traffic from nine major service providers—Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple. The Director of National Intelligence has acknowledged the existence of the PRISM program but stated that it involves surveillance of foreign nationals outside the United States. This is misleading. The PRISM program involves the collection of Americans' communications, both international and domestic, and for reasons explained below, the program is unconstitutional.


15 While news reports have generally described PRISM as an NSA "program," the publicly available documents leave open the possibility that PRISM is instead the name of the NSA database in which content collected from these providers is stored.

a. Section 702 is unconstitutional

President Bush signed the FISA Amendments Act into law on July 10, 2008. While leaving FISA in place for purely domestic communications, the FISA Amendments Act revolutionized the FISA regime by permitting the mass acquisition, without individualized judicial oversight or supervision, of Americans’ international communications. Under the FISA Amendments Act, the Attorney General and Director of National Intelligence ("DNI") can “authorize jointly, for a period of up to 1 year . . . the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.” 50 U.S.C. § 1881a(a). The government is prohibited from "intentionally target[ing] any person known at the time of the acquisition to be located in the United States," id. § 1881a(b)(1), but an acquisition authorized under the FISA Amendments Act may nonetheless sweep up the international communications of U.S. citizens and residents.

Before authorizing surveillance under Section 702—or, in some circumstances, within seven days of authorizing such surveillance—the Attorney General and the DNI must submit to the FISA Court an application for an order (hereinafter, a “mass acquisition order”). Id. § 1881a(a), (c)(2). A mass acquisition order is a kind of blank check, which once obtained permits—without further judicial authorization—whatever surveillance the government may choose to engage in, within broadly drawn parameters, for a period of up to one year.

To obtain a mass acquisition order, the Attorney General and DNI must provide to the FISA Court “a written certification and any supporting affidavit” attesting that the FISA Court has approved, or that the government has submitted to the FISA Court for approval, “targeting procedures” reasonably designed to ensure that the acquisition 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.” Id. § 1881a(g2)(A)(i).

The certification and supporting affidavit must also attest that the FISA Court has approved, or that the government has submitted to the FISA Court for approval, “minimization procedures” that meet the requirements of 50 U.S.C. § 1801(b) or § 1821(4).

Finally, the certification and supporting affidavit must attest that the Attorney General has adopted “guidelines” to ensure compliance with the limitations set out in § 1881a(b), that the targeting procedures, minimization procedures, and guidelines are consistent with the Fourth Amendment; and that “a significant purpose of the acquisition is to obtain foreign intelligence information.” Id. § 1881a(g)(3)(vii).

Importantly, Section 702 does not require the government to demonstrate to the FISA Court that its surveillance targets are foreign agents, engaged in criminal activity, or connected even remotely with terrorism. Indeed, the statute does not require the government to identify its surveillance targets at all. Moreover, the statute expressly provides that the government’s certification is not required to identify the facilities, telephone lines, email addresses, places, premises, or property at which its surveillance will be directed. Id. § 1881a(g)(4).

Nor does Section 702 place meaningful limits on the government’s retention, analysis, and dissemination of information that relates to U.S. citizens and residents. The Act requires the government to adopt “minimization procedures,” id. § 1881a, that are “reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unsuspecting United States persons.” Id. §§ 1801(b)(1), 1821(4)(A). The Act does not, however, prescribe specific minimization procedures. Moreover, the FISA Amendments Act specifically allows the government to retain and disseminate information—including information relating to U.S. citizens and residents—if the government concludes that it is “foreign intelligence information.” Id. § 1881a(e) (referring to id. §§ 1801(b)(1), 1821(4)(A)). The phrase “foreign intelligence information” is defined broadly to include, among other things, all information concerning terrorism, national security, and foreign affairs. Id. § 1801(e).

As the FISA Court has itself acknowledged, its role in authorizing and supervising surveillance under the FISA Amendments Act is “narrowly circumscribed.” The judiciary’s traditional role under the Fourth Amendment is to serve as a gatekeeper for particular acts of surveillance, but its role under the FISA Amendments Act is to issue advisory opinions blessing in advance broad parameters and targeting procedures, under which the government is then free to conduct surveillance for up to one year. Under Section 702, the FISA Court does not consider individualized and particularized surveillance applications, does not make individualized probable cause determinations, and does not closely supervise the implementation of the government’s targeting or minimization procedures. In short, the role that the FISA Court plays under the FISA Amendments Act bears no resemblance to the role that it has traditionally played under FISA.

---


The ACLU has long expressed deep concerns about the lawfulness of the FISA Amendments Act and surveillance under Section 702. The statute’s defects include:

- Section 702 allows the government to collect Americans’ international communications without requiring it to specify the people, facilities, places, premises, or property to be monitored.

Until Congress enacted the FISA Amendments Act, FISA generally prohibited the government from conducting electronic surveillance without first obtaining an individualized and particularized order from the FISA court. In order to obtain a court order, the government was required to show that there was probable cause to believe that its surveillance target was an agent of a foreign government or terrorist group. It was also generally required to identify the facilities to be monitored. The FISA Amendments Act allows the government to conduct electronic surveillance without indicating to the FISA Court whom it intends to target or which facilities it intends to monitor, and without making any showing to the court—or even making an internal executive determination—that the target is a foreign agent or engaged in terrorism. The target could be a human rights activist, a media organization, a geographic region, or even a country. The government must assure the FISA Court that the targets are non-U.S. persons overseas, but in allowing the executive to target such persons overseas, Section 702 allows it to monitor communications between those targets and U.S. persons inside the United States. Moreover, because the FISA Amendments Act does not require the government to identify the specific targets and facilities to be surveilled, it permits the acquisition of these communications en masse. A single acquisition order may be used to justify the surveillance of communications implicating thousands or even millions of U.S. citizens and residents.

- Section 702 allows the government to conduct intrusive surveillance without meaningful judicial oversight.

Under Section 702, the government is authorized to conduct intrusive surveillance without meaningful judicial oversight. The FISA Court does not review individualized surveillance applications. It does not consider whether the government’s surveillance is directed at agents of foreign powers or terrorist groups. It does not have the right to ask the government why it is initiating any particular surveillance program. The FISA Court’s role is limited to reviewing the government’s “targeting” and “minimization” procedures. And even with respect to the procedures, the FISA court’s role is to review the procedures at the outset of any new surveillance program; it does not have the authority to supervise the implementation of those procedures over time.

- Section 702 places no meaningful limits on the government’s retention and dissemination of information relating to U.S. citizens and residents.

As a result of the FISA Amendments Act, thousands or even millions of U.S. citizens and residents will find their international telephone and email communications swept up in surveillance that is “targeted” at people abroad. Yet the law fails to place any meaningful limitations on the government’s retention and dissemination of information that relates to U.S. persons. The law requires the government to adopt “minimization” procedures—procedures that are “reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons.” However, these minimization procedures must accommodate the government’s need “to obtain, produce, and disseminate foreign intelligence information.” In other words, the government may retain or disseminate information about U.S. citizens and residents so long as the information is “foreign intelligence information.” Because “foreign intelligence information” is defined broadly (as discussed below), this is an exception that swallows the rule.

- Section 702 does not limit government surveillance to communications relating to terrorism.

The Act allows the government to conduct dragnet surveillance if a significant purpose of the surveillance is to gather “foreign intelligence information.” There are multiple problems with this. First, under the new law the “foreign intelligence” requirement applies to entire surveillance programs, not to individual intercepts. The result is that if a significant purpose of any particular government dragnet is to gather foreign intelligence information, the government can use that dragnet to collect all kinds of communications—not only those that relate to foreign intelligence. Second, the phrase “foreign intelligence information” has always been defined extremely broadly to include not only information about terrorism but also information about intelligence activities, the national defense, and even the “foreign affairs of the United States.” Journalists, human rights researchers, academics, and attorneys routinely exchange information by telephone and email that relates to the foreign affairs of the U.S.

b. The NSA’s “targeting” and “minimization” procedures do not mitigate the statute’s constitutional deficiencies

Since the FISA Amendments Act was enacted in 2008, the government’s principal defense of the law has been that “targeting” and “minimization” procedures supply sufficient protection for Americans’ privacy. Because the procedures were secret, the government’s assertion was impossible to evaluate. Now that the procedures have
been published, however,\textsuperscript{20} it is plain that the assertion is false. Indeed, the procedures confirm what critics have long suspected—that the NSA is engaged in unconstitutional surveillance of Americans' communications, including their telephone calls and emails. The documents show that the NSA is conducting sweeping surveillance of Americans' international communications, that it is acquiring many purely domestic communications as well, and that the rules that supposedly protect Americans' privacy are weak and riddled with exceptions.

- The NSA's procedures permit it to monitor Americans' international communications in the course of surveillance targeted at foreigners abroad.

While the FISA Amendments Act authorizes the government to target foreigners abroad, not Americans, it permits the government to collect Americans' communications with those foreign targets. The recently disclosed procedures contemplate not only that the NSA will acquire Americans' international communications but that it will retain them and possibly disseminate them to other U.S. government agencies and foreign governments. Americans' communications that contain "foreign intelligence information" or evidence of a crime can be retained forever, and even communications that don't can be retained for as long as five years. Despite government officials' claims to the contrary, the NSA is building a growing database of Americans' international telephone calls and emails.

- The NSA's procedures allow the surveillance of Americans by failing to ensure that its surveillance targets are in fact foreigners outside the United States.

The FISA Amendments Act is predicated on the theory that foreigners abroad have no right to privacy—or, at any rate, no right that the United States should respect. Because they have no right to privacy, the NSA sees no bar to the collection of their communications, including their communications with Americans. But even if one accepts this premise, the NSA's procedures fail to ensure that its surveillance targets are in fact foreigners outside the United States. This is because the procedures permit the NSA to assume that prospective surveillance targets are foreigners outside the United States absent specific information to the contrary—and to presume therefore that they are fair game for warrantless surveillance.

- The NSA's procedures permit the government to conduct surveillance that has no real connection to the government's foreign intelligence interests.

One of the fundamental problems with Section 702 is that it permits the government to conduct surveillance without probable cause or individualized suspicion. It permits the government to monitor people who are not even thought to be doing anything wrong, and to do so without particularized warrants or meaningful review by impartial judges. Government officials have placed heavy emphasis on the fact that the FISA Amendments Act allows the government to conduct surveillance only if one of its purposes is to gather "foreign intelligence information." As noted above, however, that term is defined very broadly to include not only information about terrorism but also information about intelligence activities, the national defense, and even "the foreign affairs of the United States." The NSA's procedures weaken the limitation further. Among the things the NSA examines to determine whether a particular email address or phone number will be used to exchange foreign intelligence information is whether it has been used in the past to communicate with foreigners. Another is whether it is listed in a foreigner's address book. In other words, the NSA appears to equate a propensity to communicate with foreigners with a propensity to communicate foreign intelligence information. The effect is to bring virtually every international communication within the reach of the NSA's surveillance.

- The NSA's procedures permit the NSA to collect international communications, including Americans' international communications, in bulk.

On its face, Section 702 permits the NSA to conduct dragnet surveillance, not just surveillance of specific individuals. Officials who advocated for the FISA Amendments Act made clear that this was one of its principal purposes, and unsurprisingly, the procedures give effect to that design. While they require the government to identify a "target" outside the country, once the target has been identified the procedures permit the NSA to sweep up the communications of any foreigner who may be communicating "about" the target. The Procedures contemplate that the NSA will do this by "employ[ing] an Internet Protocol Filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas," by "target[ing] Internet links that terminate in a foreign country," or by identifying "the country code of the telephone number." However the NSA does it, the result is the same: millions of communications may be swept up, Americans' international communications among them.

- The NSA's procedures allow the NSA to retain even purely domestic communications.

Given the permissive standards the NSA uses to determine whether prospective surveillance targets are foreigners abroad, errors are inevitable. Some of the communications the NSA collects under the Act, then, will be purely domestic.\textsuperscript{21} The Act should require the NSA to purge these communications from its databases, but it does not. The procedures allow the government to keep and analyze even purely domestic communications if they contain significant foreign intelligence information, evidence of a crime, or encrypted information. Again, foreign intelligence information is defined exceedingly broadly.


\textsuperscript{21} Notably, a 2009 New York Times article discusses an episode in which the NSA used the Act to engage in "significant and systemic" overcollection of such domestic communications. Eric Lichtblau & James Risen, Officials Say U.S. Wiretaps Exceeded Law, N.Y. Times, April 15, 2009, http://nyti.ms/16Af7vO.
• The NSA’s procedures allow the government to collect and retain communications protected by the attorney-client privilege.

The procedures expressly contemplate that the NSA will collect attorney-client communications. In general, these communications receive no special protection—they can be acquired, retained, and disseminated like any other. Thus, if the NSA acquires the communications of lawyers representing individuals who have been charged before the military commissions at Guantanamo, nothing in the procedures would seem to prohibit the NSA from sharing the communications with military prosecutors. The procedures include a more restrictive rule for communications between attorneys and their clients who have been constitutionally indicted in the United States—the NSA may not share these communications with prosecutors. Even those communications, however, may be retained to the extent that they include foreign intelligence information.

c. Congress should amend Section 702 to prohibit suspicionless, dragnet collection of Americans’ communications

For the reasons discussed above, the ACLU believes that the FISA Amendments Act is unconstitutional on its face. There are many ways, however, that Congress could provide meaningful protection for privacy while preserving the statute’s broad outline. One bill introduced by Senator Wyden during the reauthorization debate last fall would have prohibited the government from searching through information collected under the FISA Amendments Act for the communications of specific, known U.S. persons. Bills submitted during the debate leading up to the passage of the FISA Amendments Act in 2008 would have banned dragnet collection in the first instance or required the government to return to the FISC before searching communications obtained through the FISA Amendments Act for information about U.S. persons. Congress should examine these proposals again and make amendments to the Act that would provide greater protection for individual privacy and mitigate the chilling effect on rights protected by the First Amendment.

III. Excessive secrecy surrounds the government’s use of FISA authorities

Amendments to FISA since 2001 have substantially expanded the government’s surveillance authorities, but the public lacks crucial information about the way these authorities have been implemented. Rank-and-file members of Congress and the public have learned more about domestic surveillance in the last two months than in the last several decades combined. While the Judiciary and Intelligence Committees have received some information in classified format, only members of the Senate Select Committee on Intelligence, party leadership, and a handful of Judiciary Committee members have staff with clearance high enough to access the information and advise their principals. Although the Inspectors General and others file regular reports with the Committees of jurisdiction, these reports do not include even basic information such as how many Americans’ communications are swept up in these programs, or how and when Americans’ information is accessed and used.

Nor does the public have access to the FISC decisions that assess the meaning, scope, and constitutionality of the surveillance laws. Aggregate statistics alone would not allow the public to understand the reach of the government’s surveillance powers, as we have seen with Section 215, one application may encompass millions of individual records. Public access to the FISA Court’s substantive legal reasoning is essential. Without it, some of the government’s most far-reaching policies will lack democratic legitimacy. Instead, the public will be dependent on the discretionary disclosures of executive branch officials—disclosures that have sometimes been self-serving and misleading in the past.24 Needless to say, it may be impossible to release FISC opinions without redacting passages concerning the NSA’s sources and methods. The release of redacted opinions, however, would be far better than the release of nothing at all.

Congress should require the release of FISC opinions concerning the scope, meaning, or constitutionality of FISA, including opinions relating to Section 215 and Section 702. Administration officials have said there are over a dozen such opinions, some close to one hundred pages long.25 Executive officials testified before Congress several years ago that declassification review was already underway,26 and President Obama directed the DNI to revisit that process in the last few weeks. If the administration refuses to release these opinions, Congress should consider legislation compelling their release.

Congress should also require the release of information about the type and volume of information that is obtained under dragnet surveillance programs. The leaked Verizon order confirms that the government is using Section 215 to collect telephony metadata about every phone call made by Verizon subscribers in the United States. That the government is using Section 215 for this purpose raises the question of what other "tangible things" the government may be collecting through similar dragnets. For reasons discussed above, the ACLU believes that these dragnets are unauthorized by the statute as well as unconstitutional. Whatever their legality, however, the public has a right to know, at least in general terms, what kinds of information the government is collecting about innocent Americans, and on what scale.

IV. National Security Letters

The ACLU has a number of serious concerns with the national security letter (NSL) statutes. In this testimony, we focus on only two. The first is that the NSL statutes allow executive agencies (usually the FBI) to obtain records about people who are not known or even suspected to have done anything wrong. They allow the

government to collect information, sometimes very sensitive information, not just about suspected terrorists and spies but about innocent people as well. The second concern is that the NSL statutes allow government agencies (again, usually the FBI) to prohibit NSL recipients from disclosing that the government sought or obtained information from them. This authority to impose non-disclosure orders—gag orders—is not subject to meaningful judicial review. Indeed, as discussed below, the review contemplated by the NSL statutes is no more than cosmetic.\(^{25}\)

a. The NSL statutes invest the FBI with broad authority to collect constitutionally protected information pertaining to innocent people

Several different statutes give executive agencies the power to issue NSLS.\(^{26}\) Most NSLs, however, are issued by the FBI under 18 U.S.C. § 2709(b), which was originally enacted in 1986 as part of the Electronic Communications Privacy Act ("ECPA").\(^{27}\) Since its enactment, the ECPA NSL statute has been amended several times. In its current incarnation, it authorizes the FBI to issue NSLS compelling "electronic communication service provider[s] to disclose "subscriber information," "toll billing records information," and "electronic communication transactional records."\(^{28}\) An "electronic communication service" is "any service which provides to users thereof the ability to send or receive wire or electronic communications."\(^{29}\)

Because most NSLS are issued under ECPA, this testimony focuses on that statute. All of the NSL statutes, however, suffer from similar flaws.

The ECPA NSL statute implicates a broad array of information, some of it extremely sensitive. Under the statute, an Internet service provider can be compelled to disclose a subscriber's name, address, telephone number, account name, e-mail address, and credit card and billing information. It can be compelled to disclose the identities of individuals who have visited a particular website, a list of websites visited by a particular individual, a list of e-mail addresses with which a particular individual has corresponded, or the e-mail address and identity of a person who has posted anonymous speech on a political website. As the Library Connection case shows, the ECPA NSL statute can also be used to compel the disclosure of library patron records.\(^{31}\) Clearly, all of this information is sensitive. Some of it is protected by the First Amendment.\(^{32}\)

Because NSLS can reach information that is sensitive, Congress originally imposed stringent restrictions on their use. As enacted in 1986, the ECPA NSL statute permitted the FBI to issue an NSL only if it could certify that (i) the information sought was relevant to an authorized foreign counterintelligence investigation; and (ii) there were specific and articulable facts giving reason to believe that the subject of the NSL was a foreign power or foreign agent.\(^{33}\) Since 1986, however, the reach of the law has been extended dramatically. In 1999, Congress relaxed the individualized suspicion requirement, authorizing the FBI to issue an NSL if it could certify that (i)...

\(^{25}\) The ACLU has a number of other concerns with the NSL statutes. First, the statutes do not significantly limit the retention and dissemination of NSL-derived information. See, e.g., 18 U.S.C. § 2709(b) (delegating to the Attorney General the task of determining when, and for what purposes, NSL-derived information can be disseminated). Second, the statute provides that courts that hear challenges to gag orders must review the government's submissions ex parte and in camera "upon request of the government"; this language could be construed to foreclose independent consideration by the court of the constitutional ramifications of denying the NSL recipient access to the evidence that is said to support a gag order. 18 U.S.C. § 3511(e). But see Doe v. Gonzales, 500 F. Supp. 2d 423-24 (S.D.N.Y. 2007) (construing statute more narrowly). Third, the statute provides that courts that hear challenges to gag orders must seal documents and close hearings "to the extent necessary to prevent an unauthorized disclosure of a request for records"; this language could be construed to divest the courts of their constitutional responsibility to decide whether documents should be sealed or hearings should be closed. 18 U.S.C. § 3511(d). But see Doe, 500 F. Supp. 2d at 423-24 (finding that statute "in no way displaces the role of the court in determining, in each instance, the extent to which documents need to be sealed or proceedings closed and does not permit the scope of such a decision to be made unilaterally by the government").

\(^{26}\) For instance, under 12 U.S.C. § 3414(a)(5)(A), the FBI is authorized to compel "financial institutions" to disclose customer financial records. The phrase "financial institutions" is defined very broadly, and encompasses banks, credit unions, thrift institutions, investment banks, pawnbrokers, travel agencies, real estate companies, and casinos. 12 U.S.C. § 3414(d) (adopting definitions in 31 U.S.C. § 5312). Under 15 U.S.C. § 1681u, the FBI is authorized to compel consumer reporting agencies to disclose "the names and addresses of all financial institutions... at which a consumer maintains or has maintained an account," as well as "identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment." Under 15 U.S.C. § 1681v, executive agencies authorized to conduct intelligence or counterintelligence investigations can compel consumer reporting agencies to disclose "a consumer report of a consumer and all other information in a consumer's file." Still another statute, 30 U.S.C. § 436 empowers "any authorized investigative agency" to compel financial institutions and consumer reporting agencies to disclose records about agency employees.


\(^{29}\) Id. at 2510 (15).


\(^{31}\) Cf. McIntyre v. Ohio Elections Comm., 514 U.S. 334, 341-42 (1995) ("[A]n author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment."). Talley v. California, 362 U.S. 60, 64 (1960) ("Even the Federalist Papers, written in favor of the adoption of our Constitution, were published under fictitious names.").

the information sought was relevant to an authorized foreign counterintelligence investigation; and (ii) there were specific and articulable facts giving reason to believe that either (a) the subject of the NSL was a foreign power or foreign agent, or (b) the subject had communicated with a person engaged in international terrorism or with a foreign agent or power "under circumstances giving reason to believe that the communication concerned international terrorism." By 2001, Congress removed the individualized suspicion requirement altogether and also extended the FBI's authority to issue NSLs in terrorism investigations. In its current form, the NSL statute permits the FBI to issue NSLs upon a certification that the records sought are "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities."

The放松和随后的撤销使得NSL的个体化怀疑要求的变化在每一年的NSL数量中都得到了指数级的增长。根据审计局对司法部的审计，从2001年开始， FBI已经发出5,800个NSL请求，但是，这些数字，尽管有所增长，却未显示NSL的使用量有实质性的增加。OIG调查了77个FBI的案例文件和另外22个NSL的原始记录发现，在这些案件中， FBI的怀疑要求并未得到满足。自2007年以来，OIG已经发现，FBI对NSL的使用范围已经扩大到了非美国公民和NSL用户，而不仅仅是美国公民。然而，尽管NSL的使用范围得到了扩大，但是，NSI的审计报告却显示，美国公民的NSL使用量却不增反降。

The statistics and other public information make clear that the executive branch is now using NSLs not only to investigate people who are known or suspected to present threats but also—indeed principally—to collect information about innocent people.40 Views reports indicate that the FBI has used NSLs "to obtain data not only on individuals it saw as targets but also on details of their 'community of interest'—the network of people that the target was in contact with.41 Some of the FBI's investigations appear to be nothing more than fishing expeditions. In two cases brought by the ACLU, the FBI has abdicated its demand for information after the NSL recipient filed suit; that is, the FBI withdrew the NSL rather than try to defend the NSL to a judge.42 The agency's willingness to abandon NSLs that are challenged in court raises obvious questions about the agency's need for the information in the first place.

The ACLU believes that the current NSL statutes do not appropriately safeguard the privacy of innocent people. Congress should narrow the NSL authorities that allow the FBI to demand information about individuals who are not the targets of any investigation.

b. The NSL statutes allow the FBI to impose gag orders without meaningful judicial review

A second problem with the NSL statutes is that they empower executive agencies to impose gag orders that are not subject to meaningful judicial review.43 Until 2006, the ECPA NSL statute categorically prohibited NSL recipients from disclosing to anyone that the FBI had sought or obtained information from them.44 Congress amended the statute, however, after a federal district court found it unconstitutional.45 Unfortunately, the amendments made in 2006, while addressing some problems with the statute, made the gag provisions even more oppressive. The new statute permits the FBI to decide on a case-by-case basis whether to impose gag orders on NSL recipients but strictly confines the ability of NSL recipients to challenge such orders in court.

As amended, the NSL statute authorizes the Director of the FBI or his designee (including a Special Agent in Charge of a Bureau field office) to impose a gag order on

40 The statistics also make clear that the FBI is increasingly using NSLs to seek information about U.S. persons. The percentage of NSL requests generated from investigations of U.S. persons increased from approximately 39 percent of NSL requests in 2003 to approximately 57 percent in 2008. 2008 OIG Report at 9.
41 Eric Lichtblau, F.B.I. Data Mining Reached Beyond Initial Targets, N.Y. Times, Sept. 9, 2007; see also Barton Gellman, The F.B.I.'s Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans, Wash. Post, Nov. 6, 2005 (reporting that the FBI apparently used NSLs to collect information about "close to a million" people who had visited Las Vegas).
43 All of the NSL statutes authorize the imposition of such gag orders.
any person or entity served with an NSL. To impose such an order, the Director of the FBI or his designee must "certify" that, absent the non-disclosure obligation, "there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person." If the Director of the FBI or his designee so certifies, the recipient of the NSL is prohibited from disclosing any information to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that the FBI has sought or obtained access to information or records under the NSL statute. Gag orders imposed under the NSL statute are imposed by the FBI unilaterally, without prior judicial review. While the statute requires a "certification" that the gag is necessary, the certification is not examined by anyone outside the executive branch. No judge considers, before the gag order is imposed, whether secrecy is necessary or whether the gag order is narrowly tailored.

The gag provisions permit the recipient of an NSL to petition a court "for an order modifying or setting aside a nondisclosure requirement." However, in the case of a petition filed "within one year of the request for records," the reviewing court may modify or set aside the nondisclosure requirement only if it finds that "there is no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person." Moreover, if a designated senior government official "certifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations," the certification must be "treated as conclusive unless the court finds that the certification was made in bad faith."

In December 2008, the Second Circuit issued a decision construing the NSL statute to permit a nondisclosure requirement only when senior FBI officials certify that disclosure may result in an enumerated harm that is related to "an authorized investigation to protect against international terrorism or clandestine intelligence activities"; (2) to place on the government the burden of showing that a good reason exists to expect that disclosure of receipt of an NSL will risk an enumerated harm; and (3) to require the government, in attempting to satisfy that burden, to adequately demonstrate that disclosure in a particular case may result in an enumerated harm. The court also invalidated the subsection of the NSL statute that directs the courts to treat as conclusive executive officials' certifications that disclosure of information may endanger the national security of the United States or interfere with diplomatic relations.

In addition, the Second Circuit ruled that the NSL statute is unconstitutional to the extent that it imposes a non-disclosure requirement on NSL recipients without placing on the government the burden of initiating judicial review of that requirement. The court held that this deficiency, however, could be addressed by the adoption of a "reciprocal notice" policy. Under this policy, the FBI must inform NSL recipients of their right to challenge gag orders. If a recipient indicates its intent to do so, the FBI must initiate court proceedings to establish—before a judge—that the gag order is necessary and consistent with the First Amendment.

Consistent with these judicial rulings, the ACLU supports congressional efforts to ensure that "gag orders" associated with national security letters and other surveillance directives are limited in scope, limited in duration, and imposed only when necessary.

V. Summary of recommendations

For the reasons above, Congress should amend relevant provisions of FISA to prohibit surveillance, "dragnet" monitoring or tracking of Americans' communications. Amendments of this kind should be made to the FISA Amendments Act, to FISA's so-called "business records" provision, and to the national security letter authorities.

Congress should also end the unnecessary and corrosive secrecy that has obstructed congressional and public oversight. It should require the publication of FISC opinions insofar as they evaluate the meaning, scope, or constitutionality of the foreign-intelligence laws. It should require the government to publish basic statistical information

---

46 18 U.S.C. § 2709(c).
47 Id. § 2709(c)(1).
48 Id.
49 Id. § 3511(h)(1).
50 Id. § 3511(h)(2).
51 Id. In the case of a petition filed under § 3511(h)(1) "one year or more after the request for records," the FBI Director or his designee must either terminate the non-disclosure obligation within 90 days or recertify that disclosure may result in one of the enumerated harms. Id. § 3511(b)(3). If the FBI recertifies that disclosure may be harmful, however, the reviewing court is required to apply the same extraordinarily deferential standard it is required to apply to petitions filed within one year. Id. If the recertification is made by a designated senior official, the certification must be "treated as conclusive unless the court finds that the recertification was made in bad faith." Id.
52 Doe v. Mukasey, 549 F.3d 861, 883 (2d. Cir. 2008).
53 Id.
54 Id.
55 Id. see id.
56 A district court in the Northern District of California recently issued a similar decision, finding that the nondisclosure provision of 18 U.S.C. § 2709(c) violates the First Amendment and that 18 U.S.C. § 3511(h)(2) and (b)(3) violate the First Amendment and separation of powers principles. In re Natl. Sec. Ltr., No. C 10-02175 SL, 2013 WL 1095417 (N.D. Cal. Mar. 14, 2013). The court enjoined the government from issuing NSLs under section 2709 or from enforcing the nondisclosure provision in that or any other case. Id.
about the government's use of foreign-intelligence authorities. And it should ensure that "gag orders" associated with national security letters and other surveillance directives are limited in scope and duration, and imposed only when necessary.

Finally, Congress should ensure that the government's surveillance activities are subject to meaningful judicial review. It should clarify by statute the circumstances in which individuals can challenge government surveillance in ordinary federal courts. It should provide for open and adversarial proceedings in the FISC when the government's surveillance applications raise novel issues of statutory or constitutional interpretation. It should also pass legislation to ensure that the state secrets privilege is not used to place the government's surveillance activities beyond the reach of the courts.