2015

# Section 702 and the Collection of International Telephone and Internet Content

Laura K. Donohue
*Georgetown University Law Center*, lkdonohue@law.georgetown.edu



38 Harv. J.L. & Pub. Pol'y 117 (2015)

# SECTION 702 AND THE COLLECTION OF INTERNATIONAL TELEPHONE AND INTERNET CONTENT

LAURA K. DONOHUE*



* Professor of Law, Georgetown University Law Center. Thanks to Judge Morris Arnold, William Banks, Orin Kerr, and David Kris for comments on an earlier draft of this paper. This Article is Part Two of two-part series on NSA surveillance under the Foreign Intelligence Surveillance Act. For Part One, see Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Questions*, 37 HARV. J.L. & PUB. POL'Y 757 (2014).

## INTRODUCTION

On June 6, 2013, the *Washington Post* and the *Guardian* captured public attention by reporting that the intelligence community was collecting large amounts of information about U.S. citizens.[1] 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."[2]

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-984XN).[3] The title

1. Barton Gellman & Laura Poitras, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, WASH. POST, June 7, 2013, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html [http://perma.cc/Y6F2-3UHX]; Glen Greenwald & Ewen MacAskill, *NSA Prism program taps in to user data of Apple, Google and others*, GUARDIAN, June 6, 2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [http://perma.cc/G4AD-DA88].

2. Gellman & Poitras, *supra* note 1. The Privacy and Civil Liberties Oversight Board later clarified, "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 BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 7 (2014) [hereinafter PCLOB REPORT], *available at* http://www.pclob.gov/Library/702-Report-2.pdf [http://perma.cc/VJ76-Q4CL].

3. PRISM/US-984XN Overview, April 2013, *available at* https://www.aclu.org/files/natsec/nsa/20130816/PRISM%20Overview%20Powerpoint%20Slides.pdf [http://perma.cc/F5JZ-2GMD] [herinafter PRISM SLIDES]. A Signals Intelligence Activity Designator (SIGAD) is an alphanumeric designator that identifies a facility used for collecting Signals Intelligence (SIGINT). The facilities may be terrestrial (for example, connected to internet cables), sea-borne (for example, intercept

slide referred to it as the most used NSA SIGAD.[4] The documents explained that PRISM draws from Microsoft, Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL, and Apple—some of the largest e-mail, 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 (for example, logins), social networking details, and special requests.[5] The slides noted that the program started in September 2007, with just one partner (Microsoft), gradually expanding to the most recent company (Apple, added October 2012), and that the total cost of the program was $20 million per year.[6] As of 2011, most of the more than 250 million Internet communications obtained each year by the NSA under Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act derived from PRISM.[7]

A follow-up article two days later printed another slide depicting both PRISM and "upstream" collection of communications on fiber cables and infrastructure ("[c]ollection directly from the servers of . . . U.S. Service Providers.")[8] Upstream interception allowed the NSA to acquire Internet communications "as they

---

ships), or satellite stations. 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. Glenn Greenwald & Ewen MacAskill, *Boundless informant: the NSA's secret tool to track global surveillance data*, GUARDIAN, June 11, 2013, http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining [http://perma.cc/6HYJ-VHLY]. PRISM is the name by which the program was known inside the NSA. *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., PUBLIC HEARING REGARDING THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 3 (2014) [hereinafter PCLOB HEARING], *available at* http://www.pclob.gov/Library/20140319-Transcript.pdf [http://perma.cc/GM4K-4Y99].

4. PRISM SLIDES, *supra* note 3, at 1.

5. *Id.* at 2.

6. *Id.* at 3.

7. [Redacted], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011). PCLOB later confirmed that as of mid-2011, approximately 91% of Internet communications obtained each year came through PRISM. PCLOB REPORT, *supra* note 2, at 34.

8. James Ball, *NSA's Prism surveillance program: how it works and what it can do*, GUARDIAN, June 8, 2013, http://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google [http://perma.cc/TZ3R-NJTH] (including slide entitled FAA702 Operations).

transit the 'internet backbone' facilities."[9] 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.[10] The slide urged analysts to use both PRISM and upstream collection to obtain information.[11]

Within days of the releases, the intelligence community acknowledged the existence of the programs.[12] In August 2013 the Director of National Intelligence, James Clapper, offered further confirmation, noting that PRISM had been in operation since Congress had passed the 2008 FISA Amendments Act.[13] He declassified eight documents,[14] and by the end of the month, he had announced that the intelligence community would release the to-

9. [Redacted], 2012 WL 9189263, at *1 (FISA Ct. Aug. 24, 2012), *available at* http://fas.org/irp/agency/doj/fisa/fisc0912.pdf [http://perma.cc/TP7C-JB9Q]; *see also* Raj De, Nat'l Sec. Agency Gen. Couns., Statement at the Privacy and Civil Liberties Oversight Board: Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 26 (Mar. 19, 2014) ("Upstream collection refers to collection from the, for lack of a better phrase, Internet backbone rather than Internet service providers.").

10. *[Redacted]*, 2011 WL 10945618, at *10 n.26.

11. *Id.*

12. See How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries: Hearing Before the H. Permanent Select Comm. on Intelligence, 113th Cong. (2013) (Statement of General Keith Alexander, Director of the National Security Agency).

13. Press Release, Office of the Dir. of Nat'l Intelligence, DNI Declassifies Intelligence Community Documents Regarding Collection under Section 702 of the Foreign Intelligence Surveillance Act (FISA) (Aug. 21, 2013), http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-declassifies-intelligence-community-documents-regarding-collection-under-section-702-of-the-foreign-intelligence-surveillance-act-fisa [http://perma.cc/LH9A-HKP2]; Cover Letter from James Clapper, Dir. of Nat'l Intelligence, Announcing the Document Release (Aug. 21, 2013), http://www.dni.gov/files/documents/DNI%20Clapper%20Section%20702%20Declassification%20Cover%20Letter.pdf [http://perma.cc/M62Q-36D5].

14. Press Release, Office of the Dir. of Nat'l Intelligence, *supra* note 13; Cover Letter from James Clapper, *supra* note 13 (declassifying two memorandum opinions issued by the Foreign Intelligence Surveillance Court, communications between the Administration and Congress on the existence and operation of the programs, and the Section 702 minimization procedures).

tal number of Section 702 orders issued, and targets thereby affected, on an annual basis.[15]

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.[16] Accordingly, this Article proceeds in three Parts: 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 September 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).[17] The first Part ends with a brief discussion of the current

---

15. Press Release, Office of the Dir. of Nat'l Intelligence, DNI Clapper Directs Annual Release of Information Related to Orders Issued Under National Security Authorities (Aug. 29, 2013), http://icontherecord.tumblr.com/post/59719173750/dni-clapper-directs-annual-release-of-information [http://perma.cc/AU38-AM4C]. The first such report, issued June 26, 2014, indicated that there was only one order annually issued under 702, affecting some 89,138 targets. *See* http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013 [http://perma.cc/FG3W-PTZQ].

16. Some of the most important documents that have thus far been released in relation to this program include: Foreign Intelligence Surveillance Act (FISA) Section 702, 50 U.SC § 1881a (2012); NAT'L SEC. AGENCY/CENT. SEC. SERV., EXHIBIT A: PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED, (2007) [hereinafter NSA TARGETING PROCEDURES], *available at* http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document [http://perma.cc/E2NG-PU9P].

17. For important contributions to the statutory and constitutional discussion of the FAA and the potential for further FISA reform prior to the release of the Snowden documents, see William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEXAS L. REV. 1633 (2010); Orin S. Kerr, *Updating the Foreign Intelligence Surveillance Act*, 75 U. CHI. L. REV. 225 (2010); David S. Kris, *Modernizing the Foreign Intelligence Surveillance Act: Progress to Date and Work Still to Come*, in LEGISLATING THE WAR ON TERROR: AN AGENDA FOR REFORM, 217 (Benjamin Wittes, ed., 2009); Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245 (2008); Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, U. CHI. L. REV. 287 (2008); Mark D. Young, *Electronic Surveillance in an Era of Modern Technology and Evolving Threats to National Security*, 22 STAN. L. & POL'Y

state of foreign intelligence collection under Executive Order 12,333, outside either FISA or the FAA.

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 Section 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 Section 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.

---

REV. 11 (2011). *See also* Jonathan D. Forgang, Note, *"The Right of the People": The NSA, the FISA Amendments Act of 2008, and Foreign Intelligence Surveillance of Americans Overseas*, 78 FORDHAM L. REV. 217 (2009); Stephen Vladeck, *More on Clapper and the Foreign Intelligence Surveillance Exception* LAWFARE (May 23, 2012, 3:32 PM), http://www.lawfareblog.com/2012/05/more-on-clapper [http://perma.cc/8ZW7-83VX].

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*.[18] 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 Section 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.

## I. THE EVOLUTION OF SECTION 702

Section 702 is a product of history—one influenced by the Bush Administration's response to September 11. The President initially looked to constitutional authorities to support a wide-ranging surveillance program. Subsequent efforts to move the collection of

18. 343 U.S. 579 (1952).

international content to a statutory basis led to a redefinition of "facility" and new statutory language. Part of the impetus for the 2008 FAA related to ways in which technology had evolved: Surveillance previously controlled by executive order increasingly found itself within a FISA framework. Congress thus sought to modernize the law, creating higher protections for U.S. persons' privacy in the process . Renewed in 2012, the 2008 FAA is set to expire in 2017.

### *A. The President's Surveillance Program*

On October 4, 2001, the President authorized the NSA to collect two different types of bulk information: metadata and content.[19] The former gave the agency the ability to identify terror-

19. Authorization for Specified Electronic Surveillance Activities During a Limited Period to Detect and Prevent Acts of Terrorism Within the United States, Oct. 4, 2001, cited in OFFICE OF THE INSPECTOR GEN., NAT'L SEC. AGENCY CENT. SEC. SERV., WORKING DRAFT ST-09-0002, at 1, 7–8, 11, 15 (2009) [hereinafter WORKING DRAFT], available at http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection [http://perma.cc/M3FC-QMHN]. The Obama Administration has publicly confirmed the inclusion of Internet and telephony metadata, and telephony content, as part of the President's Surveillance Program, but not Internet content. See Press Release, Director of National Intelligence, DNI Announces the Declassification of the Existence of Collection Activities Authorized by President George W. Bush Shortly After the Attacks of September 11, 2001 (Dec. 21, 2013) [hereinafter Declassification Press Release], available at http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/991-dni-announces-the-declassification-of-the-exisitence-of-collection-activities-authorized-by-president-george-w-bush-shortly-after-the-attacks-of-september-11,2001 [http://perma.cc/8L7R-386U]; Unclassified Declaration of Frances J. Fleisch, National Security Agency, Jewel v. Nat'l Sec. Agency, No. 08-cv-4373-JSW (N.D. Cal. Dec. 20, 2013) [hereinafter Fleisch Declaration], available at https://www.eff.org/files/2013/12/21/fleisch2013jewelshubert.pdf [http://perma.cc/6LHT-LS7X] (using language identical to DNI press release). *See also* OLC-132, Memorandum from a Deputy Assistant Attorney General in the Office of Legal Counsel to the counsel to the President, regarding a request from the White House for OLC's views regarding what legal standards might govern the use of certain intelligence methods to monitor communications by potential terrorists, Oct. 4, 2001, noted by Second Redacted Declaration of Steven G. Bradbury, Elec. Priv. Info. Ctr. v. Dep't of Justice, 511 F. Supp. 2d 56 (D.D.C. 2007), available at https://www.aclu.org/sites/default/files/pdfs/safefree/aclu_v_doj_2nd_declaration_steven_bradbury.pdf [http://perma.cc/B7L2-8DCV]. Note that for purposes of this paper, I cite to the Working Draft of the NSA Inspector General report, released by the Guardian on June 27, 2013. Some caution, however, should be exercised in relying wholly on this report, as the government has not formally declassified the report's contents and acknowledged its accuracy. The Administration has, however, confirmed other documents released by the Guardian at the

ist-related activity through contact chaining (the process of building a network graph that modeled communication patterns of targets and their associates).[20] The latter provided raw intelligence.[21] The NSA focused on telephony and Internet sources for each kind of information, with four categories resulting: (1) telephony metadata; (2) Internet metadata; (3) telephony content; and (4) Internet content.[22]

The Administration initially based the President's authority to conduct the President's Surveillance Program on three legal theories: (1) the President's inherent Article II authorities as Commander in Chief; (2) the 2001 Authorization for the Use of Military Force (AUMF); (3) and the War Powers Resolution (WPR).[23] 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 the President's Surveillance Program. OLC found that bulk Internet metadata collection appeared to be prohibited by FISA and Title III.[24] The President thus rescinded the authority to collect bulk Internet metadata and gave the NSA one week to terminate the program.[25]

Although known 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 the public became aware of the existence of the President's Surveillance Program.[26] As concern

---

time, and so I proceed, in part, on the assumption that the report is accurate, with the appropriate cautions in place.

20. WORKING DRAFT, *supra* note 19, at 13.

21. *Id.* at 15.

22. Within a month, the President's Surveillance Program, renewed thereafter at thirty to sixty day intervals, became operational. *Id.* at 11.

23. *See, e.g.*, President's Radio Address, WHITE HOUSE, Dec. 17, 2005, *available at* http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051217.html [http://perma.cc/Z88M-4CS3]; U.S. DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT (2006), *available at* http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf [http://perma.cc/GL5C-T7H2]; Letter from William E. Moschella, Assistant Attorney General, to Sen. Pat Roberts, Chair, Senate Select Committee on Intelligence et al. (Dec. 22, 2005), *available at* https://www.fas.org/irp/agency/doj/fisa/doj122205.pdf [http://perma.cc/Z3CA-U7ZP].

24. OLC issued opinions on this matter Mar. 15, 2004, May 6, 2004, and July 16, 2004. WORKING DRAFT, *supra* note 19, at 37.

25. *Id.* at 38.

26. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, *available at* http://www.nytimes.com/2005/12/16/politics/

increased, the Attorney General sent a five-page missive to key congressional leaders justifying the program. The problem, according to the letter, was that FISA lacked the flexibility needed to identify potential threats.[27] At that time, only a narrow part of the program's contours was public: the NSA's interception of (some) telephone content between the United States and overseas.[28] During his end-of-the-year press conference, President Bush stated that the program was limited to international communications to and from known terrorists and their associates.[29] Pressed for the legal rationale behind what became known as the Terrorism Surveillance Program (TSP), the Bush Administration cited the three legal theories (Article II, the 2001 AUMF, and the WPR).[30]

In the face of mounting pressure, the legal basis for the component parts of the President's Surveillance Program gradually altered.[31] On May 24, 2006, the NSA transferred the bulk collection

---

16program.html?pagewanted=all&_r=0 [http://perma.cc/8PT9-JGKE] ("Months after the Sept. 11 attacks, President Bush secretly authorized the National Security Agency to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without the court-approved warrants ordinarily required for domestic spying, according to government officials."). *See also* Eric Lichtblau & James Risen, *Spy Agency Mined Vast Data Trove*, Officials Report, N.Y. TIMES, Dec. 24, 2005, http://www.nytimes.com/2005/12/24/politics/24spy.html?pagewanted=all [http://perma.cc/99QY-P9BX] ("The National Security Agency has traced and analyzed large volumes of telephone and Internet communications flowing into and out of the United States as part of the eavesdropping program that President Bush approved after the Sept. 11, 2001, attacks to hunt for evidence of terrorist activity, according to current and former government officials.").

27. Terry Frieden, *Administration Defends NSA Eavesdropping to Congress*, CNN (Dec. 23, 2005, 10:51 AM), http://www.cnn.com/2005/POLITICS/12/23/justice.nsa/index.html [http://perma.cc/KP62-EZS7]. The letter was sent to Senators Pat Roberts (R-KS) and John Rockefeller (D-WV), as well as Reps. Peter Hoedstra (R-MI) and Jane Harman (D-CA).

28. Lichtblau & Risen, *Spy Agency Mined Vast Data Trove*, *supra* note 26.

29. Frieden, *supra* note 27.

30. *See supra* note 23.

31. *See, e.g.*, Josh Meyer & Joseph Menn, *U.S. Spying is Much Wider, Some Suspect*, L. A. TIMES, Dec. 25, 2005, at A1 (citing the potential wholesale collection of communication data outside of FISA and discussing the consequent threat to citizens' privacy); Shane Harris, *FISA's Failings*, NAT'L J., Apr. 8, 2006, at 59; 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 [http://perma.cc/Y25W-P9DZ]; Seymour M. Hersh, *Listening In*, NEW YORKER, May 29, 2006, http://www.newyorker.com/archiva/2006/05/29/060529ta_talk_hersh [http://perma.cc/M6XN-GNTY]. Calls for reform also emerged. *See, e.g.*, Richard A. Posner, Op-Ed., *A New Surveillance Act*, WALL ST. J., Feb. 15, 2006, at A16 (arguing for reforms to

of telephony metadata to FISA's Section 501 "tangible things" provisions (as amended by USA PATRIOT Act Section 215).[32] Then in July 2007 the NSA transferred the Internet metadata program to FISA's Pen Register/Trap and Trace authorities. It operated until December 2011, when it was discontinued for failure to deliver sufficient operational value to the NSA.[33]

The remaining collection programs of the President's Surveillance Program, focused on content, proved more troublesome. To transfer them to a different statutory basis, the government would have to find a legal theory to support the NSA's addition and withdrawal of thousands of foreign targets for content collection.[34] The initial solution came in a redefinition of the language of FISA. That redefinition was followed by temporary statutory changes, and finally, a broad understanding of the 2008 FAA.

### *B. Redefinition of "Facility" under FISA*

DOJ's immediate solution to finding a statutory basis for the content portion of the President's Surveillance Program appears

---

FISA to take account of new and emerging technologies); K.A. Taipale & James Jay Carafano, Op-Ed., *Fixing Surveillance*, WASH. TIMES, Jan. 25, 2006, at A15.

32. USA PATRIOT Act, Sec. 215, amending FISA Sec. 501, codified at 50 U.S.C. § 1861 (2012) (Access to certain business records for foreign intelligence and international terrorism investigations). For the original order for Verizon, see *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [Telecommunications Providers] Relating to [REDACTED], Order, No. BR-05 (FISA Ct. May 24, 2006), *available at* https://www.eff.org/sites/default/files/filenode/docket_06-05_1dec201_redacted.ex_-_ocr_0.pdf [http://perma.cc/5QVN-VU3T] (released by court order as part of the Electronic Frontier Foundation's FOIA litigation). Note that the specific telecommunications company from which such records were sought were redacted, as well as the remaining title; however, the government also released an NSA report that provided more detail on the title of the Order. OFFICE OF THE INSPECTOR GEN., NAT'L SEC. AGENCY/CENT. SEC. SERV., ST-06-0018, REPORT ON THE ASSESSMENT OF MANAGEMENT CONTROLS FOR IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE COURT ORDER: TELEPHONY BUSINESS RECORDS (2006) (see page 94 of 1846 and 1862 Production, Mar. 5, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf [http://perma.cc/U3W4-YDC7].

33. *See* Declassification Press Release, *supra* note 19; Fleisch Declaration, *supra* note 19. For detailed discussion of the legality and constitutionality of the Section 215 program and, by analogy, the transfer of Internet Metadata to PRTT, see Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. PUB. POL'Y 757 (2014).

34. WORKING DRAFT, *supra* note 19, at 40.

to have turned on a new definition of "facility" as that term was employed in FISA. From being understood narrowly in its traditional sense—as a particular telephone number—DOJ began to interpret it to mean a central server at telecommunications service providers' facilities, a shift that exponentially increased the amount of information that could be collected.

FISA, at the time, specified that orders approving electronic surveillance include:

> (A) the identity, if known, or a description of the specific target of the electronic surveillance identified or described in the application pursuant to [50 U.S.C. § 1804(a)(3)];
>
> (B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, *if known;*
>
> (C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;
>
> (D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance;
>
> (E) the period of time during which the electronic surveillance is approved; and
>
> (F) whenever more than one electronic, mechanical, or other surveillance device is to be used under the order, the authorized coverage of the device involved and what minimization procedures shall apply to information subject to acquisition by each device.[35]

Any order approving electronic surveillance must direct:

> (A) that the minimization procedures be followed;
>
> (B) that, upon the request of the applicant a specified communication or other common carrier, landlord, custodian, or other specified person, *or in circumstances where the Court finds*, based upon specific facts provided in the application, *that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons,* furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its

35. 50 U.S.C. § 1805(c) (2012).

> secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance;
>
> (C) that such carrier, landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and
>
> (D) that the applicant compensate, at the prevailing rate, such carrier, landlord, custodian, or other person for furnishing such aid.[36]

The italicized portions of the above passages reflect changes made by the 2001 USA PATRIOT Act and 2002 Intelligence Authorization Act, to enable the government to conduct roving wiretaps in cases where the target was attempting to avoid detection by repeatedly changing telephones.[37] Congress explained the rationale behind adding the new language:

> The multipoint wiretap amendment to FISA in the USA PATRIOT Act (Section 206) allows the FISA court to issue generic orders of assistance to any communications provider or similar person, instead of to a particular communications provider. This change permits the Government to implement new surveillance immediately if the FISA target changes providers in an effort to thwart surveillance. The amendment was directed at persons who, for example, attempt to defeat surveillance by changing wireless telephone providers or using pay phones.[38]

---

36. 50 U.S.C. § 1805(c)(2)(B) (2012). Note that the clause "furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services" reflects changes made by the USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. 109-177, § 108, 120 Stat. 192, 203–04 (2006), codified at 50 U.S.C. § 1805(c)(3) (2012)).

37. Intelligence Authorization Act for FY 2002, Pub. L. No. 107-108 (2001); USA PATRIOT Act of 2001, Pub. L. No. 107-56. *See also* ELIZABETH B. BAZAN, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: AN OVERVIEW OF THE STATUTORY FRAMEWORK AND U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT AND U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW DECISIONS, CRS REPORT FOR CONGRESS 24 (2007), *available at* http://www.fas.org/sgp/crs/intel/RL30465.pdf [http://perma.cc/R5N4-LSTQ].

38. H.R. REP. NO. 107-328, at 24 (2001).

The aim was to ensure that where a *particular* target (such as a foreign power or its agents) was the object of foreign intelligence collection, and *where that target was attempting to avoid detection*, the government had some flexibility in switching carriers or telephone lines to continue to keep the target under surveillance.[39]

In 2005 Congress underscored the need for specificity regarding the facilities or places to be placed under surveillance by adding new language:

> An order approving an electronic surveillance under this section in circumstances where the nature and location of each of the facilities or places at which the surveillance will be directed is unknown shall direct the applicant to provide notice to the court within ten days after the date on which surveillance begins to be directed at any new facility or place, unless the court finds good cause to justify a longer period of up to 60 days, of—
>
> (A) the nature and location of each new facility or place at which the electronic surveillance is directed;
>
> (B) the facts and circumstances relied upon by the applicant to justify the applicant's belief that each new facility or place at which the electronic surveillance is directed is or was being used, or is about to be used, by the target of the surveillance;
>
> (C) a statement of any proposed minimization procedures that differ from those contained in the original application or order, that may be necessitated by a change in the facility or place at which the electronic surveillance is directed; and
>
> (D) the total number of electronic surveillances that have been or are being conducted under the authority of the order.[40]

This wording underscored the importance of the Executive Branch being able to articulate *which* facility would be placed under surveillance and the procedures to be followed to ensure minimal collection of non-relevant and non-target communications. In such cases, the government would have to provide information about where the intercept would occur. A facility was understood

---

39. *See also* 147 CONG. REC. S10990 (statement of Senator Feinstein); Edward C. Liu, Cong. Research Serv., R40138, Amendments to the Foreign Intelligence Surveillance Act Extended Until June 1, 2015 (2011), *available at* available at http://www.fas.org/sgp/crs/intel/R40138.pdf [http://perma.cc/C5UD-2VA7].

40. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. 109-177, Mar. 9, 2006, § 108, 120 Stat. 192 (2006), codified at 50 U.S.C. § 1805(c)(3) (2012).

to mean a particular place (such as a home, where a land line was located), a particular telephone number, or a particular computer that was likely to be used by a foreign power or an agent thereof.

According to a leaked working draft of the NSA's Inspector General report, in order to move the content collection involved in the President's Surveillance Program to a more secure legal footing, from mid-2005 to January 2007, DOJ worked with NSA to redefine facility.[41] Instead of understanding the word in the traditional sense, (as a specific telephone number or email address), DOJ argued that it should be understood as a "general gateway" or "cable head."[42]

This change expanded the amount of information that could be obtained by the government under FISA. The Internet consists of a number of interconnected networks that allow computers to communicate. A "gateway" is the entrance point from one network to another, or a node, which converts one protocol stack into another. It is thus an essential feature in most routers (although other devices may also function as gateways). Routers may transfer, accept, and relay packets of information, but they are limited to networks using similar protocols. Gateways, however, can accept packets that are formatted for one protocol and convert it into another protocol format. They house routing databases, which determine the flow of information. A "cable head," in turn, includes computer systems, databases required to provide Internet access, and the cable modem termination system (CMTS), which is a system of devices that sends and receives digital signals on a cable network. The mechanism resides at a phone company's central location, linking customer connections to a single point.

---

41. *See* WORKING DRAFT *supra* note 19, at 41; Letter from Alberto R. Gonzales, U.S. Attorney Gen., to Patrick Leahy, U.S. Senator, & Arlen Specter, U.S. Senator (Jan. 17, 2007), *available at* http://www.fas.org/irp/congress/2007_cr/fisa011707.html [http://perma.cc/C75E-J9KW] ("In the spring of 2005 . . . the Administration began exploring options for seeking . . . FISA Court Approval. . . . These orders are innovative, they are complex, and it took considerable time and work for the Government to develop the approach that was proposed to the Court and for the Judge on the FISC to consider and approve these orders.").

42. WORKING DRAFT, *supra* note 19, at 41 (noting the DOJ ultimately decided "to pursue a FISC order for content collection wherein the traditional FISA definition of a 'facility' as a specific telephone or email address was changed to encompass the gateway or cable head that foreign targets use for communications").

Redefining facility to include gateways held by the telecommunications company, as well as the cable head and CMTS (instead of, more narrowly, specific telephone numbers or Internet protocol addresses associated with particular computers), exponentially increased the amount of content that could be obtained by the government. Instead of just obtaining the content carried by a single telephone line, or to and from a particular computer address, the government could obtain the content of *all* telephone calls or Internet content run through telecommunication companies' routers.

The new interpretation did not immediately gain acceptance. The NSA inspector general's draft report explains, "After 18 months of concerted effort and coordination, the FISC ultimately accepted the theory for foreign selectors but rejected it for domestic selectors."[43]

On January 10, 2007, FISC signed two separate orders: the Foreign Telephone and Email Order and a domestic content order.[44] One week later, Attorney General Alberto Gonzales

---

43. *Id.* at 41–42. A "selector" is a particular communications facility analysts determine is used by a target. Although examples of selectors commonly given by officials tend to be e-mail addresses and telephone numbers, in light of the broader definition of "facility" adopted with regard to the PAA, it is not clear whether a selector under the FAA may include servers, gateways, or cable heads. If it did, however, it would be at odds with the assertion that if a U.S. person is determined to be a user of a selector, the selector may not be tasked to Section 702 acquisition. PCLOB REPORT, *supra* note 2, at 33. In Judge Bates's October 2011 opinion, he writes, "With regard to 'about' communications, the Court previously found that the user of the tasked facility was the 'target' of the acquisition, because the government's purpose in acquiring such communications is to obtain information about that user." [Redacted], 2011 WL 10945618, at *14 (FISA Ct. Oct. 3, 2011). He continues, "the communication is not acquired because the government has any interest in the parties to the communication, other than their potential relationship to the user of the tasked facility . . . " *Id.* This suggests that the continued use by the government of e-mails and telephone numbers as examples of what is being placed under surveillance is misleading. The NSA "tasks" selectors to collect communications. In contrast, the people who *use* the selectors are "targets." Selectors may not be key words (for example, "Tularemia" or "gelignite"); nor may they be names of targeted individuals (for example, "Jane Smith"). Once a selector has been tasked under the targeting procedures, it is forwarded to an electronic service provider to begin acquisition. PCLOB REPORT, *supra* note 2, at 33.

44. Foreign Content Order, Jan. 10, 2007 and Domestic Content Order, Jan. 10, 2007, *cited in* WORKING DRAFT, *supra* note 19, at 41–42. For additional sources noting the ending of the President's Surveillance Program in January 2007 see also S. REP. NO. 110-209, at 4 (2007); Letter from Att'y Gen. Alberto Gonzales to Sen. Patrick Leahy and Sen. Arlen Specter (Jan. 17, 2007); Declassification Press Release,

wrote to the Senate Judiciary Committee, indicating that a FISC judge had issued orders moving the Terrorism Surveillance Program to FISA.[45]

According to the NSA Inspector General, the domestic content order did not have an immediate or significant impact on collection.[46] The Foreign Telephone and Email Order, however, appears to have immediately and negatively affected the number of selectors that could be used with regard to collection.[47]

Under the order, FISC authorized the government to intercept communications passing through listed facilities where the government had made a probable cause determination regarding one of the communicants, and the e-mail addresses and telephone numbers were reasonably believed to be used by individuals outside domestic bounds.[48] At renewal, a different FISC judge approved the program under the condition that the *court*, as opposed to the government, made the probable cause determination with regard to the telephone numbers and e-mail addresses to be used to conduct surveillance.[49] Although the renewal statute pro-

---

*supra* note 19; Fleisch Declaration, *supra* note 19 (suggesting that TSP transitioned to FISA in January 2007).

45. Letter from Alberto R. Gonzales, U.S. Attorney Gen., to Sens. Patrick Leahy, U.S. Senator, & Arlen Specter, U.S. Senator, *supra* note 41. Although the U.S. District Court for the Eastern District of Michigan had entered summary judgment for plaintiffs, finding the warrantless wiretapping in TSP unconstitutional and entering a permanent injunction barring further operation of TSP, in July 2007 the Sixth Circuit Court of Appeals dismissed the suit for lack of standing. ACLU v. NSA, 493 F.3d 644 (6th Cir. 2007), *rev'g* ACLU v. NSA, 438 F. Supp. 2d 754 (E.D. Mich. 2006). According to Gonzales, the order authorized "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." *Id.*

46. WORKING DRAFT, *supra* note 19, at 42. It did, however, slow the process down to where, by January 2009, there was only a single selector directed towards collection. The FBI subsequently assumed responsibility for the Domestic Content Order before the FISC. *Id.* While attention has been paid post-June 2013 to Section 702, significantly less focus has been drawn to the Domestic Content Order.

