SWORD OR SHIELD? THE GOVERNMENT'S SELECTIVE USE OF ITS DECLASSIFICATION AUTHORITY FOR TACTICAL ADVANTAGE IN CRIMINAL PROSECUTIONS

*Joshua L. Dratel**

INTRODUCTION

One of the principles underlying the Classified Information Procedures Act ("CIPA"),[1] which regulates the use of classified information in the context of federal criminal prosecutions, is that the classified status of any item of evidence or information shall not, by itself, deprive a defendant of access to that evidence or information, or, in turn, a fair trial. Notwithstanding this fundamental tenet, which is articulated in CIPA's legislative history and interpretive case law, the government's exclusive control over critical aspects of litigation and proceedings conducted pursuant to CIPA often undermines the statute's legislative intent. The government achieves this control by determining whether and what classified material to *de*classify in preparation for a criminal prosecution and trial, including a defendant's own communications intercepted pursuant to the Foreign Intelligence Surveillance Act ("FISA").[2]

The government may selectively declassify inculpatory evidence for use at trial, while, at the same time, deny the defense the ability to adequately prepare for a case by not declassifying exculpatory information. As a result, an essential objective of CIPA—that the existence of classified material in a criminal case not impair a defendant's Fifth and Sixth Amendment rights—is thwarted at the unilateral discretion of the government. The solution is to reform the procedures under which classified information is used in the context of criminal trials so that defendants, in preparing for trial, are not deprived of access to their own statements and communications.

---

* Joshua L. Dratel is a criminal defense lawyer in New York City. He is the former President of the New York State Association of Criminal Defense Lawyers and has been a defense attorney in many cases alleging terrorism offenses and involving classified information and national security issues, including *United States v. Usama Bin Laden*, which is discussed in this article.

1 18 U.S.C. app. III (2000).

2 50 U.S.C. §§ 1800-1811 (2000).

This solution will require not only amending CIPA but also harmonizing it with FISA, under which a defendant's electronic communications are most often intercepted, usually in a classified manner. In order to understand the need for CIPA reform and to appreciate fully the asymmetrical access to evidence that the government's declassification authority creates, first CIPA's purposes and applications must be reviewed. It is then important to evaluate the impermeability of the government's classification authority in the CIPA context, before proceeding to review the specific cases in which the government has exploited its declassification discretion in comparison to cases in which the government has not sought such advantage. This article will demonstrate that the aforementioned analysis can lead to only one conclusion: statutory reform is necessary in order to preserve CIPA and its objectives, and to put the government and the defense on equal footing regardless of whether information and evidence are classified.

I. CIPA's History and Purposes

CIPA was enacted "to 'minimize the problem of so-called greymail—a threat by the defendant to disclose classified information in the course of trial—by requiring a ruling on the admissibility of the classified information before trial.'"[3] In furtherance of that objective, CIPA provides procedures for informing the government of the classified information, prior to trial, which will be compromised by the prosecution.[4]

The prosecution of Lewis I. "Scooter" Libby presents the paradigmatic situation that the CIPA was designed to address. The defendant was fully aware of the nature and content of the classified information at issue. Indeed, the defendant was charged with lying about his disclosure of that very information.[5] As part of his defense, Mr. Libby sought access to certain classified information in the government's possession

---

3 United States v. Pappas, 94 F.3d 795, 799 (2d Cir. 1996) (quoting S. Rep. No. 96-823, at 2 (1980), *as reprinted in* 1980 U.S.C.C.A.N. 4294, 4295) (citing United States v. Wilson, 721 F.2d 967, 975 (4th Cir. 1983)); *see generally,* United States v. Libby, 429 F. Supp. 2d 18 (D.D.C. 2006) ("*Libby I*").

4 *See* United States v. Collins, 720 F. 2d 1195, 1197 (11th Cir. 1983); United States v. Abu Marzook, 412 F. Supp. 2d 913, 917-18 (N.D. Ill. 2006).

5 *See* United States v. Libby, 429 F. Supp. 2d 1, 13 (D.D.C. 2006) ("*Libby II*") (prosecutor arguing that defendant's discovery requests for classified materials constituted "a transparent effort at 'greymail'").

and indicated his intention to use that information, as well as other classified information already in his possession.

However, terrorism cases present very different situations and *very* different defendants than those for which CIPA (as a reaction to greymail) was designed. In terrorism cases, the defendant is *not* in possession of the classified information (unlike government officials charged with espionage offenses or other misconduct), and there is no chance that they will obtain the necessary security clearance to view classified materials. Thus, the greymail opportunities are minimized, if not eliminated altogether, since the defendant is not in a position to threaten disclosure of classified information other than that provided by the government in discovery.

CIPA was not intended to supplant ordinary discovery principles. Normal discovery[6] and evidentiary[7] rules apply to CIPA. Ultimately, CIPA is not supposed to put the defendant in a worse position than if the evidence was *not* classified. As the Seventh Circuit noted in *United States v. Dumeisi*, CIPA's fundamental purpose is to "protect and restrict the discovery of classified information in a way that does not impair the defendant's right to a fair trial."[8] Indeed, explicit in CIPA's legislative history is the admonition that "the defendant should not stand in a worse position, because of the fact that classified information is involved, than he would without this Act."[9]

Consequently, as the Fourth Circuit pointed out in *United States v. Fernandez*,[10] "[a]lthough CIPA contemplates that the use of classified information be streamlined, courts must not be remiss in protecting a

---

6 *Id.* at 7 ("[CIPA] creates no new rights or limits on discovery of a specific area of classified information . . . [,] it contemplates an application of the general law of discovery in criminal cases to the classified information based on the sensitive nature of the classified information.") *Id.* (quoting United States v. Yunis, 867 F.2d 617, 621 (D.C. Cir. 1989)).

7 *See, e.g.,* United States v. Baptista Rodriguez, 17 F.3d 1354, 1363-1364 (11th Cir. 1994); United States v. Smith, 750 F.2d 1215, 1217 (4th Cir. 1984), *rev'd on other grounds*, 780 F.2d 1102 (4th Cir. 1985) (en banc); *Yunis*, 867 F.2d at 621-22.

8 424 F.3d 566, 578 (7th Cir. 2005) (quoting United States v. O'Hara, 301 F.3d 563, 569 (7th Cir. 2002)); *see generally,* United States v. Moussouai, 365 F.3d 292 (4th Cir. 2004), *reh'g granted*, 382 F.3d 453 (4th Cir. 2004); United States v. Cardoen, 898 F. Supp. 1563, 1571 (S.D. Fla. 1995); United States v. Anderson, 872 F.2d 1508, 1519 (11th Cir. 1989); *Abu Marzook*, 412 F. Supp. 2d at 918; United States v. Paracha, No. 03 CR. 1197(SHS), 2006 WL 12768, at *10 (S.D.N.Y. Jan. 3, 2006); United States v. North, 698 F. Supp. 316, 320 (D.D.C. 1988).

9 S. REP. NO. 96-823, at 9 (1980), *as reprinted in* 1980 U.S.C.C.A.N. 4302; *see also North*, 698 F. Supp. at 320.

10 913 F.2d 148, 154 (4th Cir. 1990).

defendant's right to a full and meaningful presentation of his claim to innocence." Consistent with that mandate, CIPA also does not diminish the government's obligation to provide exculpatory material to the defendant in compliance with *Brady v. Maryland*.[11]

Similarly, within the context of CIPA and classified information, a defendant retains Fifth and Sixth Amendment rights to a fair trial and to compulsory process.[12] More recently, courts have consistently held that CIPA should not operate as an impediment to a defendant's right to discoverable or exculpatory information, or more broadly, to a fair trial consistent with Fifth and Sixth Amendment standards.[13]

II. The Asymmetrical Nature of the Government's Declassification Authority

The executive branch controls the scope of disclosure to a defendant through its power to decide what information is classified and what information will be declassified for purposes of the case. Consequently, this governmental power amplifies and adds to the general inequity created by CIPA in cases in which the defendant lacks knowledge of the classified information.

Regarding classification, it is widely recognized that "the Federal Government exhibits a proclivity for over-classification of information."[14] Yet, under CIPA, the defense "cannot challenge this classifica-

---

11 373 U.S. 83 (1963); *see* United States v. Moussaoui, No. CR. 01-455-A, 2003 WL 21263699, at *4 (E.D. Va. Mar. 10, 2003) ("*Moussaoui I*") (holding that *Brady* principles apply in the CIPA context, including information negating guilt as well as that affecting a potential sentence).

12 *See Moussaoui I*, 2003 WL 21263699, at *4-6; *see also* United States v. Moussaoui, 2003 WL 22258213, at *2 (E.D. Va. Aug. 29, 2003); United States v. Moussaoui, 282 F. Supp. 2d 480, 482 (E.D. Va. 2003).

13 CIPA has consistently been declared constitutional in the face of Fifth and Sixth Amendment challenges. *See, e.g.,* United States v. bin Laden, No. S(7) 98 CR. 1023 (LBS), 2001 WL 66393, at *9 (S.D.N.Y. Jan. 25, 2001); United States v. Wilson, 750 F.2d 7, 9-10 (2d Cir. 1984), *cert. denied,* 479 U.S. 839 (1986); United States v. Ivy, No. 91-00602-04, 1993 WL 316215, at *7 (E.D. Pa. Aug. 12, 1993).

14 Ray v. Turner, 587 F.2d 1187, 1209 (D.C. Cir. 1987) (Wright, J., concurring) (quoting former Sen. Baker). *See also* United States v. Morison, 844 F.2d 1057, 1081 (4th Cir. 1988) (Wilkinson, J., concurring) ("[t]here exists the tendency, even in a constitutional democracy, for government to withhold reports of disquieting developments and to manage news in a fashion most favorable to itself"); Halperin v. Kissinger, 606 F.2d 1192, 1204 n. 77 (D.C.Cir.1979) (noting "the well-documented practice of classifying as confidential much relatively innocuous or noncritical information"); United States v. Rosen, 445 F. Supp.2d 602, 633 (E.D. Va. 2006); "Security Classification Policy and Procedure: E.O. 12958 as Amended," Congressional Research Service (updated January 7, 2005), at 2.

tion. A court cannot question it."[15] Thus, a defendant lacks recourse for assistance in penetrating the classification and declassification processes.[16] The exclusive remedy is administrative, which is not only time-consuming but also leaves the determination to the executive branch. Any civil lawsuit seeking to reverse an administrative decision would certainly still be pending long after the criminal trial concluded.

Unfettered government discretion is often too great a temptation to exploit, as it permits the government to use its unreviewable classification authority as an offensive weapon, effectively placing voluminous amounts of critical evidence off limits to the defense.[17] For example, a prosecutor can decline to seek declassification of critical evidence such as

---

15 United States v. Aref, No. 04-CR-402, WL 1877142 (N.D.N.Y. July 6, 2006) (quoting *Smith*, 750 F.2d at 1217, *rev'd on other grounds*, 780 F.2d 1102 (4th Cir. 1985) (en banc)) (citing United States v. Musa, 833 F. Supp. 752, 755 (E.D. Mo. 1993); *see also* United States v. Collins, 720 F. 2d 1195, 1198 n.2 (11th Cir. 1983) ("It is an Executive function to classify information, not a judicial one."); *Abu Marzook*, 412 F. Supp. 2d at 921; *cf.* United States v. Moussouai, 65 F. App'x 881, 886 (4th Cir. 2003) (explaining that while the court must defer to the government regarding classification, ultimately the court decides which materials remain sealed).

16 The federal government's penchant for hyper classification is legend and legion. Recently, the General Accounting Office issued a report regarding overclassification at the Department of Defense, including questioning the classification of 26% of the sample of documents reviewed. *See* U.S. GOVERNMENT ACCOUNTABILITY OFFICE, MANAGING SENSITIVE INFORMATION: DOD CAN MORE EFFECTIVELY REDUCE THE RISK OF CLASSIFICATION ERRORS 5, 20 (2006), *available at* http://www.fas.org/sgp/gao/gao-06-706.pdf. Similar results were obtained during a National Archives audit. *See* INFORMATION SECURITY OVERSIGHT OFFICE, AUDIT REPORT: WITHDRAWAL OF RECORDS FROM PUBLIC ACCESS AT THE NATIONAL ARCHIVES AND RECORDS ADMINISTRATION FOR CLASSIFICATION PURPOSES (2006), *available at* http://www.archives.gov/isoo/reports/2006-audit-report.pdf [hereinafter AUDIT REPORT].

17 Given the president's admission that he unilaterally, and in likely violation of the administrative prerequisites for declassification set forth in Executive Order 13,292 (March 25, 2003), declassified the identity of a covert Central Intelligence Agency operative, obviously that unbridled discretion enjoyed by the executive branch is all too tempting in the political arena as well. *See, e.g.,* David E. Sanger & David Johnston, *Bush Ordered Declassification, Official Says*, N.Y. TIMES, April 10, 2006, at A14; Douglas Jehl, *Ex-Intelligence Group Presses for Congressional Inquiry on Disclosure of C.I.A. Officer*, N.Y. TIMES, Jan. 22, 2004, at A21 (describing 10 former intelligence officers who wrote a letter to House of Representatives Speaker J. Dennis Hastert that the disclosure of Valerie Plame Wilson's name as a CIA operative "was an unprecedented and shameful event in American history and, in our professional judgment, has damaged U.S. national security, specifically the effectiveness of U.S. intelligence-gathering using human sources . . ."); Editorial, *Playing Hardball With Secrets*, N.Y. TIMES, Apr. 7, 2006, at A24. ("It's not even clear that Mr. Bush can legally declassify intelligence at whim."); Editorial, *A Bad Leak*, N.Y. TIMES, Apr. 16, 2006, § 4, at 11 ("Mr. Bush did not declassify the National Intelligence Estimate on Iraq—in any accepted sense of that word . . . . He permitted a leak of cherry-picked portions of the report. The declassification came later . . . . Even a president cannot wave a wand and announce that an intelligence report is declassified.").

the intercepts of a defendant's own conversations, facsimile transmissions, or electronic mail, which are made pursuant to electronic surveillance authorized under FISA.[18] As a result, it is more than just a coincidence that the government timely and effortlessly declassifies the FISA-intercepted communications it intends to introduce in evidence. Yet somehow, the government finds itself incapable of performing that task for the remainder of the interceptions, which comprise the overwhelming majority.[19]

However, the intercepts are often voluminous and in a foreign language, such as Arabic or Urdu. In *United States v. Al-Hussayen*,[20] the defendant's telephone conversations and e-mails, captured for a thirteen-month period pursuant to FISA warrants, comprised eighty-nine

---

There is also a current obsession not only with keeping materials classified for an inordinate period of time, but also for *re*classifying previously declassified materials. As reported by *The New York Times*, federal government agencies have removed approximately 55,000 documents, some decades old, from public access at the National Archives. *See* Scott Shane, *Why the Secrecy? Only the Bureaucrats Know*, N.Y. TIMES, Apr. 16, 2006, § 4, at 4. In addition, the subsequent National Archives audit, AUDIT REPORT, *supra* note 16, at 1, concluded that a large portion of documents withdrawn from public access on purported national security grounds did not meet the standard for classification and should not have been removed.

General classification figures also compare rather unfavorably with previous convention: although federal agency decisions to classify information declined nine percent from 2004 to 2005, total classification activity, was more than *sixty* percent higher in 2005 than in 2001. *See* Michelle Chen, *Cheney's Office Declares Exemption from Secrecy Oversight*, THE NEW STANDARD, June 7, 2006, *available at* http://newstandardnews.net/content/index.cfm/items/3261. As Max Weber wrote in *Economy and Society*, "[e]very bureaucracy seeks to increase the superiority of the professionally informed by keeping their knowledge and intentions secret." MAX WEBER, ESSAYS IN SOCIOLOGY 233 (H.H. Gerth & C. Wright Mills trans. & ed., New York: Oxford University Press, 1946). From secrecy a bureaucracy derives power, and "nothing is so fanatically defended." *Id.*

18 Recently, in *Doe v. Gonzales*, Judge Cardamone, remanding in light of new legislation with respect to permanent nondisclosure provisions of 18 U.S.C. § 2709 (regarding National Security Letters), stated that "a ban on speech and a shroud of secrecy in perpetuity are antithetical to democratic concepts and do not fit comfortably within the fundamental rights guaranteed American citizens. Unending secrecy of actions taken by government officials may also serve as a cover for possible official misconduct and/or incompetence." 449 F.3d 415, 422 (2d Cir. 2006) (Cardamone, J., concurring); *see also* Exec. Order No. 13,292 at § 1.7(a) (1), (2) & (4), 68 C.F.R. 15,315, 15,318 (March 23, 2003), *reprinted in* 50 U.S.C. § 435 (2006) ("In no case shall information be classified in order to: (1) conceal violations of law, inefficiency, or administrative error; [or] (2) prevent embarrassment to a person, organization, or agency [or (3)] prevent or delay the release of information that does not require protection in the interest of national security . . ."); *cf. Abu Marzook*, 412 F. Supp. 2d at 921-23 (finding that classification was not designed to avoid embarrassment to Israeli government).

19 *See infra*, note 25.

20 No. CR03-048-C-EJL, 2004 U.S. Dist. LEXIS 29793 (D. Idaho Apr. 6, 2004), *available at* http://ecf.edd.uscourts.gov.

CDs, virtually all in Arabic.[21] The language of the tapes effectively placed the classified materials "off limits" to the defense since it was impossible to engage the services of an Arabic interpreter with the appropriate security clearance willing to relocate to Boise, Idaho, for an indeterminate period of time in order to translate the classified materials. Indeed, as of the time the case proceeded to trial, months after the filing of the initial indictment, the security clearance application of the Arabic interpreter retained by the defense was still pending. The defense was still awaiting clearance at the conclusion of the ten-week trial.

However, on the weekend prior to commencement of the *Al-Hussayen* trial, the government sought to blunt the obvious advantage it had gained by declassifying all of the CDs without any explanation of why that was not done earlier. Obviously, such eleventh-hour declassification was of no value to Mr. Al-Hussayen's defense.

Similarly, in *United States v. Al-Arian*,[22] the government initially refused to declassify approximately 17,000 hours of FISA intercepts of the defendants' own conversations which were predominantly in Arabic. Mr. Al-Arian, however, introduced a novel element into the process. By deciding to appear pro se, he forced the issue: how could he effectively represent himself if he were denied access to the FISA intercepts of his own conversations? Later, the court noted that it could not compel the government to declassify the FISA intercepts, but it could, and would, do *something* to remedy the situation. Days later, all of the FISA intercepts were miraculously declassified.[23]

---

21 *Id.* The documents setting forth the history of the litigation on this issue in *Al-Hussayen* can be found on the District of Idaho's web site via the PACER system. The pertinent documents include numbers 87, 90, 109, 112, 134, 137, 166, 250, 268, 359-362, 379, 433-34, 445, 524-26, 540-43, 572, 578, 584, 589, 595.

22 03 Cr. 77-T-30-TBM (M.D. Fla Feb. 20, 2003).

23 *Id.* A year earlier, Zacarias Moussaoui was denied access to classified materials despite his pro se status. *See* United States v. Moussaoui, 2002 WL 1987964 (E.D. Va. Aug. 23, 2002) (In light of offenses charged, and defendant's prior statements, standby counsel's review of documents was sufficient to protect pro se defendant's Fifth and Sixth Amendment rights adequately. Also, the government was in the process of declassifying many of the documents designated by the defendant for review.); *see also* United States v. Rezaq, 156 F.R.D. 514, 524 (D.D.C. 1994) (denying represented defendant access to classified materials, but providing that "[t]o the extent that defendant himself does need to know the information for his defense, paragraph 10(f) of the protective order permits warranted disclosures. Under paragraph 10(f), defendant's counsel may seek the court's permission to disclose certain evidence to defendant, and the United States may oppose such disclosure.") (footnote omitted), *vacated as moot*, 899 F. Supp. 697 (D.D.C. 1995).

In *United States v. Holy Land Foundation*,[24] two years after the indictment, and only months before the scheduled trial date, the government finally relented to persistent pressure from the defense and declassified the summaries of the FISA intercepts (denominated "tech cuts") for which such summaries were prepared. The FISA intercepts in *Holy Land* were over an eight year time period and the "tech cuts" constituted only ten percent of the total number of intercepts. Thus, ninety percent of the intercepts remained classified and, since they were almost all in Arabic, they were essentially inaccessible to the defense.[25]

The disproportionate number of FISA intercepts that have not been reviewed (or translated, or reduced to a transcript) by the government, combined with the refusal to declassify all of the intercepts, creates another disadvantage for the defense. Practically, it reverses the obligation imposed upon the government, pursuant to *Brady v. Maryland*,[26] i.e., to provide the defense with exculpatory material within its custody and control. By not listening to the vast majority of FISA intercepts, the government places the burden on defense counsel to find *Brady* material. Yet defense counsel's inability to discuss the classified FISA intercepts with the defendants ensures that most, if not all, of such *Brady* material will not be identified or fully exploited.

The tactical use of the declassification authority in cases throughout the nation is clearly *not* the product of uniform or national Department of Justice policy. Indeed, the use of declassification as a sword rather than as a shield—easily and promptly declassifying the FISA in-

---

[24] 04-CR-240G (N.D. Tex. July 26, 2004). The documents are available on the district court's web site at https://ecf.txnd.uscourts.gov.

[25] That appears to be the general equation in cases involving foreign-language FISA electronic surveillance, i.e., that the government has the resources to summarize only a small fraction of the total number of intercepts. A July 2005 report by the Department of Justice Inspector General revealed that, as of March 30, 2005, the Department of Justice had a 38,514-hour backlog of untranslated and unreviewed foreign-language FISA counterterrorism audio intercepts (not including those classified as "counterintelligence"—an even larger number; nor do the figures include text backlog, such as unreviewed e-mails). This represents a more than 50% increase from the total as of December 31, 2003. *See Federal Bureau of Investigation's Foreign Language Translation Program Follow-Up*, U.S. Department of Justice, Office of the Inspector General, Audit Division, Audit Report 05-33, July 2005, *available at* http://www.usdoj.gov:80/oipr/readingroom/oipr_records.htm (last visited Oct. 10, 2006). Since FISA warrants increased by 18% percent in 2005 over the 2004 total, http://fas.org/irp/agency/doj/fisa, it is inconceivable that the backlog has diminished since the report was issued. Consequently, and ironically, declassification of a defendant's FISA intercepts for discovery purposes may provide the best chance for someone reviewing the vast bulk of foreign-language FISA intercepts.

[26] 373 U.S. 83 (1963).

tercepts that the government intends to introduce in evidence, while avoiding declassification of all other conversations (which, presumably, the government has some reason *not* to introduce in evidence)—stands in stark contrast to the ordinary practice in the Southern District of New York.

For example, in *United States v. Rahman*, (the Blind Sheikh/ "Landmarks" prosecution),[27] *United States v. Usama bin Laden*, (the "Embassy Bombings" case),[28] *United States v. Sattar*, (ten years' worth of FISA intercepts)[29] and *United States v. Shah*, (post-September 11 interceptions),[30] the government declassified and produced the FISA intercepts of the defendants' own communications as part of discovery (and did so even FISA intercepts from other cases that were relevant, even when the government did not introduce any of those intercepts as evidence).[31]

In *bin Laden*, with respect to defendant Wadih El-Hage, the majority of the intercepts were not even gathered pursuant to FISA. Rather, under Executive Order 12,333,[32] they were the product of warrantless overseas electronic surveillance of two telephones in Kenya, where Mr. El-Hage, a U.S. citizen, resided at the time.[33] Security concerns, however, were obviated, because the identity of the agency that performed the wiretapping and the methodology employed remained classified.

In this regard, the author is unaware of a single case in which the Southern District of New York has not promptly declassified and made available FISA intercepts capturing the defendants' communications. Also, as the nature of those cases in the Southern District of New York make clear, excuses by prosecutors in other districts—whether based on the volume of interceptions making declassification more difficult, or that some security consideration requires continued classification—ring hollow.

---

27 United States v. Rahman, 861 F. Supp. 247 (S.D.N.Y. 1994).

28 126 F. Supp. 2d 264 (S.D.N.Y. 2000).

29 United States v. Sattar, 272 F. Supp. 2d 348 (S.D.N.Y. 2003).

30 05 Cr. 673 (LAP) (S.D.N.Y. 2004).

31 For instance, in *bin Laden*, during the discovery phase, the government produced the FISA intercepts from the *Rahman* case, but did not seek to offer any of those intercepts in evidence at trial. *Bin Laden*, 2001 WL 66393, at * 4.

32 Exec. Order No. 12,333, 3 C.F.R. 200 (1981), *reprinted in* 50 U.S.C. § 401 (2004) (issued in 1981 by President Reagan, and governing wiretapping of U.S. citizens and others outside of the U.S.).

33 *See* United States v. bin Laden, 126 F. Supp. 2d 264, 269 (S.D.N.Y. 2000).

III. There Is No Basis for the Government's Selective Declassification of FISA Intercepts, and the Practice Violates a Defendant's Fifth and Sixth Amendment Rights

Indeed, it cannot be argued that disclosure of a *defendant's own communications* in the course of discovery could compromise national security. The communications themselves were not classified when made, and if the defendants themselves had recorded the conversations, the government could not prevent the defendants from reviewing those tapes, introducing them at trial, or even making them public in some fashion.[34]

The same is true if the defendant retained all e-mails on his or her computer. The government simply could not classify that source of the material after the fact. Even if a defendant merely remembers the contents of certain conversations or e-mails, the government cannot "classify" that content.[35] In *bin Laden*, the Southern District of New York prosecutors also recognized the redundancy of maintaining certain documents in classified form, when they were already available to the defendant in unclassified form. The documents at issue in *bin Laden* were intercepted faxes of which the defendant possessed original hard-copies.[36]

There is also no danger that the contents of declassified communications will be published en masse. Appropriate protective orders are now de riguer in cases involving classified or sensitive information, and ensure that those intercepts excluded from evidence remain sealed and protected from public disclosure.[37]

Likewise, the traditional rationale for classification—protecting either the source or contents of the communications—is inapplicable in these circumstances. Once the FISA interceptions are divulged as part of discovery, the source of surveillance and defendant's own communications that he or she authored or received are no longer confidential. Nor do the materials in any way reveal the government's assessment of

---

34 In *United States v. Pappas*, the Second Circuit held that CIPA could not be used to preclude a defendant from publicly disseminating information (even if classified) previously obtained outside the context of pretrial discovery (although the district court could control and prohibit such dissemination during the pre-trial or trial stages). 94 F.3d 799-801 (2d Cir. 1996).

35 *Id*.

36 *Bin Laden*, 126 F. Supp. 2d at 285-286. Other aspects of CIPA and foreign intelligence electronic surveillance were challenged by Mr. El-Hage in *bin Laden*, but withstood legal challenge. *See generally*, *bin Laden*, 2001 WL 66393.

37 United States v. bin Laden, 58 F. Supp. 2d 113, 116 (S.D.N.Y. 1999).

any particular fact or person, since they consist of the *defendant's own communications*.[38]

Thus, stripped of these premises for continued classification, the rationale for the government's refusal to declassify a defendant's own FISA-intercepted communications again is clearly illuminated: to gain a tactical advantage over the defendant, in contravention to CIPA's express and fundamental intention, i.e., that "the defendant should not stand in a worse position, because of the fact that classified information is involved, than he would without this Act."[39] In fact, in one case, the government showed prospective grand jury witnesses FISA intercepts to refresh their recollections (or challenge or change them), yet denied the defendants the same opportunity to review their own communications in preparation for trial.[40] That incongruence demonstrates that the government's purpose is not to maintain security and the pristine integrity of the classified evidence, but rather to deny defendants their Due Process rights and the ability to defend themselves effectively.

Conversely, while providing a defendant access to his or her intercepted communications does not prejudice either the government or national security, denying the defendant such access irremediably prejudices a defendant's right to a fair trial. Refusal to declassify a defendant's own FISA-intercepted communications deprives defendants of

---

38 As a result, this type of situation greatly differs from the circumstances in *United States v. Yunis*, in which the means of interception were not revealed. 867 F.2d 617, 618-619 (D.C. Cir. 1989). In denying the defendant discovery requests from his own recorded conversations with the informant, and stating that these conversations were not important to the case, the court pointed out that "much of the government's security interest in the conversation lies not so much in the contents of the conversations, as in the *time, place, and nature of the government's ability to intercept the conversations at all*." 867 F.2d at 623 (emphasis added). The court also stated that "a foreign counter-intelligence specialist . . . could learn much about this nation's intelligence-gathering capabilities from what these documents revealed about sources and methods." *Id.* The same is true for those cases in which government interpretations or estimates are included within the classified materials, *see, e.g.,* United States v. Squillacote, 221 F.3d 542, 578 (4th Cir. 2000), or release of the materials provides formal government confirmation of some fact upon which the government does not wish to comment. *See* Nuclear Control Inst. v. United States Nuclear Regulatory Comm'n, 563 F. Supp. 768, 771 (D.D.C. 1983).

39 S. REP. No. 96-823, at 9 (1980), *as reprinted in* 1980 U.S.C.C.A.N. 4302; *see also North*, 698 F. Supp. at 320.

40 In a related context, while the government claimed that national security considerations superseded Moussaoui's right to access exculpatory information which were gathered from debriefings of captured al Qaeda personnel, *see Moussaoui*, 365 F.3d at 295, *reh'g granted*, 382 F.3d 453 (4th Cir. 2004), there did not appear to be any problem allowing journalists to view the reports of such debriefings when it suited the government's purposes. *See, e.g.,* John Solomon, *9/11 Planner Tells of Plot's Origins*, WASH. POST, Sept. 22, 2003, at A2.

their Sixth Amendment rights to: 1) effective assistance of counsel, since it prevents counsel from preparing defendant's potential testimony and from discussing classified evidence with the defendant (or anyone else in the course of investigating and preparing the defense); 2) confront the evidence against them, which is a *personal* right and not exercisable merely through counsel;[41] and 3) assist in the preparation and presentation of the defense to the charges, including a defendant's testimony.

Denying defendants access to their intercepted communications also violates their Fifth Amendment rights, including their right to: 1) testify on their own behalf, since it is strategically fatal to have a defendant testify without adequate preparation regarding evidence that counsel is aware of but cannot reveal to the client;[42] and 2) remain silent, since in order to introduce classified evidence at trial, *even through his or her own testimony*, the defendant must sufficiently in advance of trial notify the government of the evidence that defense seeks to admit.[43]

The practical problems are manifest and intractable, effectively eliminating a defendant's right to consult with his or her attorney regarding witnesses, tactics and a substantial volume of evidence in two critical respects. First, the defendant will be unable to consult with counsel regarding which portions of the classified intercepts are relevant and exculpatory and which might lead to such evidence or be useful in impeaching government witnesses. Second, the defendant will not be privy to certain important interceptions that could either corroborate his or her own testimony or be used as substantive exculpatory evidence.

Conversely, from the perspective of an attorney's constitutional and professional duty to provide effective assistance of counsel, it is impossible for counsel to prepare a defendant adequately for his or her *direct* testimony, much less cross-examination, without addressing the substance of thousands (often tens of thousands) of intercepted communications that remain classified. How is counsel to decide whether or not to have the defendant testify when a trove of potential impeachment

41 *See, e.g.,* Faretta v. California, 422 U.S. 806, 819 (1975).

42 Even defendants who have knowledge of the classified information are denied this right because they are not free to testify about such matters without first previewing such testimony for the court and the government, and having it subject to the CIPA process, which includes potential substitutes for the classified information itself.

43 In the Embassy Bombings case, the defense moved to have CIPA declared unconstitutional on these grounds. The district court's opinion, denying the motion, is reported at *bin Laden*, 2001 WL 66393, at *1.

exists, which the government can use at its discretion, but that defense counsel cannot discuss with the defendant? How may counsel determine which FISA-intercepted communications are exculpatory, or might expose the defendant to potentially dangerous cross-examination, without input from the defendant?

Also, even when, or if, an interpreter translates the classified FISA interceptions, that interpreter would not necessarily be able to identify the participants of the conversations, and the defendant may be the only person who could adequately inform counsel and place the communication in the appropriate (and exculpatory) context. Moreover, in these types of cases, defense counsel cannot independently learn and absorb everything that is contained in discovery because foreign-language intercepts are beyond their understanding without the benefit of an interpreter. The language barrier and cultural and ethnic diversity make the defendant's contribution all the more important in preparation and presentation of the defense's case. The result is that the defendant's lack of access to the intercepted communications seriously impairs counsel's ability to consult the defendant, which irrevocably impairs counsel's ability to represent the defendant effectively.

IV. The Courts' Recent Responses to the Inequities Created By the Government's Selective Exercise of Its Declassification Authority

In *California v. Trombetta*,[44] the Court explained that it has "long interpreted [the Due Process Clause's] . . . standard of fairness to require that criminal defendants be afforded a meaningful opportunity to present a complete defense." As the Court in *Trombetta* explained, "[t]o safeguard that right, the Court has developed 'what might loosely be called the area of constitutionally guaranteed access to evidence.'"[45]

That constitutional guarantee is violated by a system that denies one party access to materials over which the opposing party has unilateral authority to disclose or withhold without any intervention by the courts. As cases involving classified information proliferate, this becomes more than an isolated problem.[46] Rather than viewing such cases

---

[44] 467 U.S. 479, 485 (1984).

[45] *Id.* (quoting United States v. Valenzuela-Bernal, 458 U.S. 858, 867 (1982)).

[46] "'This has gotten to the crisis point,' [says] Jonathan Turley of George Washington University Law School . . . . 'We are turning our courts into something like military tribunals where the evidence is entirely up to the prosecutor.'" Mike Robinson, *Defense Lawyers Shut Out as*

as sui generis, in which particular decisions will not have broad or repetitive impact, judges are recognizing that cases involving classified information present genuine tests whether a fair trial, equal access to evidence, and the adversarial process can successfully coexist with unreviewable invocations of national security.[47]

Judges have also sought to fulfill CIPA's mandate in which courts devise innovative remedies for the inequities that inevitably arise as a result of the decidedly un-level playing field created when a case involves classified information: "CIPA is a procedural statute, and the legislative history of it shows that Congress expected trial judges to fashion creative solutions in the interests of justice for classified information problems."[48]

In *United States v. Padilla*,[49] the district court ordered that Padilla be afforded access to certain classified materials, namely government memoranda and reports setting forth his statements and videotapes of his interrogations while in U.S. military custody.[50]

In *United States v. Abu Marzook*,[51] the district court determined the procedures for defendant's suppression hearing challenging the admissibility of statements he made while in Israeli custody. The court

---

War on Terror Spawns Courtroom Secrecy, THE ASSOCIATED PRESS, June 13, 2006, at 1. The government's post-September 11 reflexive and obsessive resort to secrecy in criminal prosecutions arguably related to terrorism might lead an observer to conclude that the events of that day were somehow the product of some counterterrorism measure that was compromised by disclosure. Yet that is not the case; nor has there been any allegation to that effect. Indeed, September 11 was not the result of not enough secrecy, but rather perhaps of *too much* secrecy, such as the failure of law enforcement and intelligence agencies to share important information. *See* 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES (2004).

47 In *Moussaoui*, in ruling that families of the victims of the September 11 attacks were entitled to the same unclassified aviation security documents that had been provided to the defense in the criminal case, the district court noted during one court proceeding that "'[a]s a culture, we need to be careful not to be so wrapped up in secrecy that we lose track of our core values and laws.'" *See* Phil Hirschkorn, *Judge Blasts Government Secrecy*, CNN.com, Apr. 7, 2006, http://www.cnn.com/2006/LAW/04/07/moussaoui/index.html (last visited Sept. 2, 2006).

48 *Libby I*, 429 F. Supp. 2d at 22 (quoting United States v. North, 713 F. Supp. 1452, 1453 (D.D.C. 1989) (citing H.R. REP. NO. 96-1436, at 11, 14 (1980), *as reprinted in* U.S.C.C.A.N. 4294)).

49 04-60001-Cr. (S.D. Fla. July 5, 2006).

50 The district court's July 5, 2006 order, and the government's two July 7, 2006 letters identifying the classified materials to which Mr. Padilla would have access, are available via PACER on the Southern District of Florida's web site, https://ecf.flsd.uscourts.gov.

51 412 F. Supp. 2d 913 (N.D. Ill. 2006).

ruled that even though the Israeli agents' testimony was classified, Mr. Salah would be permitted to attend the hearing.[52] In addition, any testimony by Mr. Salah at such a hearing would not be considered classified, even though it would include "information gathered by the [Israeli agents] and the techniques used by them."[53]

Also, the district court held that the Israeli agents would not be permitted to testify in "light disguise", because Mr. Salah "presumably has already physically seen them at length."[54] However, the district court sufficiently accommodated security concerns, preventing further dissemination of the Israeli agents' identities by prohibiting anyone in the courtroom from describing their appearance to others.[55]

Also, in *United States v. Libby*, the district court ordered that Mr. Libby be provided access to his classified handwritten notes during the period relevant to the indictment, in addition to redacted versions of documents that were provided to Mr. Libby during his morning intelligence briefings and topic overviews of the subject matters contained in those documents.[56] Thus, in effect, the district court concluded that Mr. Libby is entitled to review the information that he had access to while he was the vice president's chief of staff. Therefore, the court's holding in *Libby* is not dissimilar from any other defendant being afforded access to his or her own FISA-intercepted communications.

V. Proposals for Reforming CIPA In Order to Eliminate the Government's Use of Its Declassification Authority as a Sword to Gain Tactical Advantage over Defendants

Rectifying the problems caused by the government's tactical use of its classification and declassification authority requires revision of three separate, but interrelated, provisions: CIPA, FISA, and Rule 16 of the Federal Rules of Criminal Procedure (which governs discovery in federal criminal prosecutions).[57] Indeed, part of the problem is that all three statutes, while often overlapping in cases involving classified information, were enacted and have developed independently. For example, when FISA was enacted in 1978, CIPA did not yet exist.

---

52 *Id.* at 919.

53 *Id.* at 927.

54 *Id.* at 927-28.

55 *Id*.

56 *Libby II*, 429 F. Supp. 2d at 1, 4 n.3, 17 (D.D.C. 2006).

57 All three provisions should be amended to avoid any conflict or ambiguity on these issues.

Thus, FISA's presumptive proscription on defense access to FISA applications and warrants was enacted at a time when there was no mechanism for defense counsel to review classified material.[58] While CIPA specifically permits defense counsel to see far more sensitive classified material than FISA applications, FISA has never been harmonized to account for that dramatic change in defense counsel's ability to review classified material. The revisions proposed below attempt to achieve the harmony that is essential to ensure that defendants in the burgeoning number of cases involving classified material and FISA-generated evidence receive the Due Process and fair trial guaranteed by the Fifth and Sixth Amendments.[59]

As a threshold matter, the following section should be added:

> any interceptions made pursuant to FISA, including telephone, internet, or facsimile communications, and any materials seized pursuant to searches authorized under FISA, and any pen register or trap-and-trace information obtained through FISA, shall be declassified to the extent of allowing the defendant to review the content of his or her own communications, or information (such as pen register, trap and trace, or internet addressing), or obtained from his or her telephone line(s), internet account(s), or other communications device used by the defendant, or items seized from the defendant, or at his or her residence or place of business, or other place within the control of the defendant (such as an automobile or other conveyance), or which seized items belong to the defendant but were seized from another person or location.

Another section should grant authority to the court to issue appropriate protective orders:

> the court is authorized to issue any protective order it deems necessary to limit dissemination of the information and materials covered in the above section, including restricting where such materials can be reviewed, and/or requiring that defense counsel or a representative thereof be present when a defendant is reviewing the materials.

---

58 The Act prescribed that the underlying applications, warrants and orders were not to be disclosed to the defense absent exercise of the court's discretion or some due process necessity. 50 U.S.C. § 1806 (f)-(g) (2000).

59 While the author has not been involved in drafting legislation since High School Model Congress, perhaps that is a virtue considering the abstract, imprecise, ambiguous, and inaccessible language that is often a hallmark of national security legislation.

In addition, the court should be empowered to impose specific sanctions for violation of any such protective orders:

> the court is authorized to punish violations of such protective orders by appropriate means, including: (a) evidentiary sanctions; (b) denying the violator further access to the materials; (c) re-classifying the materials; (d) adjustment of the defendant's bail status, including remand (if the defendant is the alleged violator, or knew of and consented to the violation); and/or (e) monetary sanctions. However, any violation by a defendant's counsel shall not result in any adverse sanction with respect to the defendant's ability to review the materials, to present a defense, or to cross-examine government witnesses, unless counsel's violation was committed with the defendant's knowledge and/or consent.[60] Also, no such sanction shall be imposed without first affording the alleged violator the right to be heard and present evidence in his or her defense. No sanction shall be imposed unless, after the alleged violator has had the right to be heard and present evidence, the court finds specifically by clear and convincing evidence that the violation was knowing and intentional.

The revisions should also provide each party the reciprocal right to seek the narrowing or expansion of the scope of disclosure:

> the government may move to withhold from declassification under the above section specific enumerated communications or information covered in the above section. The government must establish the need to withhold those enumerated conversations by clear and convincing evidence with respect to the individual conversations specifically (and not generally as a group). The motion cannot be made ex parte, but can be made pursuant to CIPA so that only cleared defense counsel have access to the moving papers.[61]

Conversely, the defense should be able to expand the protective order to include particular experts or other witnesses:

---

60 *See generally,* United States v. Schwarz, 283 F.3d 76 (2d Cir. 2002) (counsel's improper post-trial interview of juror would not forfeit the defendant's right to have the issue of juror misconduct during deliberations decided on the merits.).

61 Since cleared defense counsel will already have had access to all of the disclosed, classified materials, there is no legitimate basis for an ex parte proceeding regarding which particular intercepts or items the government wishes to withhold from the defendants themselves.

> the defendant may move for permission to show specific communications or materials or information to designated experts (either consultants or witnesses) or other witnesses. The defendant must provide good cause for such dissemination as to each communication or item or piece of information with respect to each expert or witness. Such motion must be made on notice, and if the government maintains a firewall Assistant United States Attorney ("AUSA"),[62] the name of the expert or witness must be provided to that firewall AUSA. Otherwise, the court may entertain the motion with the names of the witnesses remaining ex parte.[63] This section does not require a motion for those persons who have the appropriate level security clearance in the case to review the communications or materials or information even if they had remained classified, i.e., codefendants' counsel.

Also, since the government retains declassification authority, the revisions must include, as does CIPA, the possibility for sanctions should the government refuse to declassify the materials mentioned above:

> should the government refuse to declassify the materials covered in the above section, the court possesses the authority to impose sanctions upon the government for its failure to declassify. The court possesses broad discretion to fashion an appropriate remedy, which can take the form of evidentiary sanctions (preclusion of government evidence or expansion of defendant's evidence), or even dismissal of specific counts or the entire indictment.

VI. CONCLUSION

The government's unilateral and categorical authority to classify and declassify has been used to gain significant tactical advantage over defendants in certain criminal cases involving terrorism allegations. The

---

62 As conventionally defined in these types of cases, a "firewall" AUSA is not part of the prosecution team for the particular case and does not communicate to the prosecution team the identity or nature of the defense requests. Rather, the "firewall" AUSA's purpose is to receive defense requests related to the showing of sealed and/or sensitive documents to potential defense witnesses, experts, and consultants without revealing to the prosecution team the defense's strategy or activity.

63 Generally, in the CIPA context, courts have permitted defendants to make ex parte submissions in order to establish the relevance, materiality, and admissibility of classified information. *See, e.g.,* United States v. Clegg, 740 F.2d 16 (9th Cir. 1984); *Libby I*, 429 F. Supp. 2d 18 (D.D.C. 2006); *North*, 698 F. Supp. 322 (D.D.C. 1988).

practice of denying defendants access to their own FISA-intercepted communications by refusing to declassify them deprives defendants and their counsel of meaningful access to a considerable amount of evidence, much of which may very well be exculpatory. That practice constitutes a denial of defendants' Fifth and Sixth Amendment rights that exist to guarantee a fair trial. Reforms to CIPA, FISA, and Rule 16, as proposed in this article, are necessary to restore balance in those cases in which there are classified FISA intercepts of the defendants' own communications.