47. *Id.*

48. Declassified Certification of Attorney General Michael B. Mukasey at ¶37, in *In re* National Security Agency Telecommunications Records Litigation, MDL Dkt. No. 06-1791-VRW (N.D. Cal. Sept. 19, 2008) [hereinafter 2008 Mukasey Declaration], *available at* http://www.dni.gov/files/documents/0505/AG%20Mukasey%202008%20Declassified%20Declaration.pdf [http://perma.cc/ZZS9-YCLF]. *See also* PCLOB REPORT, *supra* note 2, at 17.

49. 2008 Mukasey Declaration, *supra* note 48, at ¶38.

vided for newly discovered telephone numbers and e-mail addresses to be added in advance of the court order, the intelligence agency expressed concern that the alteration and additional administrative burden was creating an "intelligence gap."[50] Simultaneously, a parallel effort appears to have been underway to compel private U.S. companies to turn over communications of individuals suspected of terrorist activities located overseas.[51] Subject to traditional FISA, a backlog in applications appears to have developed.[52]

Accordingly, 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.

### *C. The Protect America Act*

Four months after McConnell's proposal, Congress passed the Protect America Act (PAA), easing restrictions on the surveillance of foreigners where one (or both) parties were located overseas.[53] In doing so, it removed such communications from FISA's definition of "electronic surveillance," narrowing the term to include only domestic communications. The attendant restrictions, such as those related to probable cause that the target be a foreign power or an agent thereof, or likely to use the facilities to be placed under surveillance, or specifications related to the facility in question, dropped away.

---

50. PCLOB REPORT, *supra* note 2, at 18.

51. There is some confusion in the public literature about the programs underway. While the Draft IG report refers only to a foreign content order and a domestic content order, the PCLOB Report does not mention the domestic content order, instead discussing the Foreign Telephone and Email Orders and a parallel project, using traditional FISA to compel private companies to assist in obtaining the communications of individuals overseas, suspected of engaging in international terrorism, and using U.S.-based communication service providers. *Compare* WORKING DRAFT, *supra* note 19, at 42, *with* PCLOB REPORT, *supra* note 2, at 17–18.

52. PCLOB REPORT, *supra* note 2, at 17–18. *See* William C. Banks, *Responses to the Ten Questions*, 35 WM. MITCHELL L. REV. 5007, 5012 (2009) ("[A] different FISC judge decided in May 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 are subject to individualized FISA processes. After a backlog of FISA applications developed, the Bush administration successfully persuaded Congress to pass statutory authorization for the program.").

53. Protect America Act of 2007, Pub. L. No. 110-55, § 2, 121 Stat. 552 (2007).

The PAA removed FISC from supervising the interception of communications that began or ended in a foreign country (outside of the international communications of individuals targeted under traditional FISA for surveillance). Instead, the Attorney General and the Director of National Intelligence could authorize, for up to one year, the acquisition of communications "directed at" persons reasonably believed to be outside the United States, where five criteria were met: (1) 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 (it did not involve solely domestic communications); (3) The acquisition involved obtaining the communications data from or with the assistance of a communications service provider who had access to communications; (4) A significant purpose of the acquisition was to obtain foreign intelligence information; and (5) Minimization procedures outlined in FISA would be used.[54]

It therefore became easier to establish that the target was located outside the United States. No individualized showing to the court was required. Instead, the presence of reasonable procedures to ascertain the location of the person would suffice. Whether or not an individual could be placed under surveillance turned on geography, not on whether the target was a foreign power, or an agent of a foreign power, as was previously required by FISA for electronic surveillance as defined under FISA.

The PAA required the Attorney General to submit targeting procedures to FISC and to certify that the communications to be intercepted were not purely domestic in nature.[55] Once certified, FISC was required to grant the order.[56] The statute gave immunity to service providers for providing information, facilities, or assis-

54. *Id.*

55. *Id.* at § 3.

56. *Id.* 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, incidents of noncompliance with FISC-approved procedures, and the numbers of certifications or directives issued during the reporting period. *Id.*

tance to the government in its exercise of authority under the PAA.[57]

Efforts by a telecommunications company to challenge the statute on Fourth Amendment grounds later failed.[58] FISC held that while the service provider had standing, the PAA, as applied, satisfied the Fourth Amendment's reasonableness requirement.[59]

Intended to operate for six months, the PAA expired in February 2008, when the executive and legislative branches reached an impasse over whether retroactive immunity should be extended to businesses implicated in TSP.[60] Cases attempting to hold private industry responsible began to make their way through the courts.

### *D. The FISA Amendments Act*

After months of deadlock, Congress finally agreed to provide telecommunications companies with blanket, retroactive immunity.[61] In July, 2008, the legislature enacted the FISA Amendments

---

57. *Id.* at § 6 ("Notwithstanding any other law, no cause of action shall lie in any court against any person for providing any information, facilities, or assistance in accordance with a directive under this section.").

58. *See In re* Directives Pursuant to § 105b of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1009-16 (FISA Ct. Rev. 2008).

59. *Id.*

60. Various bills were proposed in the interim. *See, e.g.*, FISA Amendments Act of 2008, S. 2248, 110th Cong. (2007).

61. A number of Members opposed the final bill because of its inclusion of retroactive immunity. The issue was a pressing one, since more than 40 lawsuits had been filed against telecommunications providers. 154 CONG. REC. S6426 (daily ed. July 8, 2008). Attendant concerns included the constitutionality of the President's Surveillance Program, separation of powers concerns (whether the legislature could preempt the courts and strip them of jurisdiction and the impact of doing so on the rule of law), and the failure of Congress to construct an alternative remedy, as well as whether the vote on retroactive immunity could, in essence, be delegated to a minority of the whole. *See, e.g.*,154 CONG. REC. H5740 (daily ed. June 20, 2008) (statement of Rep. McGovern); 154 CONG. REC. H5773 (daily ed. June 20, 2008) (statement of Rep. Blumenauer) ; 154 CONG. REC. H5773, H5763 (daily ed. June 20, 2008) (statements of Rep. Nadler); 154 CONG. REC. H5762 (daily ed. June 20, 2008) (statement of Rep. Lofgren); 154 CONG. REC. H5768 (daily ed. June 20, 2008) (statement of Rep. Inselee); 154 CONG. REC. 5769 (daily ed. June 20, 2008) (statement of Rep. Conyers); 154 CONG. REC. H5771 (daily ed. June 20, 2008) (statement of Rep. Eshoo); 154 CONG. REC. H5772 (daily ed. June 20, 2008) (statement of Rep. Levin); 154 CONG. REC. H5773 (daily ed. June 20, 2008) (statement of Rep. Dingell); 154 CONG. REC. H5773 (daily ed. June 20, 2008) (statement of Rep. Hall); 154 CONG. REC. S6410-6413 (daily ed. July 8, 2008) (statements of Sens. Specter & Whitehouse); 154 CONG. REC. S6424-S6425 (daily ed. July 8, 2008) (statement

Act (FAA).[62] The statute was hailed as a bipartisan solution to the tension among new technologies, the protection of civil rights, and the preservation of U.S. national security.[63] Codified as Title

---

of Sen. Levin). *But see* 154 CONG. REC. H5773 (daily ed. June 20, 2008) (statement of Rep. Boswell); 154 CONG. REC. S6416 (daily ed. July 8, 2008) (statement of Senator Warner); 154 CONG. REC. S6425 (daily ed. July 8, 2008) (statement of Sen. Chambliss) (explicitly supporting the FAA on immunity grounds).

The bill passed the House on June 20, 2008. Final Vote Results for Roll Call 437, H.R. 6304, FISA Amendments Act of 2008, June 20, 2008, *available at* http://clerk.house.gov/evs/2008/roll437.xml [http://perma.cc/DM2P-JCCH]. But the issue of retroactive immunity continued to dog the proceedings. Senators Russ Feingold and Chris Dodd blocked the bill via filibuster June 26, 2012, delaying a vote until after the July 4, 2012 recess. *Senators Block Consideration of Wiretap Bill*, CNN, June 26, 2008, http://www.cnn.com/2008/US/06/26/senate.fisa/ [http://perma.cc/2X3Q-DJKV]. (Feingold objected on grounds of the violation of civil liberties; Dodd's objections centered on constitutional questions and the impact of retroactive immunity on the rule of law. *Id.*) On July 8, 2008, Senator Specter unsuccessfully offered an amendment altering the liability protections to require the district court to assess the constitutionality of the President's warrantless wiretapping program before cases against telecommunications companies could be dismissed. 154 CONG. REC. S6410-S6412 (daily ed. July 8, 2008) (statement of Senator Specter). Senator Dodd offered an amendment to strike the immunity provisions altogether; however, the Senate rejected the amendment 66 to 32. 154 CONG. REC. S6427 (daily ed. July 8, 2008) (introducing the amendment) and U.S. Senate Roll Call Votes, 110th Cong., 2nd Sess., July 9, 2008, *available at* http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=110&session=2&vote=00164 [http://perma.cc/ANP9-H5HP] (Senate voting against the amendment). Three hours later, the Senate voted on (and passed) the FAA 69 to 28. U.S. Senate Roll Call Votes 110th Cong., 2nd Sess., July 9, 2008, *available at* http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=110&session=2&vote=00168 [http://perma.cc/KR4R-WMC7].

The Ninth Circuit subsequently found the immunity granted to telecommunications companies to be constitutionally sufficient with regard to the legislative process followed, nondelegation doctrine, independent decision-making authority of the courts, and due process. In re National Security Agency Telecommunications Records Litigation, 671 F.3d 881 (9th Cir. 2011), *affirming in part and reversing in part In re* National Security Agency Telecommunications Records Litigation, 633 F. Supp. 2d 949 (N. D. Cal. 2009, *reconsideration denied by* In re National Security Agency Telecommunications Records Litigation, No. 06-1791, 2009 WL 2171061 (N.D. Cal. July 20, 2009).

62. FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (2008).

63. *See, e.g.*, 154 CONG. REC. H5739 (daily ed. June 20, 2008) (statement of Rep. Arcuri) (commending majority leader Mr. Hoyer, Minority Whip Blunt, Chairman Reyes, and others, for reaching bipartisan and bicameral agreement on FISA and noting that the legislation is the result of several months of deliberation between the House and the Senate, Democrats and Republicans, and Congress and the White House); 154 CONG. REC. H5739 (daily ed. June 20, 2008) (statement of Rep. Hastings) (noting the bipartisan nature of the bill and underscoring the importance of updating FISA for current technologies: "This bill is not perfect, but it

VII of FISA, the legislation strengthened and weakened protections for U.S. persons' international communications. A brief discussion of the three most important statutory provisions added by the FAA (FISA Sections 702, 703, and 704) helps to establish a basis for subsequent analysis of PRISM and upstream collection.

### *1. Section 702*

FISA Section 702 empowers the Attorney General (AG) and the Director of National Intelligence (DNI) 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."[64] Five limitations apply. Acquisition may not intentionally (a) target a person known to be located in the United States;[65] (b) target an individual reasonably believed to be located outside the United States, if the actual purpose is to target an individual reasonably believed to be located in domestic bounds;[66] (c) target a U.S. person reasonably believed to be outside domestic bounds;[67] or (d) obtain wholly domestic communications.[68] In addition, (e), all acquisition must be conducted consistent with the Fourth Amendment.[69]

Procedurally, five steps must be followed for acquisition to commence. First, the AG and DNI must adopt targeting and minimization procedures consistent with the statutory requirements.[70]

---

takes vital steps to modernize FISA to reflect 21st century cell phone and Internet technology, and to protect our Nation from today's determined and sophisticated terrorist threats."); Editorial, *A Better Surveillance Law*, WASH. POST, June 20, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/06/19/AR2008061903078.html, [http://perma.cc/GN89-LYMH] ("Congressional leaders of both parties should be commended for drafting legislation that brings the country's surveillance laws into the 21st century while protecting civil liberties and preserving important national security prerogatives.").

64. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 702, 122 Stat. 2436, 2438 (codified as amended at 50 U.S.C. § 1881(a) (2006 & Supp. V 2007-2012)). Except as otherwise noted, § 702 mirrors the definitions adopted in FISA for the terms "agent of a foreign power," "foreign intelligence information," "foreign power," and "person." *Id.*

65. 50 U.S.C. § 1881a(b)(1) (2012).

66. *Id.* § 1881a(b)(2).

67. *Id.* § 1881a(b)(3).

68. *Id.* § 1881a(b)(4).

69. *Id.* § 1881a(b)(5).

70. *Id.* § 1881a(d)–(e).

Second, the two officials must provide FISC with a written certification and any supporting affidavits, attesting that there are procedures in place reasonably designed to ensure that the acquisition is limited to targeting individuals outside of the United States and to prevent the intentional acquisition of domestic communications, and that the minimization procedures meet the requirements of the statute.[71] They must guarantee that guidelines have been adopted to ensure compliance with the statutory limitations.[72] They also must attest that "a significant purpose of the acquisition is to obtain foreign intelligence information."[73] Third, the targeting and minimization procedures must be provided to the Congressional intelligence committees, as well as the Committees on the Judiciary of the Senate and the House of Representatives.[74]

FISC is limited in the role it can play with regard to reviewing the certification, as well as the targeting and minimization procedures. As long as the certification elements are present, the targeting procedures are reasonably designed to ensure that acquisition targets persons are reasonably believed to be outside the United States and do not knowingly intercept domestic communications, the minimization procedures are statutorily consistent, and the procedures are consistent with the Fourth Amendment, "the Court *shall* enter an order approving the certification and the use, or continued use . . . " of an acquisition.[75]

The FAA created numerous reporting requirements. At least twice a year, the Attorney General and DNI must assess compliance with the targeting and minimization procedures and submit the assessments to FISC, House Permanent Select Committee on Intelligence (HPSCI) and the Senate Select Committee on Intelligence (SSCI), and the House and Senate Committees on the Judiciary.[76] The inspectors general of DOJ and the IC agency using Section 702 authorities are authorized to review compliance with

71. *Id.* § 1881a(g)(2)(A)(i)–(ii).

72. *Id.* § 1881a(g)(2)(A)(iii)–(iv).

73. *Id.* § 1881a(g)(2)(A)(v).

74. *Id.* § 1881a(f).

75. *Id.* § 1881(i)(3)(A) (emphasis added). The inclusion of FISC in the process of international intercepts of electronic communications for foreign intelligence purposes departs from previous practice under Executive Order, in which the courts played no role. Thus, having a judicial role created stronger protections; however, the role accorded to FISC was still limited.

76. *Id.* § 1881a(l)(1).

the targeting and minimization procedures, and required to review (a) the number of intelligence reports containing U.S. persons' identities disseminated to other agencies; and (b) the number of targets later determined to be located in the United States.[77] The IG reports are provided to the AG, the DNI, and the same Congressional committees receiving the AG and DNI targeting and minimization reports.[78] In addition, the head of each IC agency obtaining information under Section 702 must annually review the programs to ascertain whether foreign information has been, or will be, obtained from the acquisition.[79] The annual review must also consider the number of intelligence reports disseminated to other agencies containing references to U.S. persons, the number of targets later ascertained to be located within the United States, and a description of any procedures approved by the DNI relevant to the acquisition, the adequacy of the minimization procedures.[80] This review must then be provided to FISC, the Attorney General, the DNI, the Congressional intelligence committees, and the Committees on the Judiciary of the House of Representatives and the Senate.[81] Finally, every six months, the Attorney General must inform the intelligence and judiciary committees of any certifications submitted consistent with Section 702, the reasons for exercising the authority, any directives issued in conjunction with the acquisition, a description of the judicial review during the reporting period of the certifications as well as targeting and minimization procedures (including copies of orders or pleadings submitted in connection with such reviews that contain a significant legal interpretation of the law), any actions taken to challenge or enforce a directive issued, any compliance reviews, and a description of any incidents of noncompliance.[82]

The FAA created an opportunity for telecommunications companies served with orders to challenge the request for information.[83] FISC may only grant such petition where the request for

77. *Id.* § 1881a(l)(2)(A)–(C).
78. *Id.* § 1881a(l)(2)(D).
79. *Id.* § 1881a(l)(3)(A).
80. *Id.*
81. *Id.* § 1881a(*l*)(3)(C).
82. *Id.* § 1881f.
83. *See id.* § 1881a(h)(4)(A) ("An electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition to modify

information is unlawful.[84] Otherwise, the electronic communication service provider must provide the information or risk being held in contempt of court.[85] Either the government or the provider may appeal to the Foreign Intelligence Surveillance Court of Review (FISCR), with final review by the Supreme Court.[86]

### *2. Sections 703 and 704*

Section 702 focused on the targeting of non-U.S. persons abroad. Sections 703 and 704 addressed the targeting of U.S. persons outside of the United States for electronic surveillance and other types of acquisitions. By incorporating these provisions into the statute, Congress departed from previous practice, where the targeting of all persons overseas had been conducted under the auspices of Executive Order 12,333.[87]

As a threshold matter, Section 704 prevents the intelligence community from targeting a U.S. person who is reasonably believed to be outside the country unless FISC or another provision in FISA authorize it to do so.[88] The limit applies where the target of the surveillance has a reasonable expectation of privacy and, if the activity were conducted within the country for law enforce-

---

or set aside such directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.").

84. *See id.* § 1881a(h)(4)(C).

85. *See id.* § 1881a(h)(4)(G).

86. *See id.* § 1881a(h)(6).

87. Exec. Order 12,333, 3 C.F.R. 200 § 2.3 (1982). For discussion of this order, see *infra* Part I.E.

88. 50 U.S.C. § 1881c(a)(2) (2012). ("No element of the intelligence community may intentionally target, for the purpose of acquiring foreign intelligence information, a United States person reasonably believed to be located outside the United States under circumstances in which the targeted United States person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes, unless a judge of the Foreign Intelligence Surveillance Court has entered an order with respect to such targeted United States person or the Attorney General has authorized an emergency acquisition pursuant to subsection (c) or (d), respectively, or any other provision of this chapter.") *See also* EDWARD C. LIU, CONG. RESEARCH SERV., R42725, REAUTHORIZATION OF THE FISA AMENDMENTS ACT 8 (2013) ("As an initial matter, § 704(a)(2) prohibits the intelligence community from targeting a U.S. person who is reasonably believed to be abroad unless authorized by the FISC or another provision of FISA.")

ment purposes, a warrant would be required.[89] Section 704 thus appears to cover physical searches as well as electronic intercepts.[90] As a practical matter, what this means is that where the NSA *knows* a U.S. person is located overseas, *and that person is the target of the intercept*, it may only engage in electronic surveillance (as statutorily defined) consistent with FISA.

The steps outlined in Section 703 apply only to electronic surveillance, or the acquisition of stored electronic communications or data, that would traditionally require an order under FISA if the acquisition were conducted inside the United States.[91] That is, where a U.S. person is located outside the country, and acquisition is to occur inside the country, the government must use Section 703. Where both target and the acquisition are outside the United States, Section 704, whose standards are weaker than those of Section 703, applies.[92]

The procedures to be followed generally reflect the structure employed by traditional FISA with regard to electronic surveillance and physical search. The government must submit an application to FISC identifying the target, as well as the facts and circumstances upon which the government relies for probable cause that the target is a foreign power or an agent thereof.[93] The Court also must ascertain that there is probable cause to believe that the target is located outside the United States.[94]

---

89. 50 U.S.C. § 1881c(a)(2) (2012). *See also* LIU, *supra* note 88, at 8 ("This prohibition only applies in circumstances where the target has a reasonable expectation of privacy and a warrant would be required if the acquisition was conducted in the United States for law enforcement purposes.")

90. The Congressional Research Service explains, "Whether a 'reasonable expectation of privacy' exists depends upon whether an 'individual manifested a subjective expectation of privacy in [a] searched object' and whether 'society is willing to recognize that expectation as reasonable.' Although such a determination is inherently dependent upon the particular circumstances in a given case, it is likely that activities like physical searches and wiretaps conducted on foreign soil would require authorization from the FISC based on the target's 'reasonable expectation of privacy.'" *Id.* (quoting Kyllo v. United States, 533 U.S. 27, 33 (2001)).

91. *See* 50 U.S.C. § 1881b(a)(1) (2012).

92. *See id.* § 1881a(a).

93. *Id.* §§ 1881b(b)–(c), 1881c(b)–(c). There are short-term provisions in the event of emergency situations. Within seven days, the government must make formal application to the court. *Id.* §§ 1881b(d), 1881c(d).

94. *Id.* § 1881c(c).

The central difference between Sections 703 and 704 is that, in certain respects, less specificity is required under the latter.[95] The government need not assert that the information to be obtained cannot be garnered via normal investigative means. Section 704 also requires that FISC approve the minimization procedures only in regard to the *dissemination* of acquired information, as opposed to Section 703, which requires minimization procedures to be applied with regard to both acquisition and retention.[96]

Unlike traditional FISA, which requires that applications identify the facilities to be searched or subject to electronic surveillance, and probable cause that the facilities are or will be used by the target, Sections 703 and 704 have no such equivalent.[97] And unlike Section 702, under Sections 703 and 704 only the government is authorized to appeal the determination of FISC either to FISCR or to the Supreme Court.[98]

### *E. Executive Order 12,333*

In 1978, Congress excluded three types of foreign intelligence collection from FISA: (1) electronic communications *outside* U.S. borders, (2) intelligence in the U.S. and overseas falling outside the statutory definition of "electronic communications," and (3) incidental collection of U.S. persons' communications.[99] HPSCI

---

95. Note, however, that the same standard of probable cause is required.

96. *Compare* 50 U.S.C. § 1881c(c)(1)(C) *with* 50 U.S.C. § 1881b(c)(1)(C).

97. *Compare* 50 U.S.C. § 1801, *with* 50 U.S.C. § 1881a.

98. 50 U.S.C. § 1881b(f) (2012).

99. *See* H.R. REP. NO. 95-1283(I), at 50 (1978) ("[T]his bill does not afford protections to U.S. persons who are abroad, nor does it regulate the acquisition of the contents of international communications of U.S. persons who are in the United States, where the contents are acquired unintentionally. The committee does not believe that this bill is the appropriate vehicle for addressing this area."); S. REP. NO. 95-701, at 7 & n.2, 34–35 & n.16 (1978). In 1978 the definition of "electronic surveillance" limited FISA to four types of collection. First, the acquisition of the contents of any wire or radio communication obtained by "intentionally targeting" a particular, known U.S. person located within domestic bounds. 50 U.S.C. § 1801(f)(1) (2012). Second, the acquisition of the contents of a wire communication to or from someone located in the United States, where the collection takes place on domestic soil. 50 U.S.C. § 1801(f)(2) (2012). Third, the intentional collection of the contents of some radio communications where "the sender and all intended recipients are located within the United States." 50 U.S.C. § 1801(f)(3) (2012). Fourth, the installation and use of other surveillance devices, on U.S. soil, directed at monitoring or acquiring information other than wire or radio communications. 50 U.S.C. § 1801(f)(4) (2012).

explained, "[T]he standards and procedures for overseas surveillance may have to be different than those provided in this bill for electronic surveillance within the United States or targeted against U.S. persons who are in the United States."[100] At the same time, the legislature was careful to hedge. HPSCI noted, at least with regard to intelligence community activities abroad:

> The fact that S.1566 does not bring the overseas surveillance activities of the U.S. intelligence community within its purview . . . should not be viewed as congressional authorization of such activities as they affect the privacy interests of Americans. The committee merely recognizes at this point that such overseas surveillance activities are not covered by this bill.[101]

Instead, the framing for these foreign intelligence collection activities (foreign-to-foreign electronic communications, foreign intelligence collection at home and abroad outside of FISA's definition of "electronic communications," and the incidental collection of U.S. persons' communications) came from Executive Order 12,333.[102] Issued by President Reagan in 1981, this order required each agency to establish procedures, approved by the Attorney General, to govern collection methods.[103]

The order offered heightened protections for U.S. persons. It required that the Attorney General "approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes."[104] Surveillance could only be undertaken where the Attorney General had "determined in each case that there [was] probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power."[105] For the military, for instance, to engage in foreign intelligence collection on U.S. persons, an application to the Attorney General must be made consistent with DOD

---

100. H.R. REP. NO. 95-1283(I), at 50–51 (1978).
101. *Id.*
102. Exec. Order No. 12,333, 3 C.F.R. 200, § 2.4 (1982).
103. *Id.*
104. *Id.* at § 2.5.
105. *Id.*

regulations.[106] Procedures adopted in the early 1980s required that the applicant include a statement of facts demonstrating probable cause and necessity, as well as the period for which surveillance was being sought.[107]

All electronic surveillance had to take place consistent with FISA *and* Executive Order 12,333.[108] The order directed the intelligence community to "use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad."[109] The physical surveillance of U.S. persons overseas for foreign intelligence purposes, in turn, could only be conducted where the purpose was "to obtain significant information" that otherwise could not reasonably be acquired.[110]

The order included institutional protections. It prohibited the CIA from conducting electronic surveillance within domestic bounds (outside of counterintelligence investigations of military personnel).[111] Within the United States, the FBI had the lead, "provided that no foreign intelligence collection by such agencies may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons."[112] And all domestic physical surveillance of U.S. persons had to be undertaken by the FBI.[113]

One of the chief complaints of the Bush Administration that spurred the introduction of the PAA and, subsequently, the FAA, was that changes in telecommunications technologies meant that communications that had previously fallen under the less restrictive contours of Executive Order 12,333 had gradually been brought within FISA. In 2006, the Director of National Intelligence, Admiral Mike McConnell, argued that, as a result, the intelligence community was not collecting some two-thirds of the

106. U.S. Dep't of Def. Dir. 5240.1-R, Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons, Proc. 5, Pt. 2.3 (1982).

107. *Id.*

108. Exec. Order No. 12,333, 3 C.F.R. 200, § 2.5.

109. *Id.* at § 2.4.

110. *Id.* at § 2.4(d).

111. *See id.* at § 2.4(a). The order also excepted searches of non-U.S. person property lawfully in the CIA's possession. *Id.* at § 2.4(b)(2).

112. *Id.* at § 2.3(b).

113. *See id.* at § 2.4(c). But note the exception of government employee-related investigations. *Id.*

foreign intelligence information that it had collected before.[114] Three technology-based arguments helped to drive the demand for FISA reform.[115] The resulting FAA supplanted Executive Order 12,333, in some ways, with a statutory framing. In other ways, it left the existing 12,333 authorities intact. The end result is relevant to analyzing the scope of the FAA and the NSA's programs under Section 702.

*1. Shifting Communications and FISA Modernization*

The arguments put forward in support of modernizing FISA are of varying strength. The strongest claim relates to the nature of e-mail communications.[116] Congress explicitly exempted foreign-to-foreign wire communications from FISA's remit. The exclusion made sense: the voice transmission of a British subject in London, calling a French citizen in Paris, at no point crossed U.S. borders. It would be impractical and cumbersome to expect the intelligence community to obtain court approval for every interception of foreign intelligence between foreign nationals overseas. By grounding the exception in territorial limits, Congress thus acted consistently with Fourth Amendment doctrine—reserving, in the process, the potential to act where U.S. persons' privacy might be at stake.

The same types of communications exempted from FISA, however, in the modern age of e-mail, had begun to fall within traditional FISA. For instance, U.S. Internet Service Providers (ISPs) store e-mail on servers in the United States. The same British subject, if she accesses her email from London (pulling it from a server within the United States), suddenly falls within FISA—even when the e-mail she is retrieving is sent by the same French citizen in Paris. In other words, merely by using an American ISP,

---

114. 158 CONG. REC. H5891 (daily ed. Sept. 12, 2012) (statement of Rep. Smith).

115. David S. Kris & J. Douglas Wilson, National Security Investigations and Prosecutions § 16:3 (2012) [hereinafter Kris & Wilson, NSIAP].

116. *Open/Closed Hearing: FISA Before the S. Select Comm. on Intelligence,* 110th Cong. (2007) (statement of John M. McConnell, Director of National Intelligence); *see also* 154 CONG. REC. H5756–57 (daily ed. June 20, 2008) (Letter from Michael Mukasey, Attorney General, and J.M. McConnell, Director of National Intelligence, to Hon. Nancy Pelosi, Speaker, House of Representatives (June 19, 2008)); 154 CONG. REC. S6400–01 (daily ed. July 8, 2008) (Letter from Michael Mukasey, Attorney General, and J.M. McConnell, Director of National Intelligence, to Hon. Harry Reid, Majority Leader, Senate (July 7, 2008)).

non-citizens could obtain the protections of the more rights-protective FISA framework—even where such persons had no other ties to the United States and presented a classic foreign intelligence threat (and would otherwise be covered by the less rigorous contours of Executive Order 12,333). Exacerbating the problem was the difficulty of determining where the user was located—inside the U.S. or on foreign soil—a consideration crucial to determining whether the intelligence community must first approach FISC for an order.

The other two arguments put forward in support of modernizing FISA were less robust. First, the government argued that the transition from satellite to fiber optic cables for trans-oceanic communications meant that international communications, previously carried by radio waves (exempted from FISA unless the target was a particular, known, U.S. person on domestic soil), began to fall within FISA's wire communications provisions.[117] While accurate in its assertion that fiber optic cable communications came within FISA's remit, it was an exaggeration to say that Congress did not expressly contemplate this in 1978. The Committee explained at the time: "It is the committee's intent that acquisition of the contents of a wire communication, without the consent of any party thereto, would clearly be included" in the definition of "wire communication." It continued, "Excluded would be . . . commercial broadcasts, as well as ham radio and citizen band radio broadcasts."[118] Also exaggerated was the claim that most communications at the time of FISA's enactments were carried on radio waves, as opposed to fiber optic cables.[119] The government further over-emphasized the change in terms of the trend.[120]

Second, the government argued that the difference of a mile or two should not matter with regard to whether the U.S. intercepted communications offshore or within U.S. borders.[121] The intelligence community might need the assistance of a U.S.

---

117. KRIS & WILSON, NSIAP, § 16:3.

118. S. Rep. No. 95-701, at 34 (1978).

119. *See* KRIS & WILSON, NSIAP, § 16:3, citing § 16.4 ("A review of telecommunications history . . . shows this claim to be exaggerated: the transition from satellite to cable was neither as dramatic, nor as unanticipated, as the government argued.").

120. *Id.*

121. For discussion of this point, see KRIS & WILSON, NSIAP, § 16.5.

company. The location of the actual intercept was a matter of accident, not design—and entirely outside the government's control. The location turned on where the company had chosen to concentrate the flow of traffic. So, where previously the wiretap offshore would not trigger the protections of traditional FISA, the same wiretap just inside US borders would—even where the same conversation or communication was being obtained. The problem with this argument is that it was precisely the point of FISA to draw a line at the border of the country. Trying to move that line a matter of feet and call it a day fell short of understanding the point of the statute.

In light of all three arguments, Members of Congress began to focus on the need to "modernize" FISA.[122] The FAA, however, still only reaches electronic communications as defined in FISA. Other forms of foreign intelligence collection continue to be governed by executive order.

### *2. Executive Order 13,470*

Executive Order 12,333 has thrice been amended.[123] The most recent, in July 2008, drew attention to areas outside the traditional foreign intelligence emphasis.[124]

The new order emphasized that intelligence collection should be conducted in a manner consistent with the intelligence priorities set by the President, with "[s]pecial emphasis" given to detecting and countering not just espionage, but "[t]hreats to the

---

122. *See, e.g.*, 154 CONG. REC. S6379 (daily ed. July 8, 2008) (statement of Sen. Cardin) ("Congress must indeed make needed changes to FISA to account for changes in technology and rulings from the FISA Court involving purely international communications that pass through telecommunications routes in the United States."); 154 CONG. REC. H5759 (daily ed. June 20, 2008) (statement of Sen. Blunt) ("We modernized the law to adapt to changes in technology since the 1978 FISA statute. The bill would accomplish all this while adding new protections and strengthening the individual liberties and privacy protections of Americans."); 154 CONG. REC. H5767 (daily ed. June 20, 2008) (statement of Rep. Pelosi) ("[W]e all recognize the changes in technology necessitate a change in the legislation, and this legislation today modernizes our intelligence-gathering system by recognizing and responding to technological developments that have occurred since the original FISA Act in 1978.").

123. Exec. Order No. 13,284, 68 Fed. Reg. 4,075 (Jan. 23, 2003); Exec. Order No. 13,355, 69 Fed. Reg. 53,593 (Aug. 27, 2004); Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (July 30, 2008).

124. Exec. Order No. 13,470, 73 Fed. Reg. 45,325.

United States and its interests from terrorism; and [t]hreats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction."[125] The amendments directed the intelligence community to take into account state, local, and private sector responsibilities and requirements "when undertaking the collection and dissemination of information and intelligence."[126] In addition, the new order incorporated the Director of National Intelligence into the intelligence infrastructure.[127]

Some of the language signaled a shift in how the NSA would be using its authority under the FAA. Where previously the order prohibited the dissemination of unminimized Signals Intelligence (SIGINT) pertaining to U.S. persons, the new order allowed dissemination subject to procedures developed by the DNI in coordination with the Secretary of Defense and approved by the Attorney General.[128] This change enabled other agencies to obtain SIGINT to ascertain whether the information could be kept, at which point it becomes subject to that agency's U.S. person rules (pursuant to the first part of Executive Order 12,333, Section 2.3).[129] The sharing and evaluation of unminimized SIGINT data thus appears to create an internal process that can be thought of as a form of intelligence "discovery." Although the previous order required that intelligence be collected in a manner consistent with the restrictions in FISA and Executive Order 12,333, the amendments only required that information be collected subject to restrictions in FISA.[130] This change made a differ-

---

125. *Id.* at § 2, Pt. 1.1(d).

126. *Id.* at § 2, Pt. 1.1(f).

127. *See id.* at § 2, Pts. 1.3–1.6.

128. *Compare* Exec. Order No. 12,333, 3 C.F.R. 200, § 2.3 (1982), *with* Exec. Order No. 13,470, 73 Fed. Reg. 45,325, § 3(p). The new order replaced all references to "agencies" with "elements," referring to entities with intelligence responsibilities.

129. The relevant DNI/DOD/AG procedures, if they have been developed, have not been declassified.

130. *Compare* Exec. Order No. 12,333, 3 C.F.R. 200, § 2.5 ("Electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be conducted in accordance with that Act, as well as this Order."), *with* Exec. Order No. 13,470, 73 Fed. Reg. 45,325, § 3(y) (deleting sentence quoted in prior citation and replacing with: "The authority delegated pursuant to this paragraph, including the authority to approve the use of electronic surveillance as defined in the Foreign Intelligence Surveillance Act of 1978, as amended, shall be exercised in accordance with that Act.").

ence. The FAA, for instance, amended FISA to allow for U.S. person data to be retained to protect life and property, and for the NSA to retain encrypted communications. Under Executive Order 12,333's more general guidelines, these practices would not have been allowed; however, they appear now to fall within the scope of intelligence agencies' authorities.

Some of the regulations implementing Executive Order 12,333 have been made publicly available.[131] But many of the guidelines, and the programs conducted under the order, remain veiled from public scrutiny. Even Congress has limited view. Although the procedures approved by the Attorney General under the order must be provided to the Congressional intelligence committees,[132] SSCI Chairman, Senator Dianne Feinstein, has acknowledged that the committee does not conduct extensive oversight of intelligence gathering conducted under the order's auspices.[133]

The Snowden documents provide some detail on different ways in which the order appears to be interpreted and used. Accessing social network data or stored information (for example, address book contacts, "buddy lists," and draft e-mails) may fall within Executive Order 12,333, insofar as FISA does not apply.[134]

---

131. *See, e.g.* U.S. Dep't of Justice, Federal Bureau of Investigation, The Attorney General's Guidelines for Domestic FBI Operations (Sept. 29, 2008), *available at* http://www.usdoj.gov/ag/readingroom/guidelines.pdf [http://perma.cc/G8XH-UMRY]. A Fact Sheet explaining the new Domestic Operations Guidelines is available at: http://www.usdoj.gov/opa/pr/2008/October/08-ag-889.html [http://perma.cc/X5HC-ZAVM] (addressing the FBI's primary investigative activities within the United States related to law enforcement, counterintelligence, and collection of foreign intelligence). For a thoughtful discussion of how these guidelines differ from their predecessors see Kris & Wilson, NSIAP, §§ 2.16–2.18.

132. Exec. Order No. 12,333, 3 C.F.R. 200, § 3.3.

133. Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST, Oct. 30, 2013, *available at* http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html [http://perma.cc/JR36-2V45]. Kris & Wilson note that there is an additional statutory requirement that the President keep the congressional intelligence committees "fully and currently informed of the intelligence activities of the United States." *See* 50 U.S.C. § 413 (2012). They point out, however, that the Bush Administration made concerted efforts to protect what was seen as the President's inherent constitutional authorities with regard to foreign affairs—including not informing Congress of certain activities. *See generally* KRIS & WILSON, NSIAP, § 2.7.

134. For slides detailing collection of this data and released by Edward Snowden, see Barton Gellman & Matt DeLong, *The NSA's Problem? Too Much Data*,

For example, Section 703 applies to stored electronic data acquired in the United States in the process of targeting U.S. persons overseas. It would thus cover the acquisition of U.S. persons' buddy lists on U.S. soil.[135] FISA would not, however, govern the overseas acquisition of buddy lists of non-U.S. persons located abroad. This acquisition would come within Executive Order 12,333. Similarly, to the extent that social network information, such as Instagram postings, fall outside FISA's definition of electronic surveillance or stored communications, regardless of whether a U.S. person is located inside or outside the country, collection would be governed by the weaker restrictions of Executive Order 12,333.

These other types of programs can potentially yield significant amounts of information. The NSA appears to be collecting e-mail address books for most major webmail companies, and storing the information in multiple databases.[136] According to the *Washington Post*, the yield is "hundreds of millions of contact lists from personal e-mail and instant messaging accounts around the world."[137] On any representative day, in turn, the NSA appears to collect approximately half a million buddy lists and inboxes (which frequently include the first part of the messages that have been sent).[138]

Another example of collection under Executive Order 12,333 is the interception of content flowing between data centers overseas. In October 2013, the *Washington Post* reported that the NSA was collecting hundreds of millions of records, ranging from metadata to content, transiting fiber optics cables between Google and Yahoo data centers.[139] The principal tool used to analyze the infor-

---

WASH. POST, *available at* http://apps.washingtonpost.com/g/page/world/the-nsas-overcollection-problem/517/#document/p4/a126384 [http://perma.cc/PG4G-FRH8].

135. *See* FISA Amendments Act of 2008, Pub. L. No. 110-261, § 703(a), 122 Stat. 2436, 2448 (codified as amended at 50 U.S.C. § 1881(b) (2012)).

136. *See* Gellman & DeLong, *supra* note 1344, at slide on p. 3. MARINA centers on internet metadata; MAINWAY focuses on telephone metadata for contact chaining; and PINWALE concentrates on written content. *Id.*

137. Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, WASH. POST, Oct. 14, 2013, *available at* http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html [http://perma.cc/3FQX-AYST].

138. Gellman & DeLong, *supra* note 134, at slide on p. 4.

139. Gellman & Soltani, *NSA Infiltrates Links*, *supra* note 133.

mation, MUSCULAR, appears to be operated jointly with the U.K.'s Government Communications Headquarters (GCHQ).[140] The collection of information held on the cloud, outside U.S. borders, shifts the program outside the FISA framework.[141]

With GCHQ in mind, it is worth noting an additional exception to both FISA and Executive Order 12,333: to the extent that it is not the United States engaged in the collection of information, but, rather, one of our allies, rules that otherwise limit the U.S. intelligence community may not apply. From the language of the order, it appears that the United States may *receive* or *benefit from* other countries' collection of information on U.S. citizens, where it does not actively participate in the collection or specifically request other countries to carry out the collection at its behest.[142] In turn, the United States can provide information about foreign citizens to their governments that their intelligence agencies, under their domestic laws, might otherwise be unable to collect. To the extent that the programs underway are extended to the closely allied "Five Eyes" (Australia, Canada, the United Kingdom, the United States, and New Zealand), structural demarcations offer a way around the legal restrictions otherwise enacted to protect citizen rights in each region.

## II. PROGRAMMATIC COLLECTION[143]

Almost immediately after passage of the FAA, members of Congress, scholars, and others began criticizing Section 702 be-

---

140. *Id.*

141. *Id.*

142. The order states with regard to indirect participation, "No element of the Intelligence Community shall participate in or request any person to undertake activities forbidden by this Order." Exec. Order No. 12,333, 3 C.F.R. 200, § 2.12 (1982), as amended by Exec. Order No. 13,470, 73 Fed. Reg. 45,325, § 3(ii) (July 30, 2008). This prohibits the intelligence community from actively participating in collection, or requesting other countries to engage in collection, outside the confines of the order; however, it does not appear to prohibit the intelligence community from simply receiving or benefiting from other countries' actions in this regard.

143. By "programmatic collection" I refer to a method of collection involving indiscriminate surveillance. The scanning of e-mail communications for reference to selectors, targets, or key words, is thus programmatic. It is not limited to the communications of particular individuals but, rather, monitors the communications of all individuals passing through particular points.

cause of the potential for the government to use the authorities to engage in programmatic surveillance.[144]

In 2009 prominent national security law Professor William Banks explained, "the FAA targets do not have to be suspected of being an agent of a foreign power or, for that matter, they do not have to be suspected of terrorism or any national security offense, so long as the collection of foreign intelligence is a significant purpose of the surveillance."[145] Surveillance could be directed at a person, organization, e-mail address, or even "an entire ISP or area code."[146] He noted, "the surveillance permitted under the FAA does not require that the Government identify a particular known facility where the intercepted communications occur."[147] These provisions represented a sea change from how FISA had previously worked (albeit introducing, for the first time, statutory restrictions in an area previously governed by Executive Order). U.S. persons' communications now could be incidentally collected under the statute, on a large scale, without many of the protections in traditional FISA.[148]

Banks presciently pointed out the most likely way in which the new authorities would be used:

> Although details of the implementation of the program . . . 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 the NSA engages in a more particularized collection of content after analyzing mined data . . . [A]ccidental or incidental acquisition of U.S. persons inside the United States [will] surely occur[], especially in light of the difficulty of ascertaining a target's location.[149]

For Professor Banks, part of the problem was that the nature of international information flows meant that it would be impossible

144. *See, e.g.*, Banks, *supra* note 52.
145. *Id.* at 5013–14.
146. *Id.*
147. *Id.*
148. *Id.* at 5014.
149. *Id.* at 5014–15.

to tell if an individual is located overseas or within domestic bounds.[150]

Banks was not the only one to question the implementation of Section 702. Cases began to appear, raising facial and as applied constitutional challenges. Problems characteristic of relying on Article III courts in the context of surveillance came to the fore. In *Clapper v. Amnesty International*, plaintiffs alleged that Section 702 violated the targets' Fourth Amendment rights because it allowed for the acquisition of international communications absent an individualized court order supported by probable cause.[151] The Supreme Court dismissed the suit for lack of standing—that is, the absence of any concrete injury. It did not reach the merits of the Fourth Amendment claim.[152]

The FAA was set to expire at the end of 2012. By early February, James Clapper, the Director of National Intelligence, and Attorney General Eric Holder had informed Congressional leaders that reauthorization of the FAA was "the top legislative priority of the national Intelligence Community." [153] The Administration credited the FAA with the production of "significant intelligence that is vital to protect the nation against international terrorism

150. *Id.* at 5015. In another article, he laid out guidelines for reform: Namely, that any applications for programmatic surveillance be based on a demonstration that the proposed information collection is material to specific counterterrorist or intelligence investigations, that alternative techniques are not available, and that it is likely that the program will generate the necessary information. Banks, *supra* note 17, at 1637. Higher protections for personally identifiable information, and its dissemination, and FISC review of the programs for First and Fourth Amendment implications proved equally important. Banks, *supra* note 17, at 1637.

151. 133 S. Ct. 1138 (2013).

152. *Id.*

153. Letter from DNI James Clapper and AG Eric Holder to John Boehner, Speaker of the House; Harry Reid, Majority Leader, U.S. Senate; Nancy Pelosi, Democratic Leader, U.S. House of Representatives, Mitch McConnell, Republican Leader, U.S. Senate (Feb. 8, 2012), *available at* http://www.intelligence.senate.gov/pdfs112th/dni_ag_letter.pdf [http://perma.cc/24FR-BEJ3]. This statement resurfaced repeatedly over the next six months. *See, e.g.*, Letter from Kathleen Turner, Director of Legislative Affairs ODNI and Ronald Weich, Assistant Attorney General Office of Legislative Affairs, DOJ, to Dianne Feinstein, Chair, and Saxby Chambliss, Vice Chair, Senate Select committee on Intelligence, (May 4, 2012), *available at* http://www.dni.gov/files/documents/Ltr%20to%20HPSCI%20Chairman%20Rogers%20and%20Ranking%20Member%20Ruppersberger_Scan.pdf [http://perma.cc/9PDN-P9MC] (writing that reauthorization of the FAA was "the top legislative priority of the Intelligence Community.").

and other threats."[154] Offering classified briefings and attaching an unclassified annex, Clapper and Holder wrote, "We are always considering whether there are changes that could be made to improve the law in a manner consistent with the privacy and civil liberties interests of Americans."[155] But their "first priority" was "reauthorization of these authorities in their current form."[156]

The NSA's inability to provide the number of American citizens' communications intercepted under the act became a matter of public debate. In May 2012 Senators Ron Wyden and Mark Udall raised concerns about what they referred to as a "back door" in the statute.[157] In June 2012 SSCI noted numerous senators' concern about the IC's inability to provide an estimate of the number of individuals whose communications had been intercepted.[158] Attention was further drawn to the lack of information about whether the NSA had attempted to search Americans' communications without a warrant.[159] By the end of July 2012, more than a dozen senators had joined a letter to Director of National Intelligence James R. Clapper, expressing alarm "that the intelligence community has stated that 'it is not reasonably possible to identify the number of people located inside the United

---

154. *Id.*

155. *Id.*

156. *Id.*

157. On May 4 2012, Senators Wyden and Udall wrote a letter to the Inspector General (IG) of the NSA as well as the IG of the Intelligence Community, requesting an estimate of "how many people inside the United States have had their communications collected or reviewed under the authorities granted by § 702[?]" Letter from Ron Wyden, U.S. Sen. and Mark Udall, U.S. Sen. to IG of the Intelligence community (May 4, 2012), *available at* http://www.wyden.senate.gov/download/?id=ce360936-dff9-4273-8777-09bf29565086&download=1 [http://perma.cc/LAJ7-XT3Y] (note that this letter was sent May 4, 2012 but incorrectly dated May 4, 2011). I. Charles McCullough responded, "The NSA IG provided a classified response on June 6, 2012. I defer to his conclusion that obtaining such an estimate was beyond the capacity of his office and dedicating sufficient additional resources would likely impede the NSA's mission." Letter from I. Charles McCullough, III, Inspector General of the Intelligence Community, to Senators Wyden and Udall, (June 15, 2012), *available at* http://www.wired.com/images_blogs/dangerroom/2012/06/IC-IG-Letter.pdf [http://perma.cc/WG7V-7EXT].

158 S. REP. NO. 112-174 (2012), *available at* https://www.fas.org/irp/congress/2012_rpt/faa-extend.html [http://perma.cc/3PDP-DRDT].

159. *Udall Calls on Intelligence Director to Provide Answers before Senate Debate on FISA Amendments Act*, MARK UDALL (July 26, 2012), http://www.markudall.senate.gov/?p=press_release&id=2586 [http://perma.cc/SDM2-3K25].

States whose communications may have been reviewed' under the FAA.'"[160]

These concerns did not stop the legislation from progressing. Congress did not hold any hearings on the renewal bill.[161] Efforts to amend the legislation failed.[162] On September 12, 2012, with minimal debate, the House voted to reauthorize the FAA 301-118.[163] The Senate passed the bill at the end of December 2012, 73 to 23.[164] President Obama signed the legislation, extending the FAA until Dec. 31, 2017.[165]

Six months later, the Snowden documents again forced Section 702 into the public discussion. The information that has since emerged raises statutory and constitutional concerns with regard to three areas: targeting, post-targeting analysis, and the use and dissemination of information.

---

160. Letter from thirteen Senators to James R. Clapper, Dir. of Nat'l Intelligence, July 26, 2012, *available at* http://www.wyden.senate.gov/download/letter-to-dni [http://perma.cc/33AY-ZG4F]. *But see* S. Rep. No. 112-174, at 8–9 (2012), *available at* https://www.fas.org/irp/congress/2012_rpt/faa-extend.html [http://perma.cc/X9U7-NPSE] (Senator Feinstein writing, "During the Committee's consideration of this legislation, several Senators expressed a desire to quantify the extent of incidental collection under section 702. I share this desire. However, the Committee has been repeatedly advised by the ODNI that due to the nature of the collection and the limits of the technology involved, it is not reasonably possible to identify the number of people located in the United States whose communications may have been reviewed under section 702 authority. Senators Ron Wyden and Mark Udall have requested a review by the Inspector General of the NSA and the Inspector General of the Intelligence Community to determine whether it is feasible to estimate this number. The Inspectors General are conducting that review now, thus making an amendment on this subject unnecessary.")

161. 158 CONG. REC. H5892, (daily ed. Sept. 12, 2012) (statement of Rep. Nadler); 158 CONG. REC. H5895 (daily ed. Sept. 12, 2012) (statement of Rep. Johnson of Georgia) (stating that the Judiciary Committee held no hearings).

162. Sen. Jeff Merkeley of Oregon unsuccessfully proposed an amendment that would have required FISC to disclose "important rulings of law." Ron Wyden proposed an amendment that would have required the government to estimate the number of US citizens whose communications had been intercepted.

163. 158 CONG. REC. H5900-5901, (daily ed. Sept. 12, 2012). The debate took only 11 pages of the Congressional Record. *See id.* at H5900-H5910.

164. 158 CONG. REC. S8461, (daily ed. Dec. 28, 2012). *See also,* U.S. Senate Roll Call Votes 112th Cong., 2nd Sess., Dec. 28, 2012, *available at* http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=112&session=2&vote=00236 [http://perma.cc/QWE9-P336].

165. FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238. 126 Stat. 1631 (2012).

### *A. Targeting*

As aforementioned, Section 702 places four limitations on acquisition, each of which is meant to restrict the amount of information that can be obtained by the government.[166] The NSA has sidestepped these statutory restrictions in three important ways: first, it has adopted procedures that allow analysts to acquire information "about" selectors (that is, communications modes used by targets) or targets, and not merely communications to or from targets (or selectors employed by targets), or information held by targets themselves. Second, it has created a presumption of non-U.S. person status: That is, if an individual is not known to be a U.S. person (and thus exempted from Section 702 and treated either under Sections 703 and 704 or under traditional FISA, depending on the location), then the NSA assumes that the individual is a non-U.S. person. Third, the NSA has failed to adopt standards that would require it to ascertain whether a target is located within domestic bounds. Instead, the agency, having looked at the available evidence, absent evidence to the contrary, assumes that the target is located outside the United States. These interpretations work together to undermine Congress's addition of Sections 703 and 704, even as they open the door to more extensive collection of domestic communications.

In 2008 Congress anticipated that U.S. person information would inadvertently be collected under Section 702. This is in part why it included minimization procedures, as well as limits on what could be collected. Most Members, however, do not appear to have contemplated broad, programmatic collection that would undermine protections introduced in Sections 702 and 703.[167] Those who did articulate this possibility voted against the bill.

---

166. 50 U.S.C. § 1881a(b)(1)–(4) (2012). The government may not (a) target individuals known to be in the United States, (b) engage in reverse targeting (that is, target someone outside the U.S. where the purpose is to acquire information about a particular person known to be in the U.S.), (c) target a U.S. person reasonably believed to be outside the country, or (d) intentionally target domestic communications. The statute also requires that acquisition be performed in a manner consistent with the Fourth Amendment. *Id.*

167. Although it could be argued that, in light of TSP, Members should have anticipated the potential for programmatic collection, it is important to recognize that at the time the 2008 FAA was introduced, many Members still had very little information about the extent of the previous programs. It was on these grounds

Even if Congress did not initially appreciate the potential for programmatic collection, however, certainly by 2012 the intelligence community had made enough information available to Congress for Members to make an informed decision. This does not mean that all Members were fully informed. But to the extent that Members selected not to access the material or to take a public stand on the matter, particularly in light of the legislature's reading of its authorities with regard to classification, fault lies with Congress.

The Foreign Intelligence Surveillance Court failed to step into the gap. In 2011, FISC realized the implications of the NSA's interpretation of to, from or about (TFA) collection. However, in light of the seriousness of the NSA's aim (protecting national security), and the limitations imposed by the types of technologies being used, the Court read the statute in a manner that found the targeting procedures to be consistent with the statute.

To the extent that NSA's TFA and assumptions regarding the target's foreignness undermine the law as it is written, the legislature failed to perform effective oversight. Congress similarly neglected to uphold the limit placed on the intelligence community to not knowingly collect domestic conversations. Instead, it relied on FISC to do so—a task that the Court failed to do. In a classified environment, when so much information is cloaked from public view, it becomes even more important for the government to ensure that the authorities as they are publicly presented are consistent with the manner in which they are being exercised.

### *1. Information To, From, and About Targets*

The FAA focuses on acquisition with reference to the status and location of the target. It is silent on the relationship between the target and the information (whether only information held by the target, or communications to which the target is a party, may be obtained). In the absence of explicit language, the NSA has interpreted Section 702 to enable the agency to obtain information "about" targets.

The NSA's 2009 targeting procedures state that the agency may seek "to acquire communications about the target that are not to

---

that Members objected to granting retroactive immunity to telecommunications companies. *See generally*, 154 CONG. REC. H5740-5773 (daily ed. June 20, 2008).

or from the target."[168] The minimization procedures similarly acknowledge the collection of information related to entities of interest.[169] They explain, "As communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication *to, from, or about a target* and is reasonably believed to contain foreign intelligence information or evidence of a crime."[170] The 2011 minimization procedures retain this focus.[171]

In implementing the procedures, the NSA draws a distinction between PRISM and upstream collection. In the context of the former, the NSA states that it only collects information to or from a target using selectors linked to that individual. It does not collect communications that are merely "about" a selector (and, by implication, a target).[172] The leaked targeting procedures, however, make no such distinction between PRISM and upstream collec-

---

168. NSA TARGETING PROCEDURES, *supra* note 16, at 1.

169. Nat'l Sec. Agency/Cent. Sec. Serv., Exhibit B: 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 (2009) *available at* http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document [http://perma.cc/F226-ASQ3] [hereinafter 2009 MINIMIZATION PROCEDURES].

170. *Id.* § 3(b)(4) (emphasis added). *But see* Nat'l Sec. Agency, NSA Director of Civil Liberties and Privacy Office Report: NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, (2014), *available at* http://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf [http://perma.cc/4TMV-Y55S] [hereinafter NSA'S IMPLEMENTATION REPORT] (stating that to, from, or about collection occurs during what "has generally been referred to as Upstream collection" and employs not keywords or particular terms, but communications modes, such as e-mail addresses or telephone numbers).

171. *See, e.g.*, regarding segregated upstream collection information: Nat'l Sec. Agency/Cent. Sec. Serv., Exhibit B: Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended § 3(b)(4) (2011), *available at* http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf [http://perma.cc/LKY3-J7CR] [hereinafter 2011 MINIMIZATION PROCEDURES] ("As a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime."); *Id.* at 3–4 ("NSA analysts seeking to use . . . a discrete communication within an Internet transaction that contains multiple discrete communications will assess whether the discrete communication . . . is to, from, or about a tasked selector").

172. PCLOB HEARING, *supra* note 3 at 70. *See also* NSA DCLPO Report, at 5; PCLOB REPORT, *supra* note 2, at 33.

tion, leaving it to the NSA, as a matter of policy, to determine when to apply about collection.[173]

The NSA adopts a different position with regard to upstream collection. The program involves two types of communications: telephone and Internet. For the former, as with PRISM, the government states that it only uses to/from, and not "about" intercepts.[174] Like the decision with regard to PRISM, this appears to be a matter of internal policy. The targeting procedures lay out the steps to be taken when the NSA elects to intercept "communications about the target."

For Internet communications, in contrast, the NSA does acknowledge that it intercepts communications "about" selectors. [175] The Privacy and Civil Liberties Oversight Board (PCLOB) explains, "An 'about' communication is one in which the tasked selector is referenced within the acquired Internet transactions, but the target is not necessarily a participant in the communication."[176]

---

173. NSA TARGETING PROCEDURES, *supra* note 16, at 1–2 ("[I]n those cases where NSA seeks to acquire communications about the target that are not to or from the target, NSA will either employ an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas, or it will target Internet links that terminate in a foreign country.")

174. Memorandum Opinion, 2011 WL 10945618, at *5, *cited in* PCLOB REPORT, *supra* note 2 at 36.

175. *See, e.g.*, Memorandum Opinion, 2011 WL 10945618, at *5–6 (discussing the government's representation regarding upstream collection), *cited in* PCLOB REPORT, *supra* note 2, at 37. It is worth noting here a discrepancy: according to the leaked procedures, the NSA may seek to acquire information "about the target." NSA TARGETING PROCEDURES, *supra* note 16, at 1–2. The government currently appears to understand this to mean "about the selector." This may be consistent with subsequent targeting procedures introduced by the NSA and approved by FISC; but the documents that would shed more light on this remain classified. Which of these is accurate carries implications for privacy. It is a very different enterprise for the NSA to intercept communications based on reference to a person (a target), versus reference to a target's telephone number or e-mail.

176. PCLOB REPORT, *supra* note 2, at 37. *See also* Memorandum Opinion, 2011 WL 10945618, at *5; Joint Statement of Lisa O. Manaco, Assistant Attorney General, National Security Division, Department of Justice, et al., Hearing Before the House Permanent Select Comm. on Intelligence: FISA Amendments Act Reauthorization, at 7 (Dec. 8, 2011) (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ), *available at* http://www.dni.gov/files/documents/Joint%20Statement%20FAA%20Reauthorization%20Hearing%20-%20December%202011.pdf [http://perma.cc/XP8U-DRWA]; PCLOB HEARING, *supra* note 3, at 55.

PCLOB's discussion is based in part on classified documents: specifically, a September 2008 FISC opinion in which the court agreed with the government that by collecting information about the selector, the target of the intercept was still the individual associated with the selector.[177] PCLOB noted that FISC had previously relied upon a congressional report to state that the "target" of a traditional FISA order "is the individual or entity . . . about whom or from whom information is sought."[178]

There are numerous grounds on which the government's interpretation of TFA can be challenged. Traditional FISA does not apply to communications "about" targets. The legislation is specific about the facilities to be placed under surveillance, requiring that the government establish probable cause that the target will actually be using such facilities. The 2002 FISCR opinion cited by PCLOB, moreover, pre-dated the introduction of Section 702. In addition, the court's reference to information about the target was *dicta*, and not central to the decision, which related instead to whether the primary purpose of the investigation for which information was sought could be criminal in nature. Without being able to read the 2008 FISC opinion, which presumably focused on the inclusion of "about," it is difficult to further assess the strength of the government's argument and the court's response.

What is clear is that the inclusion of "about" communications significantly expands the volume of Internet intercepts under Section 702. By 2011, NSA was acquiring approximately 26.5 million Internet transactions per year as part of its upstream collection.[179]

Three points related to the volume and intrusiveness of the resulting surveillance deserve notice. First, to obtain "about" communications, because of how the Internet is constructed, the NSA must monitor large amounts of data.[180] That is, if the NSA may

---

177. PCLOB REPORT, *supra* note 2, at 37.

178. *In re* Sealed Case, 310 F.3d 717, 740 (FISA Ct. Rev. 2002) (quoting H.R. Rep. 95-1283, at 73 (1978); *see also* PCLOB March 2014 Hearing Transcript, at 55 (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ) (confirming that FISC held that targeting includes communications about a particular selector that are not necessarily to or from that selector). Cited in PCLOB REPORT, *supra* note 2, at 38, note 137.

179. Memorandum Opinion, 2011 WL 10945618, at *26.

180. *See also* Charlie Savage, *NSA Said to Search Content of Messages to and From U.S.*, N.Y. TIMES, Aug. 8, 2013, http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?ref=todayspaper&pagewanted=all&_

collect not just e-mail to or from the target's e-mail account (badguy@ISP.com), but, in addition, other communications happening to mention badguy@ISP.com that pass through the collection point, then the NSA is monitoring a significant amount of traffic. And the agency is not just considering envelope information (for example, messages in which the selector is sending, receiving, or copied on the communication) but the actual content of messages.[181]

Second, wholly domestic conversations may become swept up in the surveillance simply by nature of how the Internet is constructed. Everything one does online involves packets of information. Every Web site, every e-mail, every transfer of documents takes the information involved and divides it up into small bundles. Limited in size, these packets contain information about the sender's IP address, the intended receiver's IP address, something that indicates how many packets the communication has been divvied up into, and what number in the chain is represented by the packet in question.[182]

Packet switched networks ship this information to a common destination via the most expedient route—one that may, or may not, include the other packets of information contained in the message. If a roadblock or problem arises in the network, the packets can then be re-routed, to reach their final destination. Domestic messages may thus be routed through international servers, if that is the most efficient route to the final destination.

What this means is that even if the NSA applies an IP filter to eliminate communications that appear to be within the United States, it may nevertheless monitor domestic conversations by nature of them being routed through foreign servers. In this manner, a student in Chicago may send an e-mail to a student in Bos-

---

r=0 [http://perma.cc/W94H-VFN6] (discussing to, from, or about collection and noting, "To conduct the surveillance, the N.S.A. is temporarily copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border.").

181. *See, e.g.*, PCLOB REPORT, *supra* note 2, at 38 ("The NSA cannot, however, distinguish in an automated fashion between 'about' communications that involve the activity of the target from communications that, for instance, merely contain an email address in the body of an email between two non-targets.").

182. The data is contained in the Transmission Control Protocol/Internet Protocol (TCP/IP) used by the Internet. *What is a Packet?*, HOW STUFF WORKS, http://computer.howstuffworks.com/question525.htm [http://perma.cc/WF7S-WQ5N].

ton that gets routed through a server in Canada. Through no intent or design of the individual in Chicago, the message becomes international and thus subject to NSA surveillance.

Third, further collection of domestic conversations takes place through the NSA's intercept of what are called multi-communication transactions, or MCTs. It is important to distinguish here between a transaction and a communication. Some transactions have only single communications associated with them. These are referred to as SCTs. Other transactions contain multiple communications. If even one of the communications in an MCT falls within the NSA's surveillance, all of the communications bundled into the MCT are collected.

The consequence is of significant import. FISC estimated in 2011 that somewhere between 300,000 and 400,000 MCTs were being collected annually on the basis of "about" communication—where the "active user" was not the target. So hundreds of thousands of communications were being collected that did not include the target as either the sender or the recipient of the communication.[183]

183. PCLOB REPORT, *supra* note 2 at 38. In July 2014 the *Washington Post* made headlines when it focused on the scope of communications caught in the system. The article noted that ordinary Internet users significantly outnumber targeted foreigners. Barton Gellman, Julie Tate, and Ashkan Soltani, *In NSA-intercepted data, Those Not Targeted Far Outnumber the Foreigners Who Are*, WASH. POST, July 5, 2014, http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html [http://perma.cc/T5UE-MKBZ]. Following a four month investigation based on documents leaked by Edward Snowden, the *Post* found that nine out of ten account holders found in a cache of conversations had not themselves been the target of any investigation. *Id.* The story, however, failed to distinguish between individuals in direct contact with targets and those subject to "about" collection. For further critique of the article *see* Bob Cesca, *Significant Holes Emerge in the Washington Post's NSA Story After It's Too Late*, THE DAILY BANTER, Jul. 8, 2014, http://thedailybanter.com/2014/07/significant-holes-emerge-washington-posts-nsa-story-late/ [http://perma.cc/2A9X-Y4K2]. For a response to this and other critiques *see* Barton Gellman, *How 160,000 intercepted Communications Led to Our Latest NSA Story: the Debrief*, WASH. POST. July 11, 2014, http://www.washingtonpost.com/world/national-security/your-questions-answered-about-the-posts-recent-investigation-of-nsa-surveillance/2014/07/11/43d743e6-0908-11e4-8a6a-19355c7e870a_story.html [http://perma.cc/7GH3-AQ23].

### *2. Foreignness Determinations*

Targeting procedures require NSA analysts to make a determination regarding the location and legal status of a potential target (together referred to as the "foreignness determination").[184] Two related interpretations have allowed the NSA to push the statutory limits: first is the assumption, having looked at the evidence available, that a target outside the United States or in an unknown location is a non-U.S. person, absent evidence to the contrary; second, where the target is not known to be inside the United States, the NSA presumes that the target is located outside domestic borders. These assumptions raise question about the level of due diligence required to ascertain status and location, tilt the deck in favor of allowing collection, and create, in at least some cases, a circular pattern.

The FAA is largely silent about what burden must be borne by the government to establish whether the target is a U.S. person. Instead, Section 702 directs the Attorney General to adopt targeting procedures reasonably designed (a) to ensure acquisition is limited to persons reasonably believed to be outside U.S.; and (b) to prevent the acquisition of domestic communications.[185]

In other words, the statute only requires that the NSA not *know* (a) that the target is in the U.S.; or (b) that it is intercepting entirely domestic communications. There is nothing in the targeting requirements requiring intelligence agencies to take certain steps to ascertain whether the target is a U.S. person or what must be done to ascertain the target's location.

Sections 703 and 704, which are designed to deal with U.S. persons, say nothing in turn about what is required to demonstrate whether a target either is or is not a U.S. person.[186] Instead, these provisions address situations where the applicant has probable cause to believe that the target is a person outside the United States and is a foreign power, an agent of a foreign power, or an officer or employee thereof.[187]

---

184. Legal status means whether a target is a U.S. person or a non-U.S. person.

185. 50 U.S.C. § 1881a(d) (2012).

186. 50 U.S.C. § 1881b(b) (2012).

187. 50 U.S.C. § 1881b(b)(C) (2012) (containing Section 703); *id*. § 1881c(c)(B) (containing Section 704).

In the absence of statutory guidance, the NSA interprets the statute to allow the agency to assume that the target is a non-U.S. person where there is not sufficient evidence to the contrary.[188] The NSA's minimization procedures explain:

> A person known to be currently outside the United States, or whose location is unknown, will not be treated as a United States person unless such person can be positively identified as such, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person.[189]

Thus, an important question is what specific steps must the NSA take in order to determine the legal status of the target.[190]

The Targeting Procedures do not set a high bar. When referring to databases or other surveillance systems that could be consulted to determine whether the target is a U.S. person or a non-U.S. person, the document uses the word "may"—the present tense articulation of a mere possibility. As an auxiliary verb, it adds a functional meaning to the resultant clause—specifically, in the case of "may," to intone possibility in a manner that equally incorporates the possibility of "may not." The NSA thus may consult its databases to determine whether a target is a U.S. person. It also may decide not to. At no point does the document itself suggest what the NSA "must" do.[191]

---

188. NSA TARGETING PROCEDURES, *supra* note 16, at 4 ("In the absence of specific information regarding whether a target is a United States person, a person reasonably believed to be located outside the United States or whose location is not known *will be presumed to be a non-United States person* . . . .") (emphasis added).

189. 2009 MINIMIZATION PROCEDURES, *supra* note 169, at § 2(j)(2).

190. PCLOB HEARING, *supra* note 3, at 41.

191. In response to public concerns about the use of a majority "foreignness" test, the NSA's new Privacy and Civil Liberties Officer reported in April 2014 that the agency employs a totality of circumstances test:

> This is not a 51% to 49% 'foreignness' test. Rather the NSA analyst will check multiple sources and make a decision based on the totality of the information available. If the analyst discovers any information indicating the targeted person may be located in the U.S. or that the target may be a U.S. person, such information must be considered. In other words, if there is conflicting information about the location of the person or the status of the person as a non-U.S. person, that conflict must be resolved before targeting can occur.

NSA'S IMPLEMENTATION REPORT, *supra* note 170, at 4.

Once analysts have information about the target, the next question is how to weigh the evidence. Here, the test employed appears to be a totality of the circumstances. As Raj De, General Counsel of the NSA, explained:

> [A]n analyst must take into account all available information . . . [A]n analyst cannot ignore any contrary information to suggest that that is not the correct status of the person . . . [A]ny such determination is very fact-specific to the particular facts at hand.[192]

De illustrated the point with reference to a hypothetical used in the NSA's internal training manual: Say that an analyst has four pieces of information, two of which suggest U.S. person status and two of which indicate non-U.S. person status. A majoritarian test would be insufficient.[193] De explained that, "[o]ne must take into account the strength, credibility, and import of all relevant information."[194] Once deciding, "analysts have an affirmative obligation to periodically revisit the foreignness determination."[195]

It does not appear that analysts are required to document the basis for the non-U.S. person determination.[196] This practice differs from that adopted in relation to location determinations. According to a 2012 declassified (and heavily redacted) compliance report, after making a location determination, analysts are required to "document in the tasking database a citation to the information that led them to reasonably believe that a targeted person is located outside the United States."[197] The citation entered

---

192. PCLOB HEARING, *supra* note 3, at 41.

193. *See also* NSA's Implementation Report, *supra* note 170 at 4 ("This is not a 51% to 49% 'foreignness' test."); PCLOB Report, *supra* note 2, at 44 ("The government has stated, and the Board's review has confirmed, that this is not a '51% to 49% test.'").

194. PCLOB HEARING, *supra* note 3, at 42.

195. *Id.*

196. *See, e.g.*, PCLOB REPORT, *supra* note 2, at 46 ("[A]s a matter of NSA policy, as opposed to a requirement in the NSA targeting procedures, NSA analysts document the assessed non-U.S. person status of the target, but analysts do not separately document the basis for this non-U.S. person determination.").

197. Att'y Gen. & Dir. of Nat'l intelligence, Semiannual Assessment of Compliance with Procedures & Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Reporting Period: June 1, 2012–Nov. 30, 2012, at A-5 (2013) [AUG. 2013 SEMIANNUAL ASSESSMENT], *available at* http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20

"is a reference that includes the source of the information [REDACTED]." Such source records cited are "contained in a variety of NSA data repositories" or consist of "lead information" from other agencies, "such as disseminated intelligence reports."[198] The inclusion of this information enables oversight personnel "to locate and review the information that led the analyst to his/her reasonable belief."[199] PCLOB sidestepped concern about the failure of the NSA to document the legal status determination on the grounds that "[i]n general . . . the non-U.S. person analysis is based upon same information that underlies the determination regarding the target's location."[200]

The board failed to consider how the assumed commonality undermines an important check on the collection of intelligence: namely, the ability to subject the determination to a meaningful level of review. This was precisely the board's criticism with regard to NSA's omission of evidence documenting the foreign intelligence purpose of collection.[201] It is not clear why the same analysis would not apply.

Like the legal status determination, the specific steps required to make a location determination are not included in the statute. The targeting procedures, in turn, come down on the side of greater flexibility for the NSA. The agency "may also review information in its databases" to ascertain if the target is overseas.[202] It is not required to do so. Similarly, the "NSA may also apply technical analysis concerning the facility from which it intends to acquire foreign intelligence information . . . ."[203] It is under no procedural obligation to do so.[204] It is thus unclear, for both status and

---

procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf [http://perma.cc/TN8X-8E9W].

198. *Id.* at A-6.

199. *Id.* at A-5. The text continues, "Analysts must also identify the foreign power or foreign territory about which they expect the proposed targeting will obtain foreign intelligence information." *Id.*

200. PCLOB REPORT, *supra* note 2, at 46.

201. *See infra* part II.A.3.

202. NSA TARGETING PROCEDURES, *supra* note 16, at 2.

203. *Id.* at 3.

204. Emphasis, instead, is placed on the back-end. 2009 MINIMIZATION PROCEDURES, *supra* note 169, at § 3(d)(1):

> In the event that NSA determines that a person is reasonably believed to be located outside the United States and after targeting this person learns that the person is inside the United States, or if NSA concludes that a

location determinations, what level of due diligence is required, with the deck tilted in favor of acquisition.[205]

It is not clear the extent to which statutory vagueness influences the scope of collection. As a practical matter, there may not be many cases in which the NSA lacks information about the target's identity. Some sort of information must be available to ascertain that the information to be collected is of some foreign intelligence value. Precisely what level of information is sufficient, however, is not (at least as a public matter) clear. For the cases in which the only information available is that of a selector, only two assumptions are possible: Either one presumes that the individual is foreign and thus commences acquisition, or one presumes that the target is a U.S. person and thus falls within Sections 703–704. If the individual is known to be outside the United States, under a rational basis standard, it is logical to assume that he or she is more likely to be a non-U.S. person than a U.S. person. A substantially higher percentage of individuals outside the U.S. are non-U.S. persons. But in order for this to hold, the NSA must know at

---

person who at the time of targeting was believed to be a non-United States person is in fact a United States person, the acquisition from that person will be terminated without delay.

205. PCLOB states (without citation), "The government has stated that in making this foreignness determination the NSA targeting procedures inherently impose a requirement that analysts conduct "due diligence" in identifying . . . relevant circumstances." PCLOB REPORT, *supra* note 2, at 43. The board also notes that "a failure by an NSA analyst to conduct due diligence in identifying relevant circumstances regarding the location and U.S. person status of a Section 702 target is a reportable compliance incident to the FISC." *Id.*, at 43. However, the board does not specify how the agency ensures due diligence even as it notes that "[w]hat constitutes due diligence will vary depending on the target . . . ." *Id.*, at 43–44. Without more information, it is difficult to assess how much leeway is granted. Press reports suggest that the NSA assumes foreignness where the selector is being accessed from a foreign IP address, or where international locations are embedded in Yahoo tracking cookies—the former being common for Americans traveling abroad or using proxies to redirect data traffic, and the latter notoriously regarded in the advertising world as unreliable indicators of location. *See* Barton Gellman, Julie Tate, and Ashkan Soltani, *In NSA-intercepted data, those not targeted far outnumber the foreigners who are*, WASH. POST (July 5, 2014), http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html [http://perma.cc/KY7W-KYB6]. Without more publicly available information, the strength of these claims is difficult to evaluate.

the outset that the individual is outside the U.S. The circularity of the assumptions adopted by the NSA thus matter.

At some level, as a matter of status and location, the default makes sense. Intelligence collection at the point of communication is a binary system. Failure to intercept the conversation may mean a (permanent) loss of the information. Under this approach, it is better to make the assumption and to collect the information, putting more emphasis on post-tasking review by ODNI and DOJ and purge requirements, if a target is later found to be a U.S. person or located within domestic bounds.

But there are dangers of approaching intelligence collection in this manner. Certainly, the structure creates a disincentive for due diligence to affirmatively ascertain the status or location of the target—one, in this case, reinforced by judicial fiat.

### *3. Foreign Intelligence Purpose Determination*

Once a foreignness determination is made, NSA analysts must ascertain "how, when, with whom, and where" the target communicates.[206] From this, the analyst identifies "specific communications modes," obtaining identifiers linked to the target—subsequently referred to as "selectors." For each selector, NSA analysts must determine the expected foreign intelligence information, as well as information that would lead one to reasonably conclude that the selector is associated with a non-U.S. person outside the United States.[207]

The vagueness of what is understood as foreign intelligence information is of note.[208] The NSA Director of Civil Liberties and

206. NSA'S IMPLEMENTATION REPORT, *supra* note 170, at 4.

207. *Id.* at 4–5. *See also* PCLOB REPORT, *supra* note 2, at 45.

208. The term "foreign intelligence information" is not defined in the Section 702 Minimization Procedures. The procedures define "foreign communications" broadly to mean "a communication that has at least one communicant outside of the United States." 2009 MINIMIZATION PROCEDURES, *supra* note 169, at § 2. The term is, however, defined in traditional FISA as:

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

Privacy ties the contours of what qualifies to a Section 702 certification.[209] One semiannual assessment notes merely that the foreign power or foreign territory about which information is being sought must be documented.[210] Although the targeting procedures, as of the time of writing, are still classified, PCLOB reported in July 2014 that they "include a non-exclusive list of factors that the NSA will consider in determining whether the tasking of a selector will be likely to result in foreign intelligence information falling within one of the Section 702 certifications."[211] However, unlike the location portion of the foreignness determination, analysts are *not* required under the targeting procedures to document the reasons that led the analyst to make the foreign intelligence purpose determination.

PCLOB recognized the weakness of this approach:

> In the Board's view, this reduced documentation regarding the foreign intelligence purpose determination results in a less rigorous review by the NSA's external overseers of the

---

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

50 U.S.C. § 1801(e) (2012).

The items listed under (1) are consistent with FISA and, in particular, the criminal aspects of behavior that the statute is meant to address. They key to establishing the target of surveillance as a foreign power (or an agent thereof), or the involvement of the target (if a U.S. person) in illegal activities (such as sabotage, international terrorism, or the international proliferation of WMD). Item (2), in contrast, is much less precise. The terminology speaks to the importance of intelligence generally and U.S. national security and foreign affairs interests—areas that may incorporate broad swathes of information. A strong argument could be made, for instance, that conversations related to international trade, economic stability, other countries' foreign policy goals, new technologies, energy security, and food security all constitute foreign intelligence. *See, e.g.*, Laura Poitras et al., *Ally and Target: US Intelligence Watches Germany Closely*, DER SPIEGEL ONLINE INTERNATIONAL (Aug. 12, 2013, 12:44 PM), http://www.spiegel.de/international/world/germany-is-a-both-a-partner-to-and-a-target-of-nsa-surveillance-a-916029.html [http://perma.cc/M5FT-SMHK] (citing an April 2013 NSA document as highlighting these intelligence priorities for U.S. surveillance of European Union). As such, they are legitimate interests to be pursued under the exercise of Section 702 authorities, as applied overseas to non-U.S. persons.

209. NSA'S IMPLEMENTATION REPORT, *supra* note 170, at 4.

210. AUG. 2013 SEMIANNUAL ASSESSMENT, *supra* note 197, at A-5.

211. PCLOB REPORT, *supra* note 2, at 45.

foreign intelligence purpose determinations than the NSA's foreignness determination.[212]

### *4. Result of Statutory Interpretations*

The component statutory interpretations, particularly TFA and the assumptions that mark the foreignness determination, undermine the protections created for U.S. persons in Sections 703 and 704 of the statute. They make it possible for the NSA to obtain significant amounts of American citizens' communications.

Until the FAA, the surveillance of U.S. persons outside domestic bounds took place under the weaker standards of Executive Order 12,333. Part of the purpose of the FAA was thus to *increase* the protections afforded to U.S. persons travelling abroad.[213] The way in which Section 702 is being used, however, allows the NSA to bypass Section 703 by making assumptions about legal status and location and potentially subjecting U.S. persons to surveillance without meeting the requirements of Section 703.

The amount of information at stake is not insubstantial. For years, the volume of intercepts under Section 702 has been one of the principal concerns of legislators familiar with the program. Senators have consistently expressed unease about the intelligence community's claim that it is impossible to quantify how many Americans' communications have been implicated in the operation of Section 702.[214] What has gradually become clear is

---

212. *Id.* at 46.

213. In Section 703, to target a U.S. person overseas, the government must submit an application to FISC identifying the target and the facts and circumstances undergirding probable cause that the target is a foreign power or an agent of a foreign power. 50 U.S.C. §§ 1881b(b)-(c), 1881c(b)-(c) (2012). There are short-term provisions in the event of emergency situations; within seven days, however, the government must make formal application to the court. 50 U.S.C. §§ 1881b(d), 1881c(d). The government must establish probable cause that the target is located outside the United States—a higher standard than required under Executive Order 12,333, which only dictated that the AG determine that the technique was being used against a foreign power or an agent thereof. *Id.*

214. This statement has been made by ODNI, the NSA IG, and the IC IG. *See* Letter from I. Charles McCullough, III, IG of the Intelligence Cmty., to Senators Ron Wyden and Mark Udall, Washington, DC (June 15, 2012), *available at* http://www.wired.com/images_blogs/dangerroom/2012/06/IC-IG-Letter.pdf [http://perma.cc/H7ME-CQCZ] ("I defer to [the NSA IG's] conclusion that obtaining such an estimate [of 'how many people inside the United States have had their communications collected or reviewed under the authorities granted by section 702'] was beyond the capacity of his office and dedicating sufficient additional resources would likely impede the

that the program significantly more expansive than initially understood.[215]

---

NSA's mission."). Part of the unease stems from the fact that the NSA had been able to provide a rough estimate of domestic communications, in classified form, to FISC. Judge Bates asked the NSA to undertake a manual review of a statistical subsection of transactions collected through upstream intercepts in the first six months of 2011. Based on the results, Bates estimated that the NSA was collecting up to 56,000 citizen communications annually (46,000 of which consisted entirely of U.S. citizens' communications—in other words, Single Communication Transactions—and 10,000 of which became part of Multiple Communication Transactions). [Redacted], 2011 WL 10945618, at *11 (FISA Ct. Oct. 3, 2011). *See also* Senator Ron Wyden, Keynote address at Cato Institute: NSA Surveillance: What We Know; What to do About It (Oct. 9, 2013), *available at* http://www.cato.org/events/nsa-surveillance-what-we-know-what-do-about-it [http://perma.cc/E4XJ-VCR9].

215. Following the initial release of the PRISM slides on June 6, 2013, on June 18, the NSA issued a Fact Sheet, stating that FISA "allows only the targeting, for foreign intelligence purposes, of communications of foreign persons who are located abroad." The Fact Sheet, which does not have a date on it, was released June 18, 2013. The document was quickly withdrawn from the DNI's website; however, a copy of the can be found online. NSA, FACT SHEET ON SECTION 702, *available at* http://www.wyden.senate.gov/news/blog/post/wyden-and-udall-to-general-alexander-nsa-must-correct-inaccurate-statement-in-fact-sheet [http://perma.cc/3BRU-U9AU]. Consistent with the statutory language, the government stated that the purpose of such acquisition could not be to obtain information from a particular, known person inside the U.S. What followed was an elaborate back-and-forth, in the course of which the extent to which U.S. persons' information had been obtained became more visible. Two days after the government's release of the Fact Sheet, on June 20, 2013, the *Guardian* released the NSA's Section 702 Targeting Procedures, as well as its Section 702 Minimization Procedures—in the process undermining the government's assertion that U.S. persons' privacy was protected. NSA TARGETING PROCEDURES, *supra* note 16; 2009 MINIMIZATION PROCEDURES, *supra* note 169. Two days after that, Senators Wyden and Udall accused the DNI of a "significant" inaccuracy in the Section 702 fact sheet, particularly with regard to how the authority has been interpreted by the US government. Letter from Sen. Ron Wyden & Sen. Mark Udall, to Gen. Keith Alexander, Dir., Nat'l Sec. Agency (June 24, 2013), *available at* http://www.wyden.senate.gov/news/blog/post/wyden-and-udall-to-general-alexander-nsa-must-correct-inaccurate-statement-in-fact-sheet [http://perma.cc/76XS-78JA]. General Alexander replied the following day. Letter from Gen. Keith B. Alexander, Dir., Nat'l Sec. Agency, to Sen. Ron Wyden & Sen. Mark Udall (June 25, 2013), *available at* https://www.aclu.org/files/natsec/nsa/20130816/General%20Alexander%20Letter%20re%20NSA%20Fact%20Sheet%20Inaccuracy.pdf [https://perma.cc/E3N5-7HCV]. Alexander agreed with the senators that the fact sheet "could have more precisely described the requirements for collection under Section 702." *Id.* at 1. As to Wyden and Udall's second concern (whether the fact sheet implied that the NSA had the ability to determine how many American communications it had collected), he noted that this question had already been publicly addressed. *Id.* The *Guardian* followed with a release on June 27, 2013 of a draft NSA inspector general report reviewing the President's Surveillance Program and its transfer to Section 702. WORKING DRAFT, *supra* note 19. From this and subsequent leaked documents, it became clear that the program was more extensive than previously indicated. *See NSA*

### *5. Congressional Intent*

In 2008 Congress anticipated that the intelligence community would inadvertently collect U.S. persons' communications in the process of targeting non-U.S. persons under Section 702. Legislators acknowledged the possibility, and Congress inserted special back-end protections via minimization procedures and the inclusion of explicit limits. But outside of a handful of exceptions, members did not publicly anticipate that the executive would engage in such large-scale, programmatic collection, so as to undermine Sections 703 and 704.[216] Legislators who did publicly recognize the potential for programmatic surveillance opposed the statute on precisely those grounds. Not a single member who recognized the potential for programmatic surveillance defended the use of the authorities in this way.

Even if Congress did not initially understand the implications of the FAA, the executive subsequently informed the House and Senate Intelligence Committees about PRISM and upstream collection. Congress's subsequent failure to end the programs—indeed, its decision to reauthorize the FAA in 2012—suggests that the legislature intended the intelligence community to continue interpreting the statute in a manner that supported the programs. Arguments that the legislature was too hampered by classification to either read or respond to intelligence community reports fail to appreciate Congress's interpretation of its own authorities with regard to classification.

#### *a. Minimization and Explicit Limits*

During the legislative debates, not all members of Congress appear to have understood the distinction between targeting U.S. persons and collecting U.S.-person information more gener-

---

*Prism Program Slides*, GUARDIAN, Nov. 1, 2013, http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document [http://perma.cc/5RL4-FPUU].

216. Congress's aim in drafting these sections was to offer U.S. persons a greater degree of privacy than had previously existed under Executive Order. *See, e.g.*, 154 CONG. REC. S6465 (daily ed. July 9, 2008) (statement of Sen. Rockerfeller) ("[T]he bill ensures that when Americans overseas are the target, that a FISA Court judge, rather than the Attorney General—in a very important change—decide that there is clear authority and probable cause for intelligence agencies to target such an individual."); 154 CONG. REC. H5762 (daily ed. June 20, 2008) (statement of Rep. Harman) ("[This bill] expands the circumstances for which individual warrants are required, by including Americans outside the U.S.").

ally. Representative Heather Wilson (R-NM) lauded the legislation on the grounds that it would "protect the civil liberties of Americans and continue to require individualized warrants for anyone in the United States or American citizens anywhere in the world."[217] Representative Anna Eshoo (D-CA) noted that "[T]he Administration would have to seek a court order before conducting surveillance on U.S. persons abroad."[218] At no point did either member acknowledge that at least some acquisition of U.S. persons' communications overseas could occur absent a court order, as long as the target was a non-U.S. person. Representative Nancy Pelosi (D-CA) said that the bill provided that Americans overseas receive the same FISA protections ("including an individualized warrant based on probable cause") as Americans within domestic grounds.[219] She considered it "a very important improvement on the original FISA Act."[220] Similar remarks characterize the debate in the Senate. Senator Benjamin Cardin (D-MD) stated: "FISA requires the Government to seek an order or warrant from the FISA Court before conducting electronic surveillance that *may involve* U.S. persons."[221]

Individual legislators notwithstanding, in two respects the final legislation reflected a general understanding that, at a minimum, in the process of targeting non-U.S. persons, citizens' information might inadvertently be obtained. First, the statute explicitly included minimization procedures that addressed how the executive branch would handle incidental data. Legislators looked to these provisions to discount the potential for further inroads into privacy. Representative Bob Etheridge (D-NC) thus stated: "This bill . . . requires the Government to obtain an individual warrant from the FISA Court before conducting surveillance on a United States citizen. This warrant must be based on probable cause, and

---

217. 154 CONG. REC. H5763 (daily ed. June 20, 2008) (statement of Rep. Heather Wilson).

218. 154 CONG. REC. H5771 (daily ed. June 20, 2008) (statement of Rep. Anna Eshoo).

219. 154 CONG. REC. H5767 (daily ed. June 20, 2008) (statement of Rep. Nancy Pelosi).

220. *Id.*

221. 154 CONG. REC. S6379 (daily ed. July 8, 2008) (statement of Sen. Cardin) (emphasis added).

the provision now includes American citizens abroad as well."[222] He underscored the role of the FISA Court, noting that FISC's review of targeting and minimization procedures was to "ensure that any inadvertently intercepted communications by American citizens are destroyed."[223] Representative Silvestre Reyes (D-TX) similarly announced that the FAA requires "warrants for Americans anywhere in the world. It also requires the government to establish clear guidelines to ensure that no American is the target of any surveillance without a warrant."[224] Representative Jim Langevin (D-RI) stated: "Americans will no longer leave their constitutional protections at home when working, studying or traveling abroad."[225] He minimized the potential interception of U.S. persons' communications, suggesting that they would be subject to special legal protections.[226]

Second, not only did the statute include minimization requirements, but Congress expressly prohibited the acquisition of purely domestic communications, the targeting of persons within the United States, and reverse targeting. The purpose of these limits was to ensure that the NSA did not use non-U.S. person targeting to collect information on U.S. persons. The statute required the Attorney General to adopt guidelines to ensure compliance with these limitations.[227]

Even here, however, programmatic considerations gave way to particularization. Legislators' consideration of reverse targeting was individual. They looked to its prohibition as a way of preventing the government from targeting one or more individuals overseas with the aim of obtaining the communications of a spe-

---

222. 154 CONG. REC. H5772 (daily ed. June 20, 2008) (statement of Rep. Bobby Etheridge).

223. *Id.*

224. 154 CONG. REC. H5758 (daily ed. June 20, 2008) (statement of Rep. Silvestre Reyes).

225. 154 CONG. REC. H5766 (daily ed. June 20, 2008) (statement of Rep. James Langevin).

226. *Id.*

227. 50 U.S.C. § 1881a(f)(1) (2012). *See also* 154 CONG. REC. S6388 (daily ed. July 8, 2008).

cific person located within U.S. borders.[228] For many, this was a crucial part of their support for the measure.[229]

*b. Potential Programmatic Collection As a Point of Opposition*

Some legislators did express opposition to the potential for Section 702 authorities to be used on a massive scale, in the process collecting significant amounts of U.S. persons' information. Without exception, these legislators opposed the final bill.

Representative Sheila Jackson Lee from Texas, for instance, railed that the compromise bill "fail[ed] to protect American civil liberties both at home and abroad."[230] She explained her objection: "[The bill] permits the Government to conduct mass, untargeted surveillance of all communications, coming into and out of the United States, without any individualized review, and without any finding of wrongdoing."[231] Representative Bobby Scott (R-VA) similarly noted:

> The bill actually permits the government to perform mass untargeted surveillance of any and all conversations believed to be coming into and out of the United States without any individualized finding and without a requirement that wrongdoing is believed to be involved at all.
>
> It arguably is not limited just to terrorism. It could be any foreign intelligence, which would include diplomacy and anything else.[232]

Representative Jackie Speier's statement proved prescient:

> It is fundamentally untrue to say that Americans will not be placed under surveillance . . . . The truth is, any American will subject their phone and e-mail conversations to the broad government surveillance web simply by calling a son or daughter studying abroad, sending an email to a foreign

228. *See, e.g.*, 154 CONG. REC. H5756 (daily ed. June 20, 2008) (statement of Rep. John Conyers); 154 CONG. REC. H5762 (daily ed. June 20, 2008) (statement of Rep. Jane Harman).

229. *See, e.g.*, 154 CONG. REC. 5768 (daily ed. June 20, 2008) (statement of Rep. Nancy Pelosi).

230. 154 CONG. REC. H5763 (daily ed. June 20, 2008) (statement of Rep. Sheila Lee).

231. *Id.*

232. 154 CONG. REC. H5759 (daily ed. June 20, 2008) (statement of Rep. Robert Scott).

> relative, even calling an American company whose customer service center is located overseas.[233]

Speier, a California Democrat, continued: "The bottom line is, this FISA bill permits the collection of Americans' emails and phone calls if they are communicating with someone outside of the U.S."[234] Representative Rush Holt (D-NJ), a member of HPSCI, opposed the bill on similar grounds: "It permits massive warrantless surveillance in the absence of any standard for defining how communications of innocent Americans will be protected; a fishing expedition approach to intelligence collection that we know will not make Americans more safe."[235] Representative Dennis Kucinich (D-OH) opposed the legislation for the same reason: "There's no requirement for the government to seek a warrant for any intercepted communication that includes a U.S. citizen, as long as the program in general is directed towards foreign targets."[236] Kucinich added:

> Under this bill, violations of Fourth Amendment rights and blanket wiretaps will be permissible for the next 4 years. Massive and untargeted collection of communications will continue . . . .
>
> Furthermore, it allows the type of surveillance to be applied to all communications entering and exiting the United States. These blanket wiretaps make it impossible to know whose calls are being intercepted by the National Security Agency.[237]

These statements stood in sharp contrast to the legislators who supported the bill, all of whom discounted the amount and extent of incidental information thereby obtained, pointing particularly to the minimization procedures as a way to rectify any privacy interests thereby implicated.

Senator Ben Cardin from Maryland summarized the protections:

---

233. 154 CONG. REC. H5770 (daily ed. June 20, 2008).

234. *Id.* Speier noted: "This is especially true when it comes to emails, because the World Wide Web has no area codes, so it is impossible to tell where email communications originate from." *Id.*

235. 154 CONG. REC. H5765 (daily ed. June 20, 2008) (statement of Rep. Rush Holt).

236. 154 CONG. REC. H5767 (daily ed. June 20, 2008) (statement of Rep. Dennis Kucinich).

237. *Id.*

> The legislation provides for the inspector general to review the targeting and minimization provisions. The targeting is when a U.S. citizen, perhaps indirectly, is targeted. And the minimization procedures deal with when the intelligence community gets information about an American without court approval, to minimize the use of that information or to seek court approval.[238]

Cardin anticipated the potential interception of communications of *an* American—not the monitoring of *all* Americans engaged in international communications. He cabined the amount of data ("that information"), and noted that the minimization procedures would further protect the information obtained. Senator Bond similarly discounted the potential for programmatic surveillance:

> The bugaboo that this [bill] gives the intelligence community the right to listen in on ordinary citizens' conversations willy-nilly, without any limitations, is absolutely false. That is why we built in the protections in the law. That is why we have the layers of supervision to make sure it does not happen.[239]

These representations do not reflect how the authorities are being used. The concept of "incidental" does not suggest broad acquisition. The Oxford English Dictionary, for example, defines "incidental" as "accompanying but not a major part of something" or "Occurring by chance in connection with something else." If the NSA knows that it is collecting entirely domestic conversations, it is a stretch of common usage to suggest that such acquisition is occurring by chance. The volume of communications monitored is also at odds with claims that downplay the impact of the action in question.

The NSA's minimization procedures, in turn, require personnel to destroy "inadvertently acquired communications of or concerning a United States person."[240] The Privacy and Civil Liberties Board states, "it is not entirely clear what constitutes an "inadvertently acquired communication."[241] The Oxford English Dic-

---

238. 154 CONG. REC. S6380 (daily ed. July 8, 2008) (statement of Sen. Benjamin Cardin).

239. 154 CONG. REC. S6396 (daily ed. July 8, 2008) (statement of Sen. Christopher Bond).

240. 2011 MINIMIZATION PROCEDURES, *supra* note 171, at § 3 (b)(1).

241. PCLOB REPORT, *supra* note 2, at 62.

tionary understands the word "inadvertent" as "Not resulting from or achieved through deliberate planning." It seems clear, however, that the NSA and Congress anticipate that the government will obtain U.S. persons' communications under Section 702. Calling such interception "inadvertent" does not make it so.

*c. Acquiescence*

Even if Congress did not realize what it was authorizing in 2008, the intelligence community kept the legislature informed about the programs underway. Thus, at a minimum, at the point of reauthorization in 2012, Congress agreed to the exercise of authorities in this manner. For this argument to succeed, three claims must be satisfied: first, Congress must have been (accurately) informed about the program, second, Congress must have been able to act to stop the program, and, third, Congress must have affirmatively continued it. All of these conditions were met.

Title VII requires that the Attorney General twice a year inform the intelligence committees and the Committees on the Judiciary of the Senate and the House of Representatives about any certifications submitted in accordance with Section 702(g), or directives issued under Section 702(h), as well as a description of judicial review during the reporting period of the certifications and targeting and minimization procedures—including a copy of any orders or pleadings in connection with such review *containing a significant legal interpretation* of the provisions of Section 702.[242] The statute requires that the Attorney General report any actions taken to challenge or enforce a directive, any compliance reviews conducted by the Attorney General or the DNI, and a description of any incidents of noncompliance.[243] In addition, the intelligence community must review the number of disseminated intelligence reports containing references to a U.S. person, as well as the number of targets later determined to be located in the United States, and provide the information to the intelligence and judiciary committees.[244]

---

242. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 707), 122 Stat. 2436, 2457 (codified at 50 U.S.C. § 1881f) (2012)).

243. *Id.*

244 . FISA Amendments Act of 2008, § 702(l)(2)–(3) (codified at 50 U.S.C. § 1881a(l)(2)–(3)).

There is every reason to believe that the intelligence community fulfilled these statutory requirements and that all four committees were aware of the extent of the programs underway—particularly after the findings of noncompliance by FISC and the court's rejection of targeting procedures premised on the problem with MCTs.[245]

In order for the argument to be satisfied, though, reporting to a part of the whole must sufficiently indicate the acquiescence of the many. There are myriad ways in which committees in Congress substitute for the judgment of the whole body. Most Congressional oversight functions are consistent with this approach. It falls to the committees charged with oversight to review and consider the manner in which authorities are being used prior to the introduction, elimination, alteration, or continuance of authorities or appropriations.

What is different, at least with regard to FISA (albeit consistent with other areas of national security law), is the clandestine nature of the reporting and the restrictions placed on committee and non-committee members who may have access to the information. Members may not know of the existence of, or details about, programs that would enable them to ask pertinent questions or to delve further into how authorities are being exercised. The result is that Congress may agree to laws without fully understanding the implications of their actions.

One could argue that this happens all the time. It is part of the good faith exercise that is part and parcel of the legislative process. Legislators accord their colleagues, who develop an expertise in certain areas, a degree of deference. But one distinction, in regard to national security, is that the stakes are particularly high.

It is precisely this concern that arose during enactment of the FAA in 2008. Congress was being asked to pass legislation that gave telecommunication companies indemnity, but only a minority of the members of both chambers had been briefed on the President's Surveillance Program. The question, according to Senator Specter, was whether the limited briefing amounted to an uncon-

245. *See, e.g.*, Att'y Gen. & Dir. of Nat'l intelligence, Semiannual Assessment of Compliance with Procedures & Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Reporting Period: Dec. 1, 2010–May 31, 2011 (2011) [DEC. 2011 SEMIANNUAL ASSESSMENT].

stitutional delegation of authority.[246] For Senator Whitehouse, the issue was less one of constitutionality and more one of simple legislative prudence: whether the Senate ought to substitute its good faith in the few for a determination that ought to be made by the judiciary.[247] What was at stake was the rule of law.

In the case of Section 702, the intelligence community did not just keep the committees informed, but prior to the renewal debates, it made its classified briefings widely available to all Members of Congress.[248] The May 2012 report, for instance, available to

246. 154 CONG. REC. S6412 (daily ed. July 8, 2008) (statement and question of Sen. Arlen Specter). Senator Rockefeller responded by arguing that 37 members of the Senate had been briefed (15 on the Senate Intelligence Committee, 19 on the Senate Judiciary Committee (equaling 34, minus 4 crossover members), as well as 2 leadership on each side, Senator Roberts and the Appropriations Committee chairman and vice chair, plus Senator Levin and Senator McCain, who were ex officio). *Id.* (statement of Sen. John Rockefeller). Senator Specter replied that there had been 21 House Intelligence Committee members briefed, and as many as 40 Judiciary Committee members. In the Senate, 15 on the Intelligence Committee and 19 on the Judiciary Committee, for a bicameral total of 95—less than 18% of the entire Congress. *Id.* (statement of Sen. Arlen Specter). He further argued that, even taking Chairman Rockefeller's numbers, "you still have a majority of Members of Congress who have not been briefed, who are, in effect, delegating their authority to vote on a matter where they don't know what they are granting immunity for." *Id.*

247. 154 CONG. REC. S6412 (daily ed. July 8, 2008) (statement of Sen. Sheldon Whitehouse).

248. *See, e.g.*, Letter from Kathleen Turner, Dir. of Legislative Affairs ODNI, and Ronald Weich, Assistant Attorney Gen. in Office of Legislative Affairs DOJ, to the Hon. Dianne Feinstein, Chair, and the Hon. Saxby Chambliss, Vice Chair, Senate Select Comm. on Intelligence (May 4, 2012), declassified by the DNI Aug. 21, 2013, and *available at* http://www.dni.gov/files/documents/Ltr%20to%20HPSCI%20Chairman%20Rogers%20and%20Ranking%20Member%20Ruppersberger_Scan.pdf [http://perma.cc/8L76-8U6W] ("We believe that making this document available to all Members of Congress is an effective way to inform the legislative debate about reauthorization of Title VII of FISA. However, it is critical that Members understand the importance to national security of maintaining the secrecy of these programs. The enclosed document is being provided on the understanding that it will be provided only to Members of Congress (and cleared SSCI, Judiciary Committee, and leadership staff), in a secure location in the SSCI's spaces, and consistent with the rules of SSCI regarding review of classified information and non-disclosure agreements. Any notes taken by Members or staff may not be removed from the secure location. We also request your support in ensuring that Members and staff are well informed regarding the classification and sensitivity of this information to prevent any unauthorized disclosures.").

Members of Congress more than a year before the Snowden revelations, detailed PRISM and upstream collection.[249]

As to the second claim, could Congress have stopped the program if it so wished? The answer to this question is more difficult. Congress ostensibly had both private and public mechanisms it could employ to subject the program to more scrutiny and to change aspects considered repugnant as either a statutory or Constitutional matter. It could have conditioned continuation of the authorities, for instance, on curbing TFA collection, or shifting the assumptions regarding identity or location. Alternatively, it could have suspended funding for the program. It did none of these things. The House did not hold any hearings on how the law was operating prior to voting on whether to renew the FAA.[250] Publicly, Congress could have declassified materials, opened the NSA's programs to broader discussion, and subjected the executive to citizens' scrutiny. It chose not to do so.

Congress and the President disagree over whether and to what extent the legislature can make classified information public. Congress considers its authority subject only to its own rule making, and not to any executive order, statute, or constitutional provision. The Rules of Procedure for the Senate Select Committee on Intelligence state in relevant part:

> No member of the Committee or of the Committee staff shall disclose, in whole or in part or by way of summary, the contents of any classified or committee sensitive papers, materials, briefings, testimony, or other information in the posses-

249. Nat'l Sec. Agency, The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act 3–4 (, *available at* http://www.dni.gov/files/documents/Ltr%20to%20HPSCI%20Chairman%20Rogers%20and%20Ranking%20Member%20Ruppersberger_Scan.pdf [http://perma.cc/8L76-8U6W]. Although the Executive branch made the information available to Congress, there is some evidence that Congressional leadership itself prevented some 93 junior members, who had not been present during the enactment of the 2008 FAA, from seeing the reports on programmatic collection. Rachael King, *Congressman: House Members Not Given Access to NSA Documents*, WALL. ST. J., Aug. 12, 2013, *available at* http://blogs.wsj.com/cio/2013/08/12/congressman-house-members-not-given-access-to-nsa-documents/ [http://perma.cc/X9SE-WGT8]. It is unclear which members of Congress (including those who voted for renewal) were actively denied access to the material. The incident underscores concerns about Congressional abdication of its constitutional responsibilities with respect to its oversight and lawmaking functions.

250. *See* 158 CONG. REC. H5890–H5900 (daily ed. Sept. 12, 2012).

> sion of the Committee [except as provided in Section 8 of Senate Resolution 400 of the 94th Congress.][251]

Section 8 of the abovementioned Senate Resolution allows SSCI to publicly disclose any information in its possession after a determination by vote by the committee that such disclosure would be in the public interest.[252] (The rules prohibit any disclosure of information prior to the vote, which must be held within five days of any member's request.[253]) The Committee, if it votes to release information, must notify and consult with the Senate's Majority and Minority Leaders before placing the President on notice.[254] If, thereafter, the President objects, either the Majority and Minority leaders (jointly), or the Select Committee (by majority vote), may refer the question of disclosure to the Senate as a whole for consideration.[255] The Select Committee also has the authority, under its own rules, to share classified information in closed session with any members of the Senate it deems necessary.[256]

It does not appear that disagreement between the Senate and the President has ever led to the invocation of Section 8 with regard to convening the Senate as a whole, in closed proceedings, to consider whether to release classified information. But the Senate Select Committee regularly makes classified information available to non-committee members, subject to the restrictions of Section 8.[257] Nevertheless, its rules prevent non-committee members from making the information public.[258]

---

251. UNITED STATES SENATE, RULES OF PROCEDURE FOR THE SELECT COMMITTEE ON INTELLIGENCE, S. Prt. 113-7, 113th Cong. [hereinafter SSCI RULES OF PROCEDURE], § 9.7, *available at* http://www.intelligence.senate.gov/pdfs113th/sprt1137.pdf [http://perma.cc/HR24-U8JF].

252. S. Res. 400, 94th Cong. (1976), § 8(a) (quoted in SSCI RULES OF PROCEDURE, *supra* note 2511, Appendix A); *see also* S. REP. NO. 94-675, at 10 (1976), *available at* http://www.intelligence.senate.gov/pdfs_miscellaneous/94675.pdf [http://perma.cc/7RF5-QCND].

253. S. Res. 400, 94th Cong., § 8(a) (quoted in SSCI RULES OF PROCEDURE, *supra* note 251, Appendix A).

254. *Id.* at § 8(b)(1).

255. *Id.* at § 8(b)(3).

256. *Id.* at § 8(c)(1).

257. *See, e.g.*, INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2014, S. REP. NO. 113-120 (2013), *available at* http://beta.congress.gov/congressional-report/113th-congress/senate-report/120/1 [http://perma.cc/9ZMT-VUCZ] (stating, in relevant part, "The classified annex is made available to the Committees on Appropriations of the Senate and the House of Representatives and to the President.

As a constitutional matter, legislators could read information into the public record. The Speech or Debate clause in the U.S. Constitution states that members of both Houses of Congress,

> . . . shall in all Cases, except Treason, Felony and Breach of the Peace, be privileged from Arrest during their Attendance at the Session of their Respective Houses, and in going to and returning from the same; and for any Speech or Debate in either House, they shall not be questioned in any other Place.[259]

In 1971 Senator Mike Gravel, with the assistance of his Congressional aides, used this clause to read portions of the *Pentagon Papers* on the floor of the Senate and subsequently place all 47 volumes of the study into the *Congressional Record*.[260] In *Gravel v. United States*, the Supreme Court subsequently found it "incontrovertible" that the clause, at a minimum, protects legislators "from criminal or civil liability and from questioning elsewhere than in the Senate, with respect to the events occurring" in the course of Congressional hearings.[261] Justice White, writing for the Court, explained:

> The Speech or Debate Clause was designed to assure a coequal branch of the government wide freedom of speech, debate, and deliberation without intimidation or threats from the Executive Branch. It thus protects Members against prosecutions that directly impinge upon or threaten the legislative process.[262]

What this means is that Senators could disclose classified information from the floor of the Senate by reading it into the record. They would be exempt thereafter from criminal or civil liability; however, they would still be subject to censure by the

---

It is also available for review by any Member of the Senate subject to the provisions of Senate Resolution 400 of the 94th Congress (1976).").

258. *See* S. Res. 400, 94th Cong., § 8 (quoted in SSCI RULES OF PROCEDURE, *supra* note 251, Appendix A).

259. U.S. CONST. art. I, § 6, cl. 1.

260. How the Pentagon Papers Came to be Published by the Beacon Press: A Remarkable Story Told by Whistleblower Daniel Ellsberg, Dem Presidential Candidate Mike Gravel, and Unitarian Leader Robert West, DEMOCRACY NOW, July, 2, 2007, http://www.democracynow.org/2007/7/2/how_the_pentagon_papers_came_to [http://perma.cc/VQY5-FY9U].

261. Gravel v. United States, 408 U.S. 606, 615 (1972).

262. *Id.* at 616.

Senate and could be placed under a Senate investigation for breach of ethics.[263]

The executive branch has a different read on whether members of the legislature could make classified information public. This question recently arose in regard to the SSCI report on the CIA's post-9/11 detention and interrogation program.[264] In February 2014 the CIA Director of the Office of Congressional Affairs acknowledged that although the Report was a congressional record under SSCI's control, it contained information "originated and classified by the Executive Branch."[265] The executive did not "consider SSCI's control over the document to extend to control over the classification of the information therein."[266] Instead, it was the CIA's position that SSCI would have to "submit its Report for a declassification review before it could publicly release" a declassified version of the report.[267] The Department of Justice similarly noted that declassification review was "a necessary precursor to public release."[268]

So, while the Executive Branch has the position that the legislature cannot reveal classified information, the legislature

---

263. *See* S. Res. 400, 94th Cong., § 8(d) (quoted in SSCI RULES OF PROCEDURE, *supra* note 251, Appendix A).

264. In 2009 SSCI advised the CIA that it intended to conduct a review of the CIA's post-9/11 detention and interrogation program. Owing to the "highly sensitive and compartmented nature of the information at issue," the CIA insisted that SSCI conduct the review at CIA facilities. On December 14, 2012, the chair of SSCI informed the President and other officials that the committee had completed its review of the program. Declaration of Neal Higgins, Dir. of Office of Congressional Affairs, CIA at 4, ACLU v. CIA, No. 13-01870-JEB (D.D.C. Feb. 28, 2014), Document 17-2; *see also* Marty Lederman, *State of Play of the SSCI Report on the CIA Interrogation Program: the Relationship between Declassification and Disclosure*, JUST SECURITY, Apr. 10 2014, http://justsecurity.org/8294/stopping-ssci-simply-publishing/ [http://perma.cc/BX2F-QG7Z]; Mark Mazzetti & Scott Shane, *Senate and C.I.A. Spar Over Secret Report on Interrogation Program*, N.Y. TIMES. July 19, 2013, http://www.nytimes.com/2013/07/20/us/politics/senate-and-cia-spar-over-secret-report-on-interrogation-program.html?_r=0 [http://perma.cc/6BN6-RCKX].

265. Declaration of Neal Higgins, Dir. of Office of Congressional Affairs, CIA at 10, ACLU v. CIA, No. 13-01870-JEB (D.D.C. Feb. 28, 2014), Document 17-2.

266. *Id.*

267. *Id.*

268. Defendant's Reply in Further Support of Motion to Dismiss at 2, ACLU v. CIA, No. 1:13-cv-01870-JEB (D.D.C. Mar. 28, 2014), *available at* https://www.aclu.org/sites/default/files/assets/19._defendants_reply_in_further_support_of_motion_to_dismiss_2014.03.28.pdf [https://perma.cc/W7DR-D9UD].

claims that it has the authority to do so, but it has tied its own hands in this regard.

Perhaps this is the source of the frustration that members have expressed who want to air classified information to public scrutiny. Senator Leahy of the Senate Judiciary Committee noted, for instance, in wake of the leaks, that the President indicated that an opportunity presented itself "to have an open and thoughtful debate" about the surveillance issues. Leahy welcomed that statement,

> . . . because this is a debate that several of us on this committee, in both parties, have been trying to have for years. Like so many others, I'll get the classified briefings, but then of course you can't talk about them. There's a lot of these things that should be and can be discussed.[269]

It is somewhat disingenuous, however, to suggest that the Senate needed the President's permission to have a debate about the NSA's authorities. Leahy, if sufficiently concerned, could have used the Speech or Debate Clause to get the matter into the public record.

At the same time, it would be short-sighted to ignore political pressure—and the potential for actual censure under the Senate's own rules—for doing so.[270] Thus, the furthest legislators appear to have felt free to act with regard to the FAA has been to make general statements and broad objections.

At the renewal debates in the House, for instance, Representative Nadler argued in favor of making a declassified summary of FISC opinions including significant constructions of Section 702, saying, "Many American citizens and others who have nothing to do with foreign intelligence gathering are caught up in this surveillance, and government has an obligation to protect their rights."[271] He continued, "Disclosure of classified information is

---

269. *Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs Before the S. Comm. on the Judiciary*, 113th Cong. (2013) (opening statement of Sen. Patrick Leahy).

270. If a Member were to reveal classified information, it may also result in the Executive branch denying access to classified material to the Member in the future. This may potentially lead to a constitutional crisis, in light of Congress' oversight responsibilities.

271. 158 CONG. REC. H5892 (daily ed. Sept. 12, 2012) (statement of Rep. Jerrold Nadler).

not needed to know whether the court performs meaningful oversight of the executive branch, applies minimization standards correctly, and whether or not we ought to amend the law."[272] Representative Conyers advised one of his colleagues that the programs being conducted "unquestionably" affected "citizens on American soil," warning that "their communications are regularly intercepted."[273] Representatives in the House complained at the lack of transparency about how the powers were being exercised, and particularly the Director of National Intelligence's inability to estimate how many Americans' communications had been obtained.[274]

Senators Wyden and Udall, both members of the SSCI, tried to walk the line before and during the 2012 renewal debates of the FAA. In October 2012, they sent an open letter to General Keith Alexander, Director of the National Security Agency, requesting that he provide an unclassified clarification of the number of American communications intercepted under Section 702.[275] The senators opposed renewal of the legislation in committee. Senator Udall stated during the debates that he did not believe that Congress had "an adequate understanding of the effect this law has had on the privacy of law-abiding American citizens."[276] Senator Wyden offered an amendment during the debate, with the aim of making more information available, so as to better inform the public discourse.[277] Wyden's amendment would, *inter alia*, require the intelligence community to estimate the total number of communications to or from the United States acquired under Section 702, as well as the number of wholly domestic communications being collected, and any searches of the data using U.S. person information.[278] Wyden tried to convey the extent of the programs

---

272. 158 CONG. REC. H5892–93 (daily ed. Sept. 12, 2012) (statement of Rep. Nadler).

273. 158 CONG. REC. H5895 (daily ed. Sept. 12, 2012) (statement of Rep. John Conyers).

274. *See, e.g.*, 158 CONG. REC. H5893 (daily ed. Sept. 12, 2012) (statement of Rep. John Conyers); 158 CONG. REC. H5896 (daily ed. Sept. 12, 2012) (statement of Rep. Dennis Kucinich).

275. Letter from Ron Wyden and Mark Udall to General Keith Alexander, Director, NSA (Oct. 10, 2012), *reprinted in* 158 CONG. REC. S8458 (daily ed. Dec. 28, 2012).

276. 158 CONG. REC. S8458–59 (daily ed. Dec. 28, 2012) (statement of Sen. Mark Udall).

277. *Id.*

278. 158 CONG. REC. S8456 (daily ed. Dec. 28, 2012) (statement of Sen. Ron Wyden).

underway, without going into detail on either PRISM or upstream collection. As a member of the Intelligence Committee, he had access to information about the programs. But the way he couched his amendment was in the context of obtaining "yes or no answers" and furthering "real oversight."[279]

Senator Feinstein, rising in opposition, went further than Wyden in revealing classified programs, saying that although his amendment sounded benign, it was not:

> The goal of this amendment is to make information public about a very effective intelligence collection program that is currently classified. All of the information has already been made available to the Senate Intelligence and Judiciary Committees. It is available to all Members. All they have to do is read it. It is hundreds of pages of material.[280]

Feinstein went on to discuss incidental collection—and a series of closed hearings held by the Judiciary Committee in 2011 and 2012.[281]

To be sure, there are numerous logistical problems related to Congressional access to classified information. To read the material, legislators must go to a Sensitive Compartmented Information Facility (SCIF), set up for the purpose—a room tucked away in the capital, with limited access. Most Members do not have staff cleared to read the documents, so it must be the Members themselves, whose time is cabined, who review the hundreds of pages of materials. They are not allowed to remove material from the SCIFs; nor are they allowed to remove any notes they make about the material. All of this must remain under lock and key. As a result, as Wyden explained on the record, most Members of Congress remain "in the dark" about such programs.[282] But these considerations are not the responsibility of the Executive. They are in the purview of the legislature, as well as the broader context of national security concerns.

The final claim to address is whether Congress affirmatively approved of the program. Here, the facts speak for themselves.

---

279. *Id.*

280. 158 CONG. REC. S8456 (daily ed. Dec. 28, 2012) (statement of Sen. Dianne Feinstein).

281. *Id.* at S8456–57.

282. 158 CONG. REC. S8459 (daily ed. Dec. 28, 2012) (statement of Sen. Ron Wyden).

The legislature voted, and passed, reauthorization of the statute. Claims after the fact that they did not avail themselves of the opportunity to scrutinize the programs in question do not allow legislators to escape their responsibility to look into the matter before affirmatively continuing PRISM and upstream collection in 2012.

### *6. FISC Oversight of Targeting Procedures*

FISC first became aware of the implications of the NSA's interpretation of TFA in 2011.[283] The court was surprised by the government's admission that it would have to intercept significantly more content to scan it for relevant information. In its first Section 702 docket, the government had indicated that the acquisition of telephonic communications:

> would be limited to "to/from" communications—i.e., communications to or from a tasked facility. The government explained, however, that the Internet communications acquired would include both to/from communications and "about" communications—i.e., communications containing a reference to the name of the tasked account . . . . Based upon the government's descriptions of the proposed collection, the Court understood that the acquisition of Internet communications under Section 702 would be limited to discrete "to/from" communications between or among individual account users and to "about" communications falling within [redacted] specific categories that had been first described to the Court in prior proceedings.[284]

In reviewing and granting the application for an order, the court had not taken into account the NSA's acquisition of Internet

---

283. [Redacted], 2011 WL 10945618, at *5-6 (FISA Ct. Oct. 3, 2011), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-declassifies-intelligence-community-documents-regarding-collection-under-section-702-of-the-foreign-intelligence-surveillance-act-fisa [http://perma.cc/LTE7-9XBT]. This document was declassified by the Director of National Intelligence on August 21, 2013, along with a series of other documents, including, *inter alia*, [Redacted], 2011 WL 10947772 (FISA Ct. Nov. 30, 2011), [Redacted] [hereinafter Memorandum Opinion, Nov. 2011], 2012 U.S. Dist. LEXIS 189344 (FISA Ct. Sept. 25, 2012), and the 2011 MINIMIZATION PROCEDURES, *supra* note 171. All documents available at http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-declassifies-intelligence-community-documents-regarding-collection-under-section-702-of-the-foreign-intelligence-surveillance-act-fisa [http://perma.cc/LTE7-9XBT].

284. *Id.* at *5.

transactions, which "materially and fundamentally alter[ed] the statutory and constitutional analysis."[285]

FISC was troubled by the government's revelations—making it the third time in less than three years in which the NSA had disclosed a "substantial misrepresentation" on "the scope of a major collection program."[286] One of three possibilities held: the court was particularly slow, the government had been lying, or the government had made a mistake. Regardless, "[t]he government's submissions make clear not only that NSA has been acquiring Internet transactions since before the Court's approval of the first Section 702 certification in 2008, but also that NSA seeks to continue the collection of Internet transactions."[287]

FISC noted that it is a crime to "engage[] in electronic surveillance under color of law except as authorized" by statute or . . . to "disclose[] or use[] information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized" by statute.[288] Yet, to the extent that MCTs contained communications that the NSA was not supposed to collect (in other words, wholly domestic communications), this appeared to be precisely what had occurred with regard to the NSA's upstream collection.[289]

In its October 2011 memorandum opinion, the court confronted two areas: first, targeting procedures as applied to the acquisition of communications *other than* Internet transactions—that is, "discrete communications between or among the users of telephone and Internet communications facilities that are to or from a facility tasked for collection."[290] As in the past, the court found the targeting procedures with regard to non-Internet transactions to be sufficient. Second, the court considered *de novo* the sufficiency of the government's targeting procedures in relation to Internet transac-

---

285. *Id.*

286. *Id.* at *5 n.14. The court went on to cite the NSA's bulk acquisition of telephone metadata under Section 215; the second incident is entirely redacted.

287. *Id.* at *6 (footnote omitted).

288. *Id.* at *6 n.15 (quoting 50 U.S.C. § 1809(a) (2012).

289. The court stated that it would address the potential criminal violation in a separate order. *Id.* As of the time of writing, the order referenced in the October 2011 opinion has not been declassified.

290. *Id.* at *6.

tions.[291] Despite the acknowledgement by the government that it knowingly collected tens of thousands of messages of a purely domestic nature, FISC found the procedures consistent with the statutory language that prohibited the intentional acquisition of domestic communications.[292]

The court's analysis of the targeting procedures focused on upstream collection.[293] At the time of acquisition, the collection devices lacked the ability to distinguish "between transactions containing only a single discrete communication to, from, or about a tasked selector and transactions containing multiple discrete communications, not all of which may be to, from, or about a tasked selector."[294] The court continued: "As a practical matter, this means that NSA's upstream collection devices acquire any Internet transaction transiting the device if the transaction contains a targeted selector anywhere within it."[295] Because of the enormous volume of communications intercepted, it was impossible to know either how many wholly domestic communications were thus acquired or the number of non-target or U.S. persons' communications thereby intercepted.[296] The number of purely domestic communications alone was in the tens of thousands.[297]

Despite this finding, FISC determined that the targeting procedures were consistent with the statutory requirements that they be "reasonably designed" to (1) "ensure that any acquisition authorized under [the certifications] is limited to targeting persons reasonably believed to be located outside the United States" and (2) "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."[298]

To reach this conclusion, the court read the statute as applying, in any *particular* instance, to communications of individuals "*known at the time of acquisition* to be located in the United

---

291. *Id.* at *9–*13.
292. *Id.*
293. *Id.*
294. *Id.* at *10.
295. *Id.*
296. *Id.* at *11.
297. *Id.See also id.* at *13, *15–*16.
298. *Id.* at *13 (citing 50 U.S.C. §§ 1881a(d)(1), (i)(2)(B) (2012)).

States."[299] As the equipment did not have the ability to distinguish between purely domestic communications and international communications, the NSA could not *technically* know, at the time of collection, *where* the communicants were located. From this, the court was "inexorably led to the conclusion that the targeting procedures are 'reasonably designed' 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."[300] This was true despite the fact that the NSA was fully aware that it was collecting, in the process, tens of thousands of domestic communications.[301] As far as the targeting procedures were concerned, at least with regard to MCTs, the NSA had circumvented "the spirit" but not the letter of the law. [302]

The court's reading led to an extraordinary result. The statute bans the knowing interception of entirely domestic conversations. The NSA said that it knowingly intercepts entirely domestic conversations. Yet the court found its actions consistent with the statute.

A few points here deserve notice. First, it is not immediately clear why the NSA is unable to determine location at the moment of intercept and yet can ascertain the same at a later point. Second, in focusing on the technical capabilities of any discrete intercept, the court encouraged a form of willful blindness—that is, an effort to avoid criminal or civil liability for an illegal act by intentionally placing oneself into a position to be unaware of facts that would otherwise create liability.[303] In light of the court's interpretation,

---

299. *Id.* at *16 (citing 50 U.S.C. 1881a(d)(1)(B) (2012) (emphasis in original)). The full language of the section reads: "An acquisition authorized under subsection (a) . . . may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." 50 U.S.C. § 1881a(d)(1)(B) (2012).

300. [Redacted], 2011 WL 10945618, at *16 (FISA Ct. Oct. 3, 2011).

301. *Id.*

302. *Id.*

303. *Willful Blindness Law & Legal Definition*, US LEGAL, INC., http://definitions.uslegal.com/w/willful-blindness/ [http://perma.cc/JGW5-WFGC] (last visited June 25, 2014). The Supreme Court relatively recently acknowledged broad agreement among the circuits, applying the doctrine to a wide range of cases. Global-Tech Appliances, Inc. v. SEB S.A., 131 S. Ct. 2060 (2011). Two basic requirements mark the doctrine: the defendant must believe that there is a high probability that a fact exists, and the defendant must take deliberate actions to avoid learning of that fact. *Id.* at 2070.

the NSA has a diminished interest in determining at the point of intercept whether intercepted communications are domestic in nature. Its ability to collect more information would be hampered. So there is a perverse incentive structure in place, even though Congress intended the provision to protect individual privacy.

The Executive Branch kept Congress fully informed about FISC's concerns with regard to MCTs and the collection of domestic conversations. Senator Dianne Feinstein later noted that the Intelligence and Judiciary Committees had received more than 500 pages of information four days after Judge Bates' opinion, relating to the operation of Section 702.[304] Following receipt of the information (which addressed domestic communications and the knowing interception of U.S. persons' information), the Senate Intelligence Committee held a closed hearing at which the matter was discussed.[305] In December 2011, the committees received more than 100 more pages of related materials, which became the focus of another closed hearing on February 9, 2012.[306]

### *7. Law as Written Versus Law as Applied*

In terms of statutory interpretation and the knowing collection of wholly domestic conversations, Congress and FISC knew what was happening and allowed PRISM and upstream collection to continue. The situation thus could be read as one in which all three branches of the government agreed: Congress passed the FAA, the intelligence community interpreted and applied it, and the judiciary extended its blessing.

Nevertheless, in light of the highly classified nature of the programs, and their direct impact on individual rights, there is something troubling about having the only public portion of the authorities—the law—suggest one thing, when in reality the statute is being understood and applied in the opposite manner. In this case, for example, the statute's plain language suggests that a particularized judicial order is required to intercept U.S. persons' international communications and that the NSA may not knowingly intercept wholly domestic conversations. Yet FISC sanctioned the scanning and potential collection of significant portions of U.S.

304. 158 CONG. REC. S8457 (daily ed. Dec. 28, 2012) (statement of Sen. Feinstein).
305. *Id.*
306. *Id.*

persons' international communications, absent any particularized order, and it allowed the NSA to knowingly collect tens of thousands of wholly domestic conversations. Although national security is a matter of the highest importance, given the secrecy involved in the enterprise, one would expect a higher level of due diligence from those entrusted with oversight.

The targeting provisions also raise questions about the role in which Congress is placing FISC. In the FAA, Congress for the first time inserted a role for the court into the process of obtaining foreign intelligence outside the United States, but it also severely circumscribed FISC's authority. The court in some ways thus appears to be acting in the capacity of an oversight body, generally ensuring that procedures are in place and asking the NSA to police itself. Beyond the immediate question about the appropriate role for the court, as discussed above.[307]

### *B. Post-Targeting Analysis*

Section 702 makes it illegal to target someone outside the United States, where the purpose of the acquisition is to obtain information about a person known to be within domestic bounds. This practice, known as "reverse targeting," was central to Congressional debates.[308] Representative Langevin explained that the insertion of FISC would "ensure that the government's efforts are not aimed at targeting Americans, the so-called reverse targeting that we're all concerned about; and that if an American's communications is [sic] inadvertently intercepted, it is dealt with in a manner that guarantees legal protections."[309]

Despite Congress' concern about reverse targeting, the NSA instituted and the FISC approved a rule change in October 2011 to make it possible to query the content of communications obtained under Section 702 using U.S. person names and identifiers for information obtained via PRISM and upstream telephony collec-

---

307. *See supra* Part II.A.6.

308. *See, e.g.*, 154 CONG. REC. H5757 (daily ed. June 20, 2008) (letter from Michael B. Mukasey, Attorney Gen, & J. M. McConnell, Dir. Of Nat'l Intelligence, to Nancy Pelosi, Speaker, House of Representatives); 154 CONG. REC. H5740 (daily ed. June 20, 2008) (statement of Rep. McGovern); 154 CONG. REC. H5762 (daily ed. June 20, 2008) (statement of Rep. Harman).

309. 154 CONG. REC. H5766 (daily ed. June 20, 2008) (statement of Rep. Langevin).

tion.[310] The relevant definition in the 2011 minimization procedures is largely consistent with its 2009 predecessor:

> Identification of a United States person means the name, unique title, address, or other personal identifier of a United States person in the context of activities conducted by that person or activities conducted by others that are related to that person. A reference to a product by brand name, or 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.[311]

The NSA may query data obtained under Section 702 by using the names, titles, or addresses of U.S. persons, or any other information that may be related to the individual and his or her activities. If the intelligence community would like to query the data based on, for instance, membership in the Council on Foreign Relations—on the grounds that such queries are likely to yield foreign intelligence information—it may now do so.

In March 2014, the Director of National Intelligence, James Clapper, confirmed in a letter to Senator Ron Wyden that the

---

310. 2011 MINIMIZATION PROCEDURES, *supra* note 171, at § 3(b)(6). *See also* James Ball & Spencer Ackerman, NSA loophole allows warrantless search for U.S. citizens' emails and phone calls, GUARDIAN, Aug. 9, 2013, http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls [http://perma.cc/DQN8-YEY7] ("'While the FAA 702 minimization procedures approved on 3 October 2011 now allow for use of certain United States person names and identifiers as query terms when reviewing collected FAA 702 data . . . analysts may NOT/NOT [not repeat not] implement any USP [U.S. persons] queries until an effective oversight process has been developed by NSA and agreed to by DOJ/ODNI." (quoting NSA glossary document); De, *supra* note 9, at 30–31 ("[T]o clarify, U.S. person queries are not allowed under what I described as upstream collection." And "Such a query, and we're talking about PRISM collection, must be reasonably likely to return foreign intelligence information."). *But see* 2011 MINIMIZATION PROCEDURES, *supra* note 171, at § 3(b)(6); PCLOB REPORT, *supra* note 2, at 57 (clarifying that it is not all upstream collection removed from U.S. person identifier queries, but only Internet content).

311. 2009 MINIMIZATION PROCEDURES, *supra* note 169, at § 2. *Compare id.* at § 2, *with* 2011 MINIMIZATION PROCEDURES, *supra* note 171, at § 2. This definition appears to be consistent with the legislative history of FISA. *See, e.g.*, 124 CONG. REC. 33,685, 33,783 (1978) (conference report and statement filed in House by Rep. Boland) ("The procedures regarding the national defense or foreign affairs information apply to the identity of any United States person, rather than individuals only. The conferees agree that the adjectival use of the name of a United States person entity, such as the brand name of a product, is not restricted by this provision because such information is publicly available.").

NSA had queried Section 702 data "using U.S. person identifiers."[312] The following month, the NSA's Privacy and Civil Liberties Officer reiterated Clapper's statement.[313] Pressed during a June 2014 hearing for the number of queries using U.S. person identifiers, Clapper responded by noting that in 2013, the NSA approved 198 U.S. person identifiers for querying the content of Section 702 communications, even as it queried Section-702-acquired metadata approximately 9,500 times.[314]

FISC has upheld the reading of the statute supporting use of U.S. person identifiers.[315] In its October 2011 opinion, the Court explained:

> The procedures previously approved by the Court effectively impose a wholesale bar on queries using United States–Person identifiers. The government has broadened Section 3(b)(5) to allow NSA to query the vast majority of its Section 702 collection using United States-Person identifiers, subject to approval pursuant to internal NSA procedures and oversight by the Department of Justice. Like all other NSA queries of the Section 702 collection, queries using United States-person identifiers would be limited to those reasonably likely to yield foreign intelligence information.[316]

The Court did not find this problematic. Because the collection of the information centered on non-U.S. persons located outside the country, it would be less likely, in the aggregate, "to result in the acquisition of nonpublic information regarding non-consenting United States persons."[317]

---

312. Letter from James R. Clapper, Dir. Nat'l Intelligence, to Sen. Ron Wyden (Mar. 28, 2014), *available at* https://www.documentcloud.org/documents/1100298-unclassified-702-response.html [http://perma.cc/HY6F-DLUF].

313. NSA'S IMPLEMENTATION REPORT, *supra* note 170, at 7 ("Since October 2011 and consistent with other agencies' Section 702 minimization procedures, NSA's Section 702 minimization procedures have permitted NSA personnel to use U.S. person identifiers to query Section 702 collection when such a query is reasonably likely to return foreign intelligence information.").

314. Letter from James R. Clapper, Dir. Nat'l Intelligence, to Sen. Ron Wyden (June 27, 2014), at 2, *available at* http://www.wyden.senate.gov/download/?id=184D62F9-4F43-42D2-9841-144BA796C3D3&download=1 [http://perma.cc/N769-3VR7]. *But see* PCLOB REPORT, *supra* note 2, at 57 (noting that ODNI and NSD consider this number to be overinclusive).

315. [Redacted], 2011 WL 10945618, at *7–8 (FISA Ct. Oct. 3, 2011).

316. *Id.* at *7.

317. *Id.*

As a practical matter, what this rule change means is that U.S. person information that is incidentally collected via Section 702 can now be mined using U.S. person information as part of the queries. This circumvents Congress's requirements in Sections 703 and 704 that prior to U.S. person information being obtained (and therefore prior to it being analyzed), the government be required to appear before a court to justify placing a U.S. person under surveillance.

An even more serious consequence arises in the context of criminal law. The FBI stores unminimized Section 702 data together with information obtained from traditional FISA orders, allowing agents to search both caches of information simultaneously.[318] FBI queries of Section 702 information may have nothing to do with threats to U.S. national security. PCLOB explains, "With some frequency, FBI personnel will . . . query [Section 702] . . . data . . . in the course of criminal investigations and assessments that are unrelated to national security efforts."[319] The FBI is subject to no oversight in the process; the Bureau does not track the number of queries of Section 702 data using U.S. person identifiers.[320]

In light of the significant amount of U.S. person communications obtained through Section 702 collection, the impact of the FBI's policy on citizens' privacy is not insubstantial. It is thus rather surprising that PCLOB summarily dismissed the implications, stating, without citation or supporting evidence: "Anecdotally, the FBI has advised the Board that it is extremely unlikely that an agent or analyst who is conducting an assessment of a non-national security crime would get a responsive result from the query against the Section 702-acquired data."[321]

PCLOB's response rather misses the point, which is that the targeting and use provisions work together to allow the intelligence community to bypass restrictions introduced in Sections 703 and 704, as well as ordinary criminal law.

---

318. *Id.*
319. *Id.*
320. PCLOB REPORT, *supra* note 2, at 59.
321. *Id.* at 59–60.

### *C. Retention and Dissemination of Data*

One of the most concerning issues that arises in regard to the retention and dissemination of data obtained under Section 702 is that the NSA may indefinitely retain encrypted communications. In light of increasing public and private use of encryption, the exception may soon swallow the rule, resulting in fewer protections for individual and consumer privacy. In addition, the NSA's minimization procedures allow for incidental information to be kept, analyzed, and distributed if found relevant to the authorized purpose of the acquisition under one of two conditions: first, as containing foreign intelligence information, and, second, as containing evidence of a crime.[322] The former is anchored in traditional FISA and critical for U.S. national security. The latter is similarly consistent with traditional FISA; however, lacking the same procedural protections that attend searches under Titles I and II of the statute, use of information obtained under Section 702 for criminal prosecution raises important constitutional questions.

#### *1. Retention of Encrypted Communications*

For domestic communications, the NSA retains information that contains technical data base information and data necessary to assess communications security vulnerabilities.[323] The minimization procedures explain that in the context of cryptanalytics, "maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning."[324] Unlike unencrypted communications, which are retained for five years from the date of the certification authorizing the collection (unless the NSA decides otherwise), encrypted communications may be retained for "any period of time during which encrypted material is subject to, or of use in, cryptanalysis."[325]

---

322. 2009 MINIMIZATION PROCEDURES, *supra* note 169, at § 2(f); *see also* FACT SHEET ON SECTION 702, *supra* note 215 ("Any inadvertently acquired communication of or concerning a US person must be promptly destroyed if it is neither relevant to the authorized purpose nor evidence of a crime.").

323. 2011 MINIMIZATION PROCEDURES, *supra* note 171, at § 5(3). *See also* 2009 MINIMIZATION PROCEDURES, *supra* note 169, at § 5(3).

324. 2011 MINIMIZATION PROCEDURES, *supra* note 171, at § 5(3)(a).

325. *Id.*

For foreign communications of or concerning U.S. persons, the NSA retains encrypted material "for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement."[326] There is no limit on the amount of time that encrypted information may be kept, as long as it continues to be subject to, or of use in, cryptanalysis.[327]

The logic behind the default is that the government should not be forced to purge data merely because it does not hold the key or has been unable to break the code. Considering the likelihood that bad actors may try to use encryption to hide the contents of their communications, the intelligence community does not want to put itself at a disadvantage.

The problem is that it is not just bad actors who encipher messages. U.S. citizens and private industry are increasingly using encryption to try to protect their materials and communications. Windows, for instance, has an Encrypting File System that can be used to store information in an encrypted format. Systems like Pretty Good Privacy (PGP) can be set up and installed using a Firefox plugin, making it easy to encrypt e-mail. In March 2014, Google announced that it is now using https encrypted communications *whenever* users log in to Gmail, regardless of which Internet connection they are using.[328] Nicolas Lidzborski, Gmail's Security Engineering Lead explained:

> Today's change means that no one can listen in on your messages as they go back and forth between you and Gmail's servers—no matter if you're using public WiFi or logging in from your computer, phone or tablet. In addition, every single email message you send or receive—100% of them—is encrypted while moving internally. This ensures that your messages are safe not only when they move be-

326. *Id.* at § 6(a)(1).

327. *Id.* at § 6(a)(1)(a).

328. Nicolas Lidzborski, Staying at the forefront of email security and reliability: HTTPS-only and 99.978% availability, OFFICIAL GMAIL BLOG (Mar. 20, 2014), available at http://gmailblog.blogspot.com/2014/03/staying-at-forefront-of-email-security.html [http://perma.cc/5GXL-R9SW]; *see also* Lily Hay Newman, Now Gmail Encrypts Every Email. Other Services Should, Too., SLATE (Mar. 21, 2014, 2:57 PM), available at http://www.slate.com/blogs/future_tense/2014/03/21/gmail_will_now_encrypt_all_of_the_traffic_between_google_servers_to_make.html [http://perma.cc/J9QC-VDJ4].

> tween you and Gmail's servers, but also as they move between Google's data centers—something we made a top priority after last summer's revelations.[329]

The irony of Google's actions in light of the NSA's retention policies is hard to miss: in part because the NSA was intercepting Gmail and reading it (at which point the agency was required under minimization procedures to eliminate irrelevant information), the company now encrypts *all* communications, with the result that the NSA can still collect Gmail, but it can now keep it indefinitely, simply because it is encrypted at the front end. Assuming that the NSA has the tools to decrypt the communications, it is unclear how this provides greater protections for U.S. persons' privacy. Nevertheless, in light of Google's new policy, and calls from consumers for other companies to follow suit,[330] it seems that this practice may become standard.

Not only are we seeing greater individual use of encryption, but companies generally are also looking for ways to ensure the security of their data. The cost of enabling hardware encryption capabilities is falling: from $100 in 2009, by 2012, the cost of enabling hardware encryption capabilities to hard disk drives had plummeted to $15.[331] Simultaneously, a series of data breaches and their enormous cost to companies (quite apart from questions related to international consumer confidence in U.S. companies post-June 2013), encouraged industry to make greater use of encryption.[332] According to a recent market research report, the

---

329. Lidzborski, *supra* note 328.

330. Newman, *supra* note 328.

331. *Hardware Encryption Market - by Algorithms (AES, RSA), Architectures (FPGA, ASIC), Products (Hard Disk Drives, USB Drives and In-Line Encryptors), Applications, Verticals and Geography - Analysis & Forecast (2013 – 2018)*, MARKETSANDMARKETS, July 2013, available at http://www.marketsandmarkets.com/Market-Reports/hardwar.e-based-encryption-systems-market-1115.html [http://perma.cc/VC6G-WYA6].

332. Verizon, for instance, documented 198 data breaches in 2013 in retail, accommodation and food industries. Many of these attacks were on major retailers, such as Michaels, Neiman Marcus, Nordstrom, and Target, affecting millions of people. The Target breach in December 2013, for instance, impacted 70 million customers. Robert Westervelt, *Despite Prominent Retail Breaches, POS System Attacks Decline, Report Finds*, CRN (Apr. 22, 2014, 5:26 PM), *available at* http://www.crn.com/news/security/300072595/despite-prominent-retail-breaches-pos-system-attacks-decline-report-finds.htm [http://perma.cc/5WZ9-B5PG]; *see also*, Nicole Perlroth, *Latest Sites of Breaches in Security Are Hotels*, N.Y. TIMES (Jan. 31, 2014), *available at* http://www.nytimes.com/2014/02/01/technology/latest-sites-of-

hardware encryption market is expected to reach some $166.67 billion by 2018, growing at an incredible CAGR of 62.17% from 2013 to 2018.[333] These trends call attention to the NSA's back-end retention policies with regard to encrypted materials.

### *2. Use of Section 702 Data in Criminal Prosecution*

NSA's minimization procedures place a duty on the NSA to turn over any information regarding the commission of a crime to law enforcement agencies, if the NSA would like to retain the information.[334] In light of front-end considerations (the inclusion of information "about" selectors/targets and the assumption of non-U.S. person and overseas status), U.S. persons' international and, at times, domestic communications can be monitored, collected, and used against them in a court of law, without law enforcement ever satisfying Title III requirements. Neither individualized suspicion nor insertion of a neutral, third-party magistrate characterizes Section 702 collection. U.S. persons may not themselves be in direct contact with any of the approved targets under Section 702. And query of databases using U.S. person identifiers may further implicate U.S. persons in criminal activity—even acts unrelated to national security. But no individualized judicial process is required. Courts have in the past found applications under traditional FISA sufficient.[335] But Section 702 includes none of these protections, giving rise to both statutory bypass and Fourth Amendment concerns.

## III. FOREIGN INTELLIGENCE AND THE FOURTH AMENDMENT

The Fourth Amendment of the U.S. Constitution provides:

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

---

breaches-in-security-are-hotels.html?_r=0 [http://perma.cc/32XF-YGKA]; Robert Westervelt, *High-Profile Retailer Data Breaches Prompt Security Discussion, Say Providers*, CRN (Jan. 14, 2014), *available at* http://www.crn.com/news/security/240165398/high-profile-retailer-data-breaches-prompt-security-discussion-say-providers.htm [http://perma.cc/3NMQ-HW8Z].

333. *Hardware Encryption Market*, *supra* note 331.

334. 2009 MINIMIZATION PROCEDURES, *supra* note 169, at § 6(1)(3).

335. H.R. REP. NO. 95-1720, at 32 (1978).

> particularly describing the place to be searched, and the persons or things to be seized.[336]

What this language means, as a matter of criminal law, is that outside of a limited number of exceptions,[337] the search of an individual's home, office, or communications is presumptively "unreasonable" (and therefore unconstitutional), unless the government first obtains a warrant from a magistrate. The warrant must be based on a finding that the government has probable cause to believe that a crime has been, is being, or will be committed and that a search will uncover evidence relevant to the suspected crime.[338]

In 1972 the Supreme Court recognized that domestic security may merit a different Fourth Amendment standard than criminal law. By signaling deference to the political branches, the Court acknowledged that in foreign intelligence, constitutional provisions enter into tension: those related to foreign affairs, and those involved in investigations. For the former, separation of powers considerations have a role to play. While the Fourth Amendment might set an outside limit with regard to reasonableness, actions of the legislature may be imbued with constitutional meaning.

In 1972, *United States v. U.S. District Court for the Eastern District of Michigan.*[339] (commonly referred to as "*Keith*") left open the question of what would be constitutionally sufficient for the domestic surveillance of foreign powers or their agents.[340] In the absence of statutory guidance, lower courts began to recognize a foreign intelligence exception to the warrant requirement. These cases were rooted in U.S. foreign relations and the President's foreign affairs powers.

But the President shares foreign affairs authority with the legislature, and in 1978, Congress answered the invitation extended in

---

336. U.S. CONST. amend. IV.

337. *See, e.g.*, Chimel v. California, 395 U.S. 752 (1969); Terry v. Ohio, 392 U.S. 1 (1968); McDonald v. United States, 335 U.S. 451 (1948); Carroll v. United States, 267 U.S. 132 (1925).

338. Katz v. United States, 389 U.S. 347, 357 (1967) ("[S]earches conducted outside the judicial process, without prior approval by a judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.") (citations omitted).

339. 407 U.S. 297 (1972).

340. *Id.* at 308.

*Keith* by introducing FISA. It went beyond domestic security matters to include all surveillance of foreign powers or their agents, thus supplanting the exception that the courts had begun to articulate with a new standard. Congress crafted the legislation to ensure that domestic electronic foreign intelligence collection could not proceed absent prior judicial review, demonstration of probable cause, and particularity. FISA was to be the sole means via which domestic electronic intercepts could be conducted.

In the intervening years, not a single court has articulated a domestic foreign intelligence exception to the warrant requirement.[341] FISA, as informed by separation of powers, is the *de facto* Fourth Amendment standard for the contours of the warrant clause for electronic intercepts on U.S. soil.

As a matter of the interception of international communications, the Supreme Court has held that the Fourth Amendment does not apply to non-U.S. persons, who do not have a strong attachment to the United States.[342] The government is not required to obtain a warrant prior to conducting searches of such individuals outside domestic bounds. Prior to the 2008 FAA, neither was the government required to obtain a warrant, or anything even approximating a warrant, for the surveillance of U.S. persons overseas.

Sections 703 and 704 of the FAA altered the *status quo*, requiring the government to go to a court to obtain an individualized order, prior to targeting a U.S. person overseas. This shift carried constitutional meaning. Congress itself was intensely aware that in passing the FAA, it was invoking its authority under separation of powers doctrine, to limit the scope of executive action when it came to gathering foreign intelligence.

One could argue that programmatic collection (leading to the incidental collection of significant amounts of U.S. persons' communications), TFA, and the monitoring of unrelated communications embedded in MCTs run contrary to Congressional

---

341. FISCR was the first court to hold in the intervening years that a foreign intelligence exception exists overseas. In re Directives, No. 08-01, Aug. 2008, at 14-15 (acknowledging "a foreign intelligence exception to the warrant requirement for surveillance undertaken for national security purposes and directed at a foreign power or an agent of a foreign power reasonably believed to be located outside the United States.").

342. United States. v. Verdugo-Urquidez, 494 U.S. 259, 274–75 (1990).

intent under Sections 703 and 704. That is, if Congress intended U.S. persons to have a higher level of protection by inserting a neutral judicial magistrate to issue an individualized order (based on some level of suspicion of wrongdoing) for electronic surveillance, then the collection of significant amounts of U.S. persons' communications without these safeguards acts as an end-run around the protections. Under *Youngstown*, this would mean that the executive branch's actions should be considered at the lowest ebb.

The problem with this argument is that even if it might have been true in 2008, certainly by the time of the renewal debates, there was enough information available to Congress about how the executive branch was using the provisions. The decision to continue the powers at that point brought the executive branch's actions, at least insofar as the warrant clause is concerned, to the highest tier of Jackson's concurrence.

The Court's deference, however, extends only insofar as a warrant is required for the collection of foreign intelligence.[343] It does not extend to the querying of information for law enforcement purposes, for the simple reason that, at that point, foreign affairs are no longer relevant. Queries occur well within the realm of criminal law, where the Court has long insisted on a warrant, outside of limited exceptions. Nor do foreign affairs considerations reach the reasonableness component of the Fourth Amendment.

For the former, the failure of the executive to obtain prior judicial authorization, upon a showing of particularity, falls outside constitutional constraints.

For the latter, the test is one of the totality of the circumstances. The significant governmental interest in national security must be weighed against the potential intrusion into U.S. persons' privacy. The whole picture matters, including programmatic collection (resulting in the monitoring and collection of significant amounts of U.S. persons' communications), the scanning of content for information "about" selectors/targets, and the interception of non-relevant communications as part of MCTs. Equally important are

343. There are good reasons for this, such as the impracticality of obtaining warrants overseas, the problem of extending the jurisdiction of domestic courts, the diplomatic implications of extraterritorial actions, the need for stealth and secrecy, the potential for foreign corruption, and the demands of national security.

the protections built into the system at the back-end, to limit the acquisition, use, dissemination, and retention of U.S. persons' communications. In light of this analysis, the manner in which Section 702 has been implemented falls outside constitutional boundaries.

### *A. Application of the Warrant Clause in the United States*

The criminal law standard for electronic intercepts derives from *Katz v. United States*,[344] in which the Court confronted the impact of new technologies on the government's ability to listen to private communications. Recognizing the intrusive potential of electronic bugs, the Court determined that the Fourth Amendment "protects people, not places."[345] Justice Potter Stewart, writing for the majority, explained: "What a person knowingly exposes to the 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."[346] The "presence or absence of a physical intrusion" mattered naught.[347] Wiretapping transgressed the reasonable expectation that the government would not intercept telephone calls. To act within the contours of the Fourth Amendment, the government must first obtain a warrant, based on a judicial finding of probable cause.[348]

*Katz* dealt with the interception of domestic telephone conversations in a criminal context. It did not address whether and to what extent analyses change based on the purpose of the intercept (for example, criminal law, domestic security, foreign intelligence, or military), the legal status of the individuals whose conversations are being intercepted (U.S. person v. non-U.S. person), or the location of the search and seizure (that is, whether the interception takes place wholly within the United States, between the United States and overseas, or entirely overseas).

---

344. 389 U.S. 347 (1967).
345. *Id.* at 351.
346. *Id.* at 351–52 (citation omitted).
347. *Id.* at 353.
348. *Id.* at 358.

### *1. Criminal Law Versus Domestic Security*

Following *Katz*, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act to govern domestic telephone wiretaps for ordinary criminal investigations.[349] The law created prior judicial authorization and established the circumstances under which an intercept order could be issued. It requires the court to find probable cause that an enumerated offense has been, is being, or is about to be committed; probable cause that communications regarding the offense will be obtained through the intercept; and probable cause that the facilities to be placed under surveillance are to be used in conjunction with the enumerated offense or by the individual suspected of wrongdoing.[350] The officer applying for the warrant must establish that normal investigative procedures have been tried and have failed, (or appear to be unlikely to succeed if tried), or to be too dangerous to try.[351] The applicant must specify the person, location, and type of communications, as well as the length of the interception (with a thirty day limit).[352] The legislation restricts wiretaps to the investigation of certain specified crimes.[353]

Congress excluded matters related to foreign affairs from Title III, reserving to the President the latitude necessary to act in this domain. The statute explains,

> Nothing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities.[354]

---

349. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III § 802, 82 Stat. 212 (1968) (codified as amended at 18 U.S.C. §§ 2510–20 (2012)).

350. *See* 18 U.S.C. § 2518 (2012).

351. *Id.* § 2518(1)(c).

352. *Id.* § 2518(5).

353. The crimes include, *inter alia*, espionage, sabotage, treason, murder, kidnapping, extortion, and counterfeiting—all of which are associated with terrorism and threats posed to public safety. *See id.* § 2516.

354. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 212, 214 (1968).

The collection of foreign intelligence was a concomitant of the President's foreign affairs power.[355]

Legislators were careful to note during passage of Title III that this language neither amounted to an affirmative grant of authority nor limited the President's foreign affairs powers. The only exchange on this provision of Title III took place between Senator John McClellan (D-AR), who sponsored the bill, and Senators Spessard Holland (D-FL) and Gary Hart (D-CO):

> Mr. Holland: [The section] does not affirmatively give any power . . . We are not affirmatively conferring any power upon the President. We are simply saying that nothing herein shall limit such power as the President has under the Constitution . . . We certainly do not grant him a thing. There is nothing affirmative in this statement.
>
> Mr. McClellan: Mr. President, we make it understood that we are not trying to take anything away from him.
>
> Mr. Holland: The Senator is correct.
>
> Mr. Hart: Mr. President, there is no intention here to expand by this language a constitutional power. Clearly we could not do so.
>
> Mr. McClellan: Even though intended, we could not do so.
>
> Mr. Hart: . . . However, we are agreed that this language should not be regarded as intending to grant any authority, including authority to put a bug on, that the President does not have now. In addition, Mr. President, as I think our exchange makes clear, nothing in [this section] even attempts to define the limits of the President's national security power under present law . . . .[356]

One reason that question regarding the contours of Title III, and its implications for the President's foreign affairs powers, could even arise is because, consistent with separation of powers doctrine, legislative action could affect the latitude constitutionally afforded to the executive branch. This is at the heart of Jackson's concurrence in *Youngstown*.

---

355. United States v. U.S. Dist. Court for E. Dist. of Mich., 407 U.S. 297, 310–12 (1972).

356. 114 CONG. REC. 14751 (1968). The Senate Judiciary Committee Report similarly noted that the national security power of the President—whatever its contours might be, "is not to be deemed disturbed. S. REP. NO. 90-1097, at 65, *reprinted in* 1968 U.S.C.C.A.N. 2112, 2183.

Questions about what standards should govern the collection of intelligence for national security purposes (as opposed to ordinary law enforcement) arose in *Katz*. Justice Byron White, in his concurrence, suggested that the presumption against warrantless searches could be overcome by pressing need.[357] Justice William O. Douglas, joined by Justice William J. Brennan, strongly objected: "Neither the President nor the Attorney General is a magistrate. In matters where they believe national security may be involved they are not detached, disinterested, and neutral as a court or magistrate must be."[358] For Douglas, the executive branch was given the responsibility of "vigorously investigat[ing] and prevent[ing] breaches of national security and prosecut[ing] those who violate the pertinent federal laws."[359] This hardly qualified for neutral observation.[360]

*Katz* ultimately left open the question of "[w]hether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security."[361] In 1972 the Supreme Court took up this question insofar as domestic security was concerned in *Keith*.[362] The case centered on the warrantless wiretap of three individuals suspected of conspiring to bomb the Central Intelligence Agency.[363] In an 8–0 decision, the Court held that in this circumstance, government officials were required to obtain a warrant. The "inherent vagueness of the domestic security concept" and the potential for its abuse to squash political dissent underscored the importance of the Fourth Amendment when the government placed its own citizens under

357. Katz v. United States, 389 U.S. 347, 363–64 (1967) (White, J., concurring) ("We should not require the warrant procedure and the magistrate's judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable.").

358. *Id.* at 359 (Douglas, J., concurring).

359. *Id.* at 359–60.

360. *Id.* at 360 ("Since spies and saboteurs are as entitled to the protection of the Fourth Amendment as suspected gamblers like petitioner, I cannot agree that where spies and saboteurs are involved adequate protection of Fourth Amendment rights is assured when the President and Attorney General assume both the position of adversary-and-prosecutor and disinterested, neutral magistrate.").

361. *Id.* at 358 n.23 (majority opinion).

362. United States v. U.S. District Court, 407 U.S. 297, 308 (1972).

363. *Id.* at 299.

surveillance.[364] Technology presented a double-edged sword: while the government had the responsibility to ensure the safety of the people, and it would be "contrary to the public interest" for the Government to deny itself the use of new tools that could be used against it, neither was it in the people's best interest to give the government untrammeled access to new technologies.[365]

Justice Powell's arguments in *Keith* echoed those of Douglas in *Katz*: "Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch."[366] The Court determined that some sort of "prior judicial approval" was "required."[367] But the judiciary left it to Congress to determine what standards would be sufficient for Fourth Amendment purposes.[368] The Court explained, "Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."[369] In criminal law, "probable cause" was the standard against which the constitutional mandate of "reasonableness" was weighed.[370] But for domestic intercepts the showing of probable cause might reflect different requirements, alleging instead "other circumstances more appropriate to domestic security cases."[371] Congress may prefer "that the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court."[372] The time and reporting requirements need not be as strict as those in Title III.[373] The Court made it clear that Congress had the power to determine the contours of a domestic security warrant, within the outer limits of reasonableness; *that* a warrant of some sort was required provided a minimum.

---

364. *Id.* at 320.

365. *Id.* at 312.

366. *Id.* at 316–17.

367. *Id.* at 324.

368. *Id.* at 322 ("Congress may wish to consider protective standards for [domestic surveillance] which differ from those already prescribed for specified crimes in Title III.").

369. *Id.* at 322–23.

370. *Id.* at 323.

371. *Id.*

372. *Id.*

373. *Id.*

The Court was careful to limit its decision to cases involving "the domestic aspects of national security," adding, "[w]e have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents."[374]

### *2. The Domestic Foreign Intelligence Exception*

Before Congress could act, lower courts, looking to *Keith*, began to carve out a foreign intelligence exception to the warrant requirement for domestic surveillance of foreign powers and their agents. These cases dealt with matters at the core of the President's constitutional foreign affairs powers. They also drew a sharp line between the standards applied to intelligence gathering and those required in the course of criminal investigations.

One of the most important cases came on the heels of the Vietnam conflict and involved questions at the heart of U.S. international relations. David Truong, a Vietnamese citizen and the son of a prominent Vietnamese political figure, moved to the United States in 1965.[375] Eleven years later he met Dung Krall, a Vietnamese-American, who was married to a U.S. Naval Officer and had extensive contacts in France.[376] During the 1977 Paris negotiations between Vietnam and the United States, Truong asked Krall (who, unbeknownst to Truong, was a CIA informant), to carry classified documents to colleagues in Paris to pass on to the Socialist Republic of Vietnam.[377] Warrantless surveillance revealed that Truong was receiving the classified materials from Ronald Humphrey, an American citizen working at the United States' Information Agency.[378] Truong and Humphrey were convicted of espionage, as well as acting as agents of a foreign government without prior notification to the Secretary of State.[379]

The 4th Circuit agreed with the decision below, finding a domestic foreign intelligence exception to the warrant requirement, so long as the investigation was "primarily" focused on foreign

374. *Id.* at 321–22.
375. United States v. Truong, 629 F.2d 908, 911 (4th Cir. 1980).
376. *Id.*
377. *Id.* at 911–12.
378. *Id.*
379. *Id.* at 912.

intelligence.[380] At the point where the investigation turned criminal in nature, however, any information obtained without a warrant could be suppressed.[381]

The court, distinguishing its holding from *Keith*, explained that requiring a warrant for domestic foreign intelligence investigations would "unduly frustrate" the President in executing his foreign affairs powers: "[A]ttempts to counter foreign threats to the national security require the utmost stealth, speed, and secrecy."[382] The Fourth Circuit considered the courts ill-placed to second-guess the President. It wrote: "[T]he executive possesses unparalleled expertise to make the decision whether to conduct foreign intelligence surveillance, whereas the judiciary is largely inexperienced in making the delicate and complex decisions that lie behind foreign intelligence surveillance."[383]

The warrant exception stemmed from the foreign affairs component of executive power, outwardly directed at protecting U.S. national security.[384] Not only did the executive have the expertise, but, as a constitutional matter, it was the "pre-eminent authority in foreign affairs."[385] Flexibility, practical experience, and constitutional competence worked together to carve out an exception where foreign intelligence matters were concerned.

The Fourth Circuit was careful to limit its holding "to those situations in which the interests of the executive are paramount."[386] This meant that the object of the search or surveillance must be a foreign power or its agents. The foreign connection was critical. Similarly important was the point at which the surveillance moved to the criminal realm—in this case, the moment at which the criminal division at the Department of Justice became involved. The Court further noted that even if a warrant was not necessary, the Fourth Amendment still required that the surveillance be "reasonable."[387]

---

380. *Id.* at 915–16.
381. *Id.* at 912–13.
382. *Id.* at 913.
383. *Id.*
384. *Id.* at 913–14.
385. *Id.* at 914.
386. *Id.* at 915.
387. *Id.* at 916.

Other circuit courts, applying *Keith*, affirmed the existence of a domestic foreign intelligence exception to the warrant clause.[388] In *United States v. Butenko*, the Third Circuit recognized that the Constitution accorded the President foreign affairs powers.[389] It recognized the danger of allowing Fourth Amendment analysis "to be abandoned whenever the President asserts that a particular search and seizure is incident to the conduct of foreign affairs." [390] While national security threats may be "of immeasurable gravity," the court wrote, "there would seem to be nothing in the language of the Constitution to justify completely removing the Fourth Amendment's requirements in the foreign affairs field and, concurrently, imposing these requirements in all other situations."[391]

In *Butenko*, the Cold War context loomed large. The court convicted a Soviet national, Igor A. Ivanov, and U.S. citizen John Butenko of passing classified military documents to a foreign government and failing to notify the Secretary of State of their status as foreign agents.[392] The executive branch's decision to wiretap the two men stemmed from the President's foreign affairs power. The Third Circuit explained:

> As Commander-in-Chief, the President must guard the country from foreign aggression, sabotage, and espionage. Obligated to conduct this nation's foreign affairs, he must be aware of the posture of foreign nations toward the United States, the intelligence activities of foreign countries aimed

388. *See, e.g.*, United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977) ("Foreign security wiretaps are a recognized exception to the general warrant requirement."); United States v. Butenko, 494 F.2d 593, 606 (3d Cir. 1974) (finding a foreign intelligence exception); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973) ("[R]estrictions upon the President's power which are appropriate in cases of domestic security become artificial in the context of the international sphere."); United States v. Clay, 430 F.2d 165, 171 (5th Cir. 1970) (upholding warrantless foreign intelligence surveillance). The Second Circuit and the D.C. Circuit commented on the foreign intelligence exception but did not decide the question.

389. *Butenko*, 494 F.2d at 603.

390. *Id.* at 602–03. *See also* United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 314–15 (1936) (holding as constitutional Congress's delegation to the President of the authority to prevent the sale of weapons to countries engaged in hostilities).

391. *Butenko*, 494 F.2d at 603.

392. *Id.* at 596.

> at uncovering American secrets, and the policy positions of foreign states on a broad range of international issues.[393]

As the President exercised Article II foreign affairs authorities, he obtained broader latitude under the Fourth Amendment than he would otherwise have for matters involving ordinary law enforcement.

The Supreme Court has consistently held the view that where foreign affairs matters impacting international relations are involved, the executive may have more leeway.[394] In *United States v. Curtiss-Wright*, it explained:

> Not only . . . is the federal power over external affairs in origin and essential character different from that over internal affairs, but participation in the exercise of that power is significantly limited. In this vast external realm, with its important, complicated, delicate and manifold problems, the President alone has the power to speak or listen as a representative of the nation.[395]

The President, however, shares foreign affairs powers with Congress. To the extent, then, that the President is given greater latitude as an aspect of foreign affairs, so, too, may Congressional action affect the scope of the authority constitutionally afforded to the President.

### *3. Concurrent Authorities*

As a constitutional matter, the Executive is not the only branch to be entrusted with foreign affairs. To Congress is provided the ability to collect money to provide for the common defense, the authority to regulate commerce with foreign nations, and the power to define and punish piracies and felonies on the high seas.[396] It falls to the legislature to declare war.[397] Congress may raise and support armies, provide and maintain a navy, and make rules for the government and regulation of the same.[398] It may call forth and organize the militia,[399] and it

393. *Id.* at 608.
394. United States v. Curtiss-Wright Export Corp, 299 U.S. 304, 319 (1936).
395. *Id.*
396. U.S. CONST. art. I, § 8, cl. 1, 3, 10.
397. U.S. CONST. art. I, § 8, cl. 11.
398. U.S. CONST. art. I, § 8, cl. 12, 13, 14.
399. U.S. CONST. art. I, § 8, cl. 15, 16.

may "make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers."[400]

Concurrent authority means that the scope of action available to either party in some sense rests on the actions of the other. This notion lay at the heart of the Founders' concept of separation and balance of powers. Accordingly, Justice Jackson's third category in *Youngstown Sheet & Tube Co. v. Sawyer* contemplates the potential for the President to undertake measures "incompatible with the expressed or implied will of Congress."[401] In this circumstance, the courts should consider the President's power as "at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter."[402] Jackson warned:

> Courts can sustain exclusive presidential control in such a case only by disabling the Congress from acting upon the subject. Presidential claim to a power at once so conclusive and preclusive must be scrutinized with caution, for what is at stake is the equilibrium established by our constitutional system.[403]

In *Dames & Moore v. Regan*, the Court went on to discuss the three-part test based on Jackson's analysis in *Youngstown*.[404] It cautioned against an over-formalistic commitment to the framework, even as it recognized the value of thinking about concurrent authorities as a spectrum, within which actions by one branch influenced the scope of the authorities held by the other.

With this allotment in mind, the courts have traditionally recognized executive and legislative preeminence in foreign affairs and afforded the two branches a certain amount of deference with regard to related questions.[405] This does not mean that foreign af-

---

400. U.S. CONST. art. I, § 8, cl. 18.

401. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952) (Jackson, J., concurring).

402. *Id.*

403. *Id.* at 637–38.

404. 453 U.S. 654, 668–69 (1981).

405. *See, e.g.*, Chicago & S. Air Lines, Inc. v. Waterman S.S. Corp., 333 U.S. 103, 111 (1948) (stating that the courts should not interfere with the "delicate" and "complex" foreign policy decisions "wholly confided by our Constitution to the political departments of the government, Executive and Legislative"); United States v. Curtiss-Wright, 299 U.S. 304, 320 (1936) (noting the "very delicate, plena-

fairs powers are unlimited.[406] But it does suggest that on certain matters, the judiciary gives the political branches greater leeway. FISA represents one such moment, where an exercise of foreign affairs power carried constitutional meaning for the acceptable scope of Fourth Amendment protections.[407]

### *4. FISA Replacement of the Warrant Exception*

Congress responded to *Keith* by enacting the 1978 Foreign Intelligence Surveillance Act.[408] It went beyond the Supreme Court's holding by addressing questions related not just to domestic security (a subset of national security concerns) but also to foreign powers and agents thereof. Congress extended special protections to American citizens. The Courts have subsequently found FISA to be constitutionally sufficient for Fourth Amendment purposes.

For U.S. persons to fall within these categories (and thus to be targeted under the statute and subject to electronic surveillance), Congress required the government to demonstrate some level of

---

ry and exclusive power of the President as the sole organ of the federal government in the field of international relations").

406. *See, e.g.*, United States v. Robel, 389 U.S. 258, 264 (1967) ("It would indeed be ironic if, in the name of national defense, we would sanction the subversion of one of those liberties—the freedom of association—which makes the defense of the Nation worthwhile."); *Curtiss-Wright*, 299 U.S. at 320 (noting that foreign affairs powers of the President "must be exercised in subordination to the applicable provisions of the Constitution").

407. For examples of Constitutional provisions setting limits on the scope of the Fourth Amendment, see Whren v. United States, 517 U.S. 806, 813 (1996) (suggesting that the Equal Protection clause may cabin the reasonableness determination in Fourth Amendment analysis); New York v. P.J. Video, Inc., 475 U.S. 868, 874–875 (1986) (contemplating tension between First Amendment and Fourth Amendment standard of probable cause). *See also* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013) (highlighting potential First Amendment limits on Fourth Amendment search authorities).

408. *See, e.g.*, 124 CONG. REC. 36,409 (1978) (statement of Rep. Kastenmeier) ("Mr. Speaker, it has now been over 6 years since the Supreme Court in the famous Kieth [sic] case cast a cloud over current warrantless procedures for foreign intelligence surveillance. In that landmark decision Mr. Justice Powell writing for the court, specifically invited Congress, 'To consider protective standards . . . which differ from those already prescribed for specified crimes in Title III (of the Omnibus Crime Control and Safe Streets Act of 1968). Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of government for intelligence and the protected rights of our citizens.' Finally, after years of work by four congressional committees and two administrations, we have developed a bill . . . . ").

criminality and to submit to procedural protections that approximated the Fourth Amendment warrant requirement.

Traditional FISA defines "foreign power" in three ways: (a) foreign entities, (b) groups "engaged in international terrorism or activities in preparation therefor," and (c) entities not substantially composed of United States persons that are engaged in the international proliferation of weapons of mass destruction.[409] U.S. persons can only come within (b) and (c), and to qualify under either, some level of criminality must be involved: "International terrorism" means activities that involve violence or are dangerous to human life and are a violation of U.S. criminal law.[410] Similarly, the proliferation of weapons of mass destruction is a criminal act.

For a U.S. person to be considered an "agent of a foreign power," he or she must similarly engage in criminal activity.[411] The statute includes in this category 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 know-

409. 50 U.S.C. § 1801(a) (2012).

410. *Id.* § 1801(c).

411. For the definition of non-U.S. persons considered to be agents of a foreign power, see *id.* § 1801(b)(1).

> ingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).[412]

The acts that qualify U.S. persons as agents of foreign powers are criminal in nature.[413] Under traditional FISA, Congress further requires that the government demonstrate probable cause that U.S. persons come within one of the above categories.[414] The standard is slightly different than, but has largely the same effect as, the standards required under Title III.[415]

The courts have consistently upheld orders issued under FISA as constitutional. In *United States v. Cavanagh*, for instance, a defendant was indicted for attempting to deliver defense information to a foreign government.[416] His effort to suppress the fruits of the search, conducted under traditional FISA, met with zero success. The Ninth Circuit held, *inter alia,* that FISA properly provides for issuance of warrant by a detached judicial officer and that the statute satisfies the Fourth Amendment requirements of

---

412. *Id.* § 1801(b)(2) (emphasis added).

413. The first and second sections [(A) and (B)] require a violation of a criminal statute. Language in the statute referring to "sabotage" [(C)] is defined as a crime—in other words, "activities that involve a violation of [18 U.S.C. § 105], or that would involve such a violation if committed against the United States." *Id.* § 1801(d). Sections (D) and (E), above, would also require individuals to assume (or to aid, abet, or conspire another to assume) a fraudulent identity upon entering the United States—which will almost always be a crime because of the statutory regime governing customs and border entry.

414. Traditional FISA also requires that the government establish probable cause that the target is likely to use the facilities to be placed under surveillance.

415. Title III, at the time of its passage, regulated government interception of the contents of oral and wire communications involving the human voice (in other words, traditional telephone conversations). It did not apply to electronic communications, stored communications, or metadata associated with communications. To redress these deficiencies, in 1986, Congress introduced the Electronic Communications Privacy Act. *See* Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified in scattered sections of 18 U.S.C.). *See also* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, § 802, 82 Stat. 212 (1968) (codified as amended at 18 U.S.C. §§ 2510–22 (2012)); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, tit. II, § 201, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2701–11 (2012)); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, tit. III, § 301, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 3121–27 (2012)). For ordinary criminal warrants, the applicant must demonstrate probable cause that an individual is committing, has committed, or is about to commit a crime. For a traditional FISA order, the applicant for an order from FISC must demonstrate probable cause that an individual is a foreign power or an agent thereof—which, for a U.S. person, means some involvement in criminal activity.

416. 807 F.2d 787, 788 (9th Cir. 1987).

probable cause and particularity.[417] Similar challenges have met with the same result.[418]

While these cases center on situations in which foreign intelligence is the primary purpose of the interception of communications (and an order under traditional FISA was obtained prior to the collection), FISCR has gone further, stating that even where the primary purpose of the investigation is criminal in nature, the standards encapsulated in traditional FISA are sufficient for Fourth Amendment purposes. In *In re Sealed Case*, the FISA Court of Review found that the government had demonstrated probable cause to believe that the target, a U.S. person, was an agent of a foreign power and otherwise met the basic requirements of FISA.[419]

### *5. Recognition of FISA as a Constitutional Limit*

Acknowledging the concurrent authorities of the executive and legislative branches with regard to some aspects of foreign affairs, FISA nevertheless drew a sharp line at the border of the United States. The statute was to be the sole means via which the executive henceforward conducted *domestic* foreign intelligence (electronic) surveillance, as defined in FISA.[420]

Congress recognized the constitutional implications of the statute. During passage of the bill, the House wanted the text to state that the procedures established under its auspices represented the

---

417. *Id.* at 791–92.

418. *See, e.g.*, United States v. Duggan, 743 F.2d 59, 72–74 (2d Cir. 1984) (holding that traditional FISA does not violate the Fourth Amendment); *In re* Kevork, 634 F. Supp. 1002, 1010–14 (C.D. Cal. 1985) (same), *aff'd.* 788 F.2d 566 (9th Cir. 1986); United States v. Megahey, 553 F. Supp. 1180, 1185–92 (E.D.N.Y. 1982) (same); United States v. Falvey, 540 F. Supp. 1306, 1311–14 (E.D.N.Y. 1982) (same); *Duggan*, 743 F.2d at 75 n.5 ("A fortiori we reject defendants' argument that a FISA order may not be issued consistent with the requirements of the Fourth Amendment unless there is a showing of probable cause to believe the target has committed a crime."); United States v. Rosen, 447 F. Supp. 2d 538 (E.D. Va. 2006) (holding, related to Espionage Act prosecution, that disclosure of FISA orders was protected and that FISC had probable cause to believe that the targets were foreign powers or agents thereof).

419. 310 F.3d 717, 720 (FISA Ct. Rev. 2002) ("The government's application for a surveillance order contains detailed information to support its contention that the target . . . is aiding, abetting, or conspiring with others in international terrorism.").

420. Outside of electronic communications, other forms of domestic foreign intelligence collection fell subject to Exec. Order No. 12,333, 3 C.F.R. 200 (1981).

"exclusive statutory" means for the Executive Branch to conduct electronic surveillance, on the grounds that the President retained inherent surveillance powers outside the statute. The Senate rejected this view, saying that if the President were to engage in electronic surveillance outside of FISA, the Courts should consider the action to be consistent with category three of Justice Jackson's concurrence in *Youngstown*.[421] The Senate view carried.[422] Congress was aware that its actions were more than just setting a higher Fourth Amendment standard than the Court required. The statute carried constitutional meaning; and so Congress made an effort to communicate to the judiciary that further executive action should be evaluated in light of the constitutional meaning created by the new provision.

Congress went further to underscore its intent: FISA repealed the limitation previously noted in Title III, suggesting that Congress did not intend to limit the President's constitutional authorities.[423] FISA was Congress's express decision to curb executive power as a constitutional matter.

---

421. 343 U.S. 579 (1952).

422. *See* H.R. Rep. No. 95-1720, at 35 (1978) (Conf. Rep.) (quoting 343 U.S. at 637) ("Exclusive Means for Electronic Surveillance.—The Senate bill provided that the procedures in this bill . . . shall be the exclusive means by which electronic surveillance, as defined in this bill, and the interception of domestic wire and oral communications may be conducted. The House amendments provided that the procedures in this bill . . . shall be the exclusive statutory means by which the electronic surveillance as defined in this bill and the interception of domestic wire and oral communications may be conducted. The conference substitute adopts the Senate provision which omits the word 'statutory' . . . . The intent of the conferees is to apply the standard set forth in Justice Jackson's concurring opinion in the Steel Seizure Case: 'When a President takes measures incompatible with the express or implied will of Congress, his power is at the lowest ebb, for then he can rely only upon his own Constitutional power minus any Constitutional power of Congress over the matter.'").

423. *See* Foreign Intelligence Surveillance Act of 1978 (FISA), Pub. L. No. 95-511, § 201, 92 Stat. 1783 (1978), repealing 18 U.S.C. § 2511(3), stating, *inter alia*, "Nothing contained in [Title III] or in Section 605 of the Communications Act of 1934 shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government."; S. REP.

In order, then, for the Court to overturn FISA, it must disavow some amount of foreign affairs powers to Congress—a step the judiciary would be highly reluctant to take. Accordingly, in the thirty-six years that have elapsed since the introduction of FISA, the Courts have not once upheld a domestic foreign intelligence exception to the warrant requirement for foreign powers or agents thereof. Instead, it is to FISA itself that the Courts look to establish the Fourth Amendment standard for the warrant requirement when domestic electronic surveillance, as defined by FISA, is of moment.[424]

In 2008, Congress again emphasized that FISA was to be the exclusive means via which electronic surveillance, as defined in the statute, could be conducted. Congressional members underscored the importance of the exclusivity provision as a matter of constitutional, and not merely statutory, merit. Representative Reyes explained, "The language should in no way be read to imply that there is an inherent power to conduct surveillance beyond what is expressly authorized by statute."[425] California Representative Jane Harman, the ranking member of the House intelligence committee noted, "FISA is the exclusive means by which our government can conduct surveillance. In short, no more warrantless surveillance."[426] Representative

---

NO. 95-604, at 17 (1977) ("Most importantly, the disclaimer in 18 U.S.C. § 2511(3) is replaced by provisions that assure that [FISA], together with [Title III], will be the *exclusive* means by which electronic surveillance covered by [FISA], and the interception of wire and oral communications, may be conducted.") (emphasis in original). *See also* United States v. Biasucci, 786 F.2d 504, 508 n.4 (2d Cir. 1986) (noting exclusivity intent of Congress); United States v. Torres, 751 F.2d 875, 882 (7th Cir. 1984).

424. One could argue that the reason the Courts did not find a domestic foreign intelligence exception in the intervening years is simply because the executive branch conceded that it was required to act under FISA and did so. But this claim is not accurate. As addressed at the beginning of this Article, post-9/11, President Bush instituted the President's Surveillance Program, citing in support his Commander-in-Chief authorities as sufficient to overcome Fourth Amendment objections. Congress and at least one court found this claim to be unconstitutional. *See* ACLU v. NSA, 438 F. Supp. 2d 754 (E.D. Mich. 2006), *vacated on other grounds*, 493 F.3d 644 (6th Cir. 2007). The litigation weighed heavily in the Congressional debates on the FAA, in which the legislature went out of its way to condemn the warrantless surveillance on domestic soil and to extend special protections to citizens in their overseas communications.

425. 154 CONG. REC. H5758 (daily ed. June 20, 2008) (statement of Rep. Reyes).

426. 154 CONG. REC. H5762 (daily ed. June 20, 2008) (statement of Rep. Harman).

Langevin from Rhode Island, also a member of the Intelligence Committee, stated, "FISA is the exclusive means by which the executive branch may conduct electronic surveillance on U.S. soil. No President will have the power to do an end-run around the legal requirements of FISA."[427] Senator Feingold put the point most strongly, incredulous that the Bush Administration had invoked Article II "to override an absolutely clear, exclusive authority adopted by Congress pursuant to Justice Jackson's third tier of the test set out in his *Youngstown* opinion."[428]

Section 702 does not include a procedure approximating the warrant requirement in traditional FISA. Nor does it meet the standards set in Sections 703–704. Yet the NSA is using this provision to collect significant amounts of U.S. persons' communications. It is collecting information "about" targets. And it is monitoring non-relevant and, at times, entirely domestic communications that happen to be bundled in MCTs. We will return to these points in a moment.

### *B. Application of the Fourth Amendment Overseas*

Non-U.S. persons outside domestic bounds, who lack a "substantial connection" to the United States, do not benefit from the protection of the Fourth Amendment.[429] The reasoning underlying this decision raises difficult questions with regard to Section 702 authorities. Although the court has provided little guidance on what would satisfy the test, an appropriate approach to follow would be to require a legal relationship indicating membership in the political community. Physical or virtual contact alone is insufficient to satisfy the test. On the flip side, the courts should recognize that individuals do not, merely by engaging in

427. 154 CONG. REC. H5772 (daily ed. June 20, 2008) (statement of Rep. Langevin). *See also* 154 CONG. REC. H5767 (daily ed. June 20, 2008) (statement of Rep. Pelosi) (Noting that the legislation "makes absolutely clear that the enactment of an authorization for the use of force does not give the President, whoever he may be, any inherent authority to alter the requirements of FISA. Very important."); 154 CONG. REC. H5770 (daily ed. June 20, 2008) (statement of Rep. Hoyer) ("[T]his legislation makes clear that FISA is the exclusive means by which the government may conduct surveillance . . . . "); 154 CONG. REC. H5771 (daily ed. June 20, 2008) (statement of Rep. Udall) (noting the importance of the exclusivity clause).

428. 154 CONG. REC. S6382 (daily ed. July 8, 2008) (statement of Sen. Feingold).

429. United States v. Verdugo-Urquidez, 494 U.S. 259, 261 (1990).

global communications, waive their right to the protections of the Fourth Amendment.

There may be a reduced expectation of privacy in communicating directly with individuals targeted for foreign intelligence purposes. But there is no reduced expectation in communicating overseas generally—by accident or design—that would allow the government to monitor all U.S. persons' overseas communications for information "about" an individual or entity of interest. Simply by using e-mail, for instance, one does not assume the risk that the government will monitor the contents of that e-mail, should it happen to travel outside the United States.

### *1. Meaningful Contact as a Precursor*

In *Verdugo-Urquidez*, Chief Justice Rehnquist, writing for the Court, concluded that "the people" referred to in the Fourth Amendment indicated a particular group—not merely people *qua* people.[430] Rehnquist's reading stemmed from a deeply Aristotelian approach: in other words, one that emphasizes membership in the polis (πόλις), or political community, as a concomitant of forming a structure of government.[431] 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," for Rehnquist, 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."[432]

Although Justice Anthony Kennedy joined the Court's opinion, providing the critical fifth vote, in his concurrence he explicitly rejected Rehnquist's explanation of "the people."[433] Instead, Ken-

---

430. *Id.* at 265 (per curiam).

431. ARISTOTLE, POLITICS, BOOK I (350 BC), trans. by Benjamin Jowett, *available at* http://classics.mit.edu/Aristotle/politics.1.one.html [http://perma.cc/ERW5-T3AC]; *available in the Original Greek at* http://www.perseus.tufts.edu/hopper/text;jsessionid=91A85450747C74DF609D266E0A8DF8E5?doc=Perseus%3atext%3a1999.01.0057 [http://perma.cc/SPA2-LKNH].

432. 494 U.S. at 265 (per curiam).

433. *Id.* at 278 (1990) (Kennedy, J., concurring).

nedy relied on a more practical argument to find the petitioner's warrant clause assertion untenable:

> The absence of local judges or magistrates available to issue warrants, the differing and perhaps unascertainable conceptions of reasonableness and privacy that prevail abroad, and the need to cooperate with foreign officials all indicate that the Fourth Amendment's warrant requirement should not apply in Mexico as it does in this country.[434]

It was the infeasibility of obtaining a warrant overseas that made the warrant clause inapposite. Because of the distinction drawn by Kennedy in his rationale for joining the majority, lower courts have divided on whether to read *Verdugo-Urquidez* as a plurality opinion or not.[435]

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.[436] In *Martinez-Aguero v. Gonzalez*, a Mexican national with an expired visitor's visa went to the U.S. consulate in Mexico to obtain a new visa.[437] Directed to treat the old document as sufficient until the new one arrived, the woman came to the United States to visit her mother. The Fifth Circuit determined that she had sufficient connections to benefit from the protections of the Fourth Amendment as she crossed the border.[438] In contrast, a different court found in *United States v. Esparza-Mendoza*, that an illegal alien, who had previously lived in the United States (indeed, had been convicted of a drug offense and subsequently deported), who returned without the appropriate paperwork and again resided within the country before his arrest in Utah, had not established a sufficient connection to benefit from the Fourth Amendment.[439]

---

434. *Id. See also* Orin Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. (forthcoming 2015).

435. *See, e.g.*, United States v. Stokes, 710 F.Supp. 2d 689, 698–700 (N.D. Ill. 2009), aff'd 726 F.3d 880 (7th Cir. 2013); United States v. Esparza-Mendoza, 265 F.Supp. 2d 1254, 1260–61 (N.D. Utah 2003), aff'd 386 F.3d 953 (10th Cir. 2004); United States v. Guitterez, 983 F.Supp. 905, 912 (N.D. Cal. 1998), rev'd on other grounds, 203 F.3d 833 (9th Cir. 1999) (unpublished).

436. *See* Kerr, *supra* note 434.

437. 459 F.3d 618, 620–21 (5th Cir. 2006).

438. *Id.* at 625.

439. 265 F. Supp. 2d 1254, 1273–74 (N.D. Utah 2003).

The conclusion that a foreign national who lives outside the United States, and who *enters* the country without a valid visa, is protected by the Fourth Amendment, appears to be in tension with the proposition that a foreign national, who lives in the United States, and re-enters without the appropriate paperwork, does not have a sufficient connection to the country to be considered within the protections of the Fourth Amendment.[440] In both cases, the aliens' connections with the United States are voluntary. In the second case, the unlawfulness of the connection creates a carve-out for membership in the political community. The object of the unlawfulness, in other words, is citizenship or legal residency. Had the unlawfulness been merely criminal acts unrelated to residency requirements, the individual may well have been a U.S. person for purposes of Chief Justice Rehnquist's analysis. Yet, under Justice Kennedy's reasoning, it is not clear that the same outcome would hold. The search in question in the second case occurred on U.S. soil, where none of the practical obstacles cited by Kennedy in his concurrence would have come into play. Nor did the actions taken by the individual interfere with the United States' authority as a sovereign nation in its conduct of foreign affairs. If that is the rationale for determining whether an individual bears a substantial connection, then geographic location may prove the most critical question.

The lack of clarity at the margins has implications for targets of surveillance under Section 702. To the extent that the connections to the United States are lawful in regard to citizenship or residency (in other words, the target is either lawfully present at the time of the search or, if located overseas, has a substantial connection like citizenship or lawful residency), then, under Rehnquist's analysis, the target is considered one of "the people," as protected by the Fourth Amendment. Congress has already cemented these understandings into law: traditional FISA deals with domestic surveillance of not just U.S. persons but foreign powers or agents of foreign powers, even as Sections 703 and 704 addresses U.S. persons overseas.[441]

---

440. This distinction narrows if one adds the legality of residence to considerations of a sufficient nexus; but the Supreme Court did not include this condition in *Verdugo-Urquidez*.

441. Recognition of the continued existence of U.S. persons' rights when they are located overseas is not unique to the Fourth Amendment context. In a case

A gap in constitutional jurisprudence, and in understanding the application of Section 702, lies with a third class of individuals who may have a substantial connection to the country outside of outright citizenship or residency. How are they to be treated for purposes of the Fourth Amendment? An individual, for instance, with substantial professional, educational, or commercial connections may have a strong relationship with the United States. Their actions may be critical to the country's economic growth or strength. Are they to be considered protected by the Fourth Amendment?

Under Rehnquist's account, the answer appears to be no. They are not part of the political community. Professor Orin Kerr has proposed that we read *Verdugo-Urquidez* to include only sufficient physical and legal contact with the country—and not to extend to online or Internet-based contacts.[442] For him, online contacts with U.S. servers amount merely to a "'fortuitous' circumstance of where the Internet provider happens to locate the servers."[443] Customers may be located anywhere in the world. As Rehnquist reasoned in *Verdugo-Urquidez*, "the purpose of the Fourth Amendment was to protect the people of the United States against arbitrary action by their own government."[444] It was not meant to prevent the federal government from acting against aliens outside the United States.[445] The community forming "the people" is not comprised of accidental members of the polis. They rely on the Constitution to protect them from the state.[446]

This reading of "the people" appears to be right. But unlike Kerr, insofar as one considers Fourth Amendment protections as a threshold matter, I consider the legal relationship paramount and would limit it to a legal formalism establishing the relationship between the individual and the political community. That is, an individual constituting "the people" may or may not be present

---

involving the fifth and sixth amendments, for instance, the Court similarly noted that the "shield" provided to U.S. citizens by the Bill of Rights "should not be stripped away just because he [or she] happens to be in another land." Reid v. Covert, 354 U.S. 1, 5–6 (1957).

442. Kerr, *supra* note 434.

443. *Id.* at 21.

444. United States v. Verdugo-Urquidez, 494 U.S. at 266.

445. *Id*. at 266-27. *See also* Kerr, *supra* note 434.

446. *See also* Kerr, *supra* note 434.

within the country; but it is the legal framing, stemming from the constitutional tenant of the organization of the political entity, that creates the right.

The difficulty, for Section 702 purposes, enters in regard to Kennedy's reliance on the rule that he saw as most consistent with the United States' role as a sovereign nation.[447] "[W]e must interpret constitutional protections," he wrote, "in light of the undoubted power of the United States to take actions to assert its legitimate power and authority abroad."[448] What is the scope of the United States' legitimate power and authority abroad? To what degree is it rooted in the legal status of the individual against whom the state is acting? And what is the relationship between different forms of legal relationships and membership in the political community?

Let us focus here on the types of relationships most at issue with regard to Section 702: global electronic communications. One danger in according non-U.S. persons Fourth Amendment rights via (substantial) virtual contact with the United States is that individuals could use such contacts to evade detection.[449] Foreign persons could become members of Amazon Prime, communicate with associates in the United States via Verizon, and take Massive Open Online Courses (MOOCs) from the latest American university to offer them, perhaps even in the process obtaining a U.S. college or graduate degree. This could then become a shield to mask behavior that may undermine U.S. national security.

One response to this might be that in a global communications environment, privacy protections must be thought about in a broader sense. It matters little whether a customer is French, English, or American. Privacy rights should be extended to customers by nature of their dual status with U.S. persons *qua* customers—or even as a concomitant of their rights as people. This was the thrust of part of Privacy and Civil Liberties Oversight Board's (PCLOB) analysis that suggested privacy be regarded as a human right.

There is a *realpolitic* argument to be made here as well, which ties more directly to U.S. foreign interests. Namely, U.S. failure to

---

447. United States v. Verdugo-Urquidez, 494 U.S. at 276 (Kennedy, J., concurring).
448. *Id*. at 277.
449. *See* Kerr, *supra* note 434.

ensure privacy protections may lead to a loss in U.S. competitiveness. And economic concerns are central to U.S. national security. Consider the impact of the public release of information about NSA Section 702 surveillance on the U.S. cloud computing industry. There was an immediate, detrimental impact on the strength of the U.S. economy. Billions of dollars are now on the line because of concerns that the services provided by U.S. information technology companies are neither secure nor private.[450] 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.[451] Other commentators, such as Forrester Research analyst James Staten, have put actual losses as high as $180 billion by 2016, unless something is done to restore overseas' confidence in data held by U.S. companies.[452]

Failure to extend privacy protections to individuals with substantial connections to the country via industry would, in this view, make it harder, not easier for the United States to assert its legitimate power and authority abroad. So, under Kennedy's reasoning, one could argue that Fourth Amendment rights should be extended to individuals economically tied to U.S. entities. This determination, however, is ultimately one of policy—not law. Deciding whether a greater national security threat is entailed in loss of competitiveness of U.S. industry, versus loss of protections extended to non-U.S. persons in the interests of privacy, is part of the weighing that must be done by the executive branch in pursuing its interests abroad. In this way, the Rehnquist opinion and

---

450. IT industries set to lose billions because of privacy concerns, UPI (Dec. 17, 2013), http://www.upi.com/Business_News/Security-Industry/2013/12/17/IT-industries-set-to-lose-billions-because-of-privacy-concerns/UPI-30251387333206/ [http://perma.cc/Q7SC-DELW] ("Information technology companies stand to lose billions of dollars of business because of concerns their services are neither secure nor private[.]").

451. *Id. See also* Mary DeRosa, *U.S. Cloud Services Companies Are Paying Dearly for NSA Leaks,* NEXTGOV (Mar. 24, 2014), http://www.nextgov.com/technology-news/tech-insider/2014/03/us-cloud-services-companies-are-paying-dearly-nsa-leaks/81100/ [http://perma.cc/C2ZV-LEM8] (reporting estimates of losses of $22 billion over the next three years).

452. *IT industries set to lose billions because of privacy concerns*, UPI (Dec. 17, 2013), http://www.upi.com/Business_News/Security-Industry/2013/12/17/IT-industries-set-to-lose-billions-because-of-privacy-concerns/UPI-30251387333206/ [http://perma.cc/Q7SC-DELW].

the Kennedy concurrence can be read as compatible with not extending Fourth Amendment rights to individuals lacking a legal relationship (in other words, those stemming directly from the individual's status as a member of the political community).[453]

This appears to have been the crux of President Obama's effort to reassure the international community in January 2014 that the United States would not use its authority to collect trade secrets to advantage U.S. corporations.[454] In Presidential Policy Directive 28, Obama acknowledged the privacy interests held by foreign persons:

> All persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information. U.S. signals intelligence activities must, therefore, include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where that individual resides.[455]

The extent to which U.S. SIGINT follows this prescription boils down to policy, not law. As a constitutional matter, the collection of information of non-U.S. persons overseas does not need to comport with the Fourth Amendment.

A more serious challenge presents itself in relation to communications between members of the political community and individuals who are not otherwise protected by the Fourth Amendment. This is at the heart of Congress's concern about reverse targeting—namely, that the intelligence community would use Section 702 to target non-U.S. persons overseas, as a back door to gaining access to U.S. persons' communications.

To the extent that the interception of U.S. persons' communications constitutes a search or seizure within the meaning of the Fourth Amendment, it would appear that, at least at the front-

---

453. *See also* Kerr, *supra* note 434.

454. *See, e.g.*, Office of the Press Sec'y, *Presidential Policy Directive—Signals Intelligence Activities*, THE WHITE HOUSE § 1(c) (Jan. 17, 2014), http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [http://perma.cc/Y95E-PR7V] (stating that the collection of foreign commercial information is authorized "only to protect the national security of the United States or its partners and allies.")

455. *Id.* § 4.

end, U.S. persons are entitled to protections.[456] The inspection and collection of content falls within the meaning of a search and seizure under the Fourth Amendment.

Just as virtual entry into the United States should not matter for purposes of setting a threshold for application of the Fourth Amendment to aliens, use of global communications should not thereby divest U.S. persons of their constitutional protections. This approach is consistent with the geographic focus of the Courts in regard to the Fourth Amendment. It does not hinge constitutional protections on movement along global communications networks—itself an untenable proposition in light of how information flows over the Internet.

If the courts, for instance, were to construct a rule that said that U.S. persons sending information outside the United States lose the protections of the Fourth Amendment in the privacy afforded those communications, it would be difficult to police. This rule assumes that individuals have control over whether their communications leave domestic bounds. They do not. The Internet is constructed to find the most efficient route between two ISP addresses. This means that even domestic communications may be routed internationally. Individuals have no control over how their messages are conveyed. At the back end, the government would have to be able to ascertain which messages originated within the United States and then left U.S. bounds. But the NSA claims that it does not have the appropriate technologies to make this call.

As a result, the effect of this rule would essentially be to assume that every time a U.S. person communicates, she loses constitutional protections in the content of those communications. This would eviscerate the meaning of the Fourth Amendment. It would assume that U.S. persons have no reasonable expectation of privacy in their communications, regardless of whether they flow across international borders.

The Supreme Court can avoid this conclusion by underscoring the status of the individual as Rehnquist articulated for the majority in *Verdugo-Urquidez*: emphasizing membership in the political community. Where established, the protection of the Fourth Amendment applies.

---

456. For discussion of the question of search and seizure in light of *Verdugo-Urquidez*, *see* Kerr, *supra* note 434.

### *2. Limits of the Warrant Clause Abroad*

Even if the Fourth Amendment applies to U.S. persons located outside the United States, it does not necessarily follow that the Warrant Clause must be satisfied. As a matter of practice, for centuries, the executive engaged in the warrantless surveillance of U.S. persons abroad.[457] Similarly, between the enactment of traditional FISA and the introduction of the FAA, the surveillance of U.S. persons and non-U.S. persons based overseas, for foreign intelligence purposes, took place outside statutory contours. Non-U.S. persons fell largely within the President's Article II authorities, even as Executive Order 12,333 provided for the same for U.S. persons.

Accordingly, prior to the FAA, lower courts found the absence of a prior warrant for intercepts conducted abroad for criminal investigations to be consistent with the Fourth Amendment.[458] There were no statutes on point. Title III has no extraterritorial force.[459] The Federal Rules of Criminal Procedure (FRCP), in turn, limit the jurisdiction of federal magistrates.[460] Although the Supreme Court has considered a proposed amendment that would provide a way to issue "warrants to search property outside the United States," the Advisory Committee to the 1990 Amendments to the FRCP noted that, "it was unclear how federal officers might obtain warrants authorizing searches outside the district of the issuing magistrate."[461] In the absence of statutory guidance, courts relied upon a constitutional analysis.

In *United States v. Barona*,[462] the Ninth Circuit recognized that U.S. persons overseas are covered by the Fourth Amendment—but only insofar as the search in question meets the standard for reasonableness. The Warrant Clause did not apply.[463] *Barona*

---

457. William F. Brown & Americo R. Cinquegrana, *Warrantless Physical Searches for Foreign Intelligence Purposes: Executive Order 12,333 and the Fourth Amendment*, 35 CATH. U. L. REV. 97, 103 (1985) ("Warrantless electronic surveillance has been used by the Executive to collect intelligence information since at least the mid-1800s.").

458. *See, e.g.*, United States v. Peterson, 812 F.2d 486, 492 (9th Cir. 1987).

459. *See* 18 U.S.C. § 2518(3) (2012). *See also Peterson*, 812 F.2d at 492;.Stowe v. Devoy, 588 F.2d 336, 341 n.12 (2d Cir. 1978); United States v. Cotroni, 527 F.2d 708, 711 (2d Cir. 1975), *cert. denied*, 426 U.S. 906 (1976).

460. FED. R. CRIM. P. 41(b) (governing domestic law enforcement investigations).

461. *Id.* 41(a) (1990 Advisory Committee Note). *See also Peterson*, 812 F.2d at 492.

462. 56 F.3d 1087 (9th Cir. 1995).

463. *Id.* at 1096.

stemmed from a Drug Enforcement Agency operation ("Operation Pisces") conducted at the height of the war on drugs, 1985–1987.[464] Wiretaps led to the eventual conviction of individuals for involvement in the worldwide distribution of cocaine.

In *United States v. LaChapelle*,[465] the court noted that neither the Fourth Amendment "'nor the judicially created exclusionary rule applies to acts of foreign officials'."[466] Only two "very limited exceptions"[467] might apply: first, where "the circumstances of the foreign search and seizure are so extreme that they 'shock the [judicial] conscience,'"[468] (a consideration stemming from the judiciary's supervisory powers, employed to ensure "the integrity of the criminal justice system"[469]); and, second, where U.S. agents' participation was "so substantial that the action is a joint venture between United States and foreign officials."[470] In *Barona*, electronic intercepts had been issued consistent with Danish Court procedures, making the operation a joint venture. The court thus relied upon Denmark's legal framework to determine whether the search was reasonable, and whether U.S. officials relied in good faith upon Danish representations that the actions taken complied with foreign law.[471]

*Barona* dealt explicitly with criminal matters. In the foreign intelligence context, in 2000 one lower court similarly established the applicability of the Fourth Amendment reasonableness standard for surveillance of U.S. persons overseas, even as it eschewed applicability of the warrant requirement.[472] Like *Barona*, the decision pre-dated the FAA. In *United States v. Bin Laden*, the Southern District of New York (S.D.N.Y.) denied a U.S. citizen's motion to suppress evidence obtained from a warrantless wiretap placed on his landline in Nairobi, as well as on his mobile telephone.[473] The

---

464. *Id.* at 1089–90.

465. 869 F.2d 488 (9th Cir. 1989).

466. *Id.* at 489 (quoting United States v. Maher, 645 F.2d 780, 782 (9th Cir. 1981)).

467. *Id.*

468. *Id.* at 490 (quoting United States v. Rose, 570 F.2d 1358, 1362. (9th Cir. 1978)).

469. United States v. Barona, 56 F.3d 1087, 1091 (9th Cir. 1995).

470. *LaChapelle*, 869 F.2d at 490.

471. Barona, 56 F.3d at 1094.

472. United States v. Bin Laden, 126 F. Supp. 2d 264 (S.D.N.Y. 2000).

473. *Id.* The intercepts had been approved by the Attorney General in 1997. *Id.*

court considered the costs of imposing a warrant requirement on surveillance conducted overseas.[474] The court reasoned by analogy that a similar "special needs" exception existed with regard to foreign intelligence collection overseas.[475] The court noted the argument that "the judicial branch is ill-suited to the task of overseeing foreign intelligence collection," supporting this sentiment by referencing the "several persuasive points" made by the Government "about the intricacies of foreign intelligence collection conducted abroad," such as the difficulties of predicting the international consequences of decisions; the problem of foreign intelligence services and officials being seen as complicit with U.S. actions; and the danger of notifying enemies by alerting government officials sympathetic to their cause of U.S. surveillance actions underway.[476] The court further recognized the potential for breaches of security in requiring a warrant prior to foreign intelligence collection overseas.[477]

Even as it took the above considerations into account, S.D.N.Y. separately placed significant weight on the *absence of any statutory guidance* on whether the executive was required to obtain a warrant prior to the extra-territorial interception of U.S. persons'

---

474. Similar considerations mark the discussion of exceptions to the warrant requirement within the United States. *See, e.g.,* Veronia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995) (upholding high school athlete drug testing and explaining the special needs doctrine); Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 620 (1989) ("The Government's interest in regulating the conduct of railroad employees to ensure safety . . . presents 'special needs' beyond normal law enforcement that may justify departures from the usual warrant and probable-cause requirements."); Griffin v. Wisconsin, 483 U.S. 868, 876 (1987) (holding that a warrant requirement would interfere with the supervision of individuals on probation and impede the responsiveness of probation officers); Terry v. Ohio, 392 U.S. 1 (1968) (upholding patdowns for weapons to protect officer safety); Camara v. Municipal Court, 387 U.S. 523, 533 (1967) (imposition of warrant requirement "depends in part upon whether the burden of obtaining a warrant is likely to frustrate the governmental purpose behind the search.").

475. *Bin Laden*, 126 F. Supp. 2d at 274 ("[I]t is clear that imposition of a warrant requirement in the context of foreign intelligence searches conducted abroad would be a significant and undue burden on the Executive.") For discussion of the "special needs" exception in defense of warrantless wiretapping outside of FISA, *see* Letter from Assistant Attorney General William Moschella, to Hon. Pat Roberts, Chairman, Senate Select Committee on Intelligence and others 4 (Dec. 22, 2005), *available at* http://www.justice.gov/ag/readingroom/surveillance6.pdf [http://perma.cc/HGJ5-K9QW].

476. *Bin Laden*, 126 F. Supp. 2d at 274–75.

477. *Id.* at 275.

communications.[478] Just as in *Truong* and *Butenko*, absent limits established by Congress, the Executive had greater leeway to decide whether and to what extent it engaged in overseas foreign intelligence gathering.[479]

The court was uncomfortable creating a warrant requirement for foreign intelligence collection where the political branches—and particularly the legislature—had failed to do so. Instead, it deferred to the executive and legislative branches as exercising broad authority in the field of foreign affairs. Outside of the contours of reasonableness, the shape of foreign intelligence, as a concomitant of the field of foreign relations, was to be determined by the other branches working in tandem.

Like *Truong*, *Bin Laden* related to electronic surveillance authorized by the President (and the Attorney General acting at the President's behest) for foreign intelligence purposes, in investigations targeting foreign powers and their agents. The court was careful to note that the point at which the investigation turned into criminal prosecution provided a hard line: "This exception to the warrant requirement applies until and unless the primary purpose of the searches stops being foreign intelligence collection."[480]

In 2008 the Foreign Intelligence Surveillance Court of Review found a similar foreign intelligence exception to the warrant requirement for the interception of communications outside the

---

478. *Id.* ("The final consideration which persuades the Court of the need for an exception to the warrant requirement for foreign intelligence collection conducted overseas is that there is presently no statutory basis for the issuance of a warrant to conduct searches abroad.").

479. *See, e.g.*, United States v. Truong, 629 F.2d 908, 923 (4th Cir. 1980); United States v. Butenko, 494 F.2d 593, 601. (3d Cir. 1974). Judge Leonard Sand explained, "[T]he Court finds that the power of the Executive to conduct foreign intelligence collection would be significantly frustrated by the imposition of a warrant requirement in this context. Therefore, this Court adopts the foreign intelligence exception to the warrant requirement for searches targeting foreign powers (or their agents) which are conducted abroad. As has been outlined, no court, prior to FISA, that was faced with the choice, imposed a warrant requirement for foreign intelligence searches undertaken *within* the United States. With those precedents as guidance, it certainly does not appear to be unreasonable for this Court to refuse to apply a warrant requirement for foreign intelligence searches conducted *abroad*." *Bin Laden*, 126 F. Supp. 2d at 277 (emphasis in original).

480. *Id.* at 278.

United States.[481] The case centered on provisions of the Protect America Act of 2007, which pre-dated the FAA, but which contained measures similar to those now found in the law. The Attorney General and DNI could authorize electronic intercepts between the U.S. and overseas where the target of the surveillance was believed to be located abroad and a "significant purpose" of the surveillance was the collection of foreign intelligence.[482] In one of the few challenges in FISC to Section 702 or its antecedents, a telecommunications provider challenged the PAA on Fourth Amendment grounds.

Although the company claimed a facial challenge to the PAA, the court accepted the government's argument that the constitutional questions being raised related to the statute as applied.[483] The court's decision thus did not reach the validity of the law in different settings.

FISCR noted that *In re Sealed Case* did not hold that a foreign intelligence exception to the warrant requirement exists; instead, it assumed, *arguendo*, that regardless of whether or not the requirements were met, traditional FISA could survive on reasonableness grounds.[484] For *In re Directives*, FISCR thus considered *de novo*, whether, by analogy to the special needs doctrine, a similar foreign intelligence exception to the warrant requirement exists.[485]

The court underscored the exceptional nature of the subject matter over which it had jurisdiction:

> For one thing, the purpose behind the surveillances ordered pursuant to the directives goes well beyond any garden-variety law enforcement objective. It involves the acquisition from overseas foreign agents of foreign intelligence to help protect national security.[486]

---

481. *In re* Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, (FISA Ct. Rev. Aug. 22, 2008), *available at* http://www.fas.org/irp/agency/doj/fisa/fiscr082208.pdf [http://perma.cc/9DKP-M3XN].

482. *Compare* Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (2007) (repealed July 10, 2008) *with* FISA Amendments Act of 2008, Pub. L. No. 110-261, § 403, 122 Stat. 2436, 2473 (2008).

483. The statute had been "applied to the petitioner in a specific setting." *In re* Directives at 12 (FISA Ct. Rev. Aug. 22, 2008) (Selva, C.J.).

484. *Id.* at 13.

485. *Id.* at 14–15.

486. *Id.* at 15.

Even as it recognized that "the government's interest is particularly intense," citing *In re Sealed Case*, the court rejected the argument that foreign intelligence must be the primary purpose of the surveillance:

> [I]n our view the more appropriate consideration is the programmatic purpose of the surveillances and whether—as in the special needs cases—that programmatic purpose involves some legitimate objective beyond ordinary crime control . . . . Under this analysis, the surveillances authorized by the directives easily pass muster. Their stated purpose centers on garnering foreign intelligence.[487]

Because the executive branch stated that the programs in place were to protect national security, and there was "no indication" that the collection of information was primarily related to ordinary criminal law enforcement, the court would presume a legitimate exercise of authority. FISCR added, consistent with *Truong*, that "requiring a warrant would hinder the government's ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake."[488]

*In re Directives*, like *Bin Laden*, was decided prior to the FAA and Congress's introduction of Sections 703 and 704.[489] It is difficult to say how the Court would now come down on the statutory analysis and the question of foreign powers allocation between the executive and legislative branches. Nowhere in the six pages devoted to the Warrant Clause consideration does the court address *Youngstown*, the failure of the courts to recognize any domestic foreign intelligence exception post-FISA, or the absence of more particularized statutory requirements. Nor does the court consider *Verdugo-Urquidez* and the application of the Fourth Amendment overseas based on whether the target is a U.S. person or a non-U.S. person. Perhaps most importantly, the court did not address incidental collection.

---

487. *Id.* at 16.

488. *Id.* at 17.

489. *But note* that the case dealt with the PAA, which in a number of respects, was less protective of the rights of U.S. persons.

### *C. Foreign Intelligence, Criminal Prosecution*

If one accepts that the contours of the warrant requirement in foreign intelligence gathering are subject to countervailing pressure from separation of powers doctrine, it does not necessarily follow that the use of the same information for criminal law purposes, without insertion of a warrant procedure at any point, is constitutionally sufficient. Courts have repeatedly emphasized the importance of drawing a line between the two spheres. FISCR pushed the line furthest, saying that even where the primary purpose was criminal in nature, the information could be obtained as long as there was a foreign intelligence aspect.

Whatever one may say about the constitutionality of different aspects of the program underway,[490] there is at least one point where the current practice of the Administration runs well over acceptable limits: query of Section 702 data using U.S. persons' information for purposes of criminal prosecution.

As mentioned, the FBI comingles traditional FISA and Section 702 data and routinely queries it, using U.S. person identifiers, as part of criminal investigations. Yet none of the justifications offered for exempting collection from the warrant requirement apply when ordinary criminal investigations are on the line. FISCR embraced three reasons to carve out a foreign intelligence exception: when (a) the purpose of surveillance went beyond "garden-variety" law enforcement; (b) the government's interest was "particularly intense"; and (c) there was a "high degree of probability that requiring a warrant would hinder the government's ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake."[491] None of these

490. A good argument could be marshaled, for instance, that while to/from collection fits within a foreign intelligence exception to the warrant requirement, "about" monitoring and collection and the volume of incidental intercepts fall outside acceptable standards. In ordinary criminal law, there are various ways in which one's rights are dependent upon the rights of the individual with whom one is communicating. Conversations with informants, for example, are not protected. But by making use of "about" collection, a U.S. person may merely mention a selector/target, visit a server associated with the target, or join a chat room where the target might have been present. Allowing widespread monitoring and interception is akin to saying that law enforcement could open all international mail and scan it to find reference to a known mafia boss, without a warrant.

491. *In re* Directives, 551 F.3d at 1011–12.

rationales are present in the subsequent query of databases constructed of Section 702 data.

Nor are the practical concerns that limit the warrant clause's applicability in overseas foreign intelligence collection present. In *Bin Laden*, S.D.N.Y. highlighted the intricacies of foreign intelligence acquisition, the difficulty of predicting the international impact of seeking a warrant, the problem of foreign intelligence officials being seen as complicit, and the danger of notifying enemies by alerting foreign officials to U.S. actions.[492] But in the query of data already in U.S. government hands, none of the foreign affairs consequences the court contemplated still hold.

It does not necessarily follow that, just because the information has been lawfully obtained, the government has the authority to search the data. Two contexts are relevant to Section 702 analysis: (a) situations in which information has been lawfully seized, but where limits may apply on searches, and (b) situations in which information may be fed into a database and retained, with subsequent use of the database limited in some way. Nearly two decades ago, scholars argued that a use restriction could be found in the Fourth Amendment. Critiques of this position fail to take account of the Court's more recent jurisprudence, which recognizes a privacy interest in digital information and creates the potential for constitutional restrictions on use.

### *1. Lawful Seizure and Subsequent Search of Data*

The Fourth Amendment allows for line drawing between obtaining and searching information and further query of the data. One of the most recent cases illustrating this point is *United States* v. *Ganias*, a Second Circuit case involving search of information copied from a hard drive, two years after it was obtained, for purposes other than that for which it was initially seized.[493] The court held unconstitutional the retention and further search of the data, despite the fact that law enforcement had returned to a judge to obtain a warrant for the later search.[494] In *Riley* v. *California*, the Supreme Court addressed a similar situation in the context of a search incident to arrest,

492. United States v. Bin Laden, 126 F. Supp. 2d 264 (S.D.N.Y. 2000).
493. United States v. Ganias, 755 F.3d 125 (2d. Cir. 2014).
494. *Id.*

finding that even where a cell phone has been legally seized, subsequent query of the device requires judicial intervention.[495] While other cases further support the point, brief discussion of *Ganias* and *Riley* helps to illustrate the Fourth Amendment principle as relevant to the digital realm.[496]

In the first case, an accountant, Steve Ganias, provided services to a company that the Army hired to maintain a vacant Army facility in Stratford, Connecticut.[497] A confidential informant advised the Army that evidence of illegal activity was located on Ganias' hard drive. Investigators obtained a warrant to search and seize "[a]ll books, records, documents, materials, computer hardware and software and computer associated data relating to the business" in question.[498] Although Ganias was not a suspect, Army computer specialists copied all of the information located on his hard drives.[499] Just over a year later, the Army and the IRS isolated the relevant files but decided to retain the (irrelevant) information as well. The government argued that the data had become their property. As the government expanded its investigation, it began to consider the possibility that Ganias was also involved in illegal activity. Three years after having copied the hard drive, the IRS, suspecting Ganias of lying on his taxes, obtained another warrant to search the data. Convicted of tax evasion, Ganias unsuccessfully moved to suppress this evidence.[500]

---

495. Riley v. California, 134 S. Ct. 2473 (2014).

496. *See, e.g.*, United States v. Sedaghaty, 728 F.3d 885, 910–13 (9th Cir. 2013) (rejecting expansion of a warrant's limited scope to include further search of items seized); United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013) (en banc) (noting that even though the Government may have the authority to seize and search a computer at the border, further search of the computer must also comport with Fourth Amendment requirements); United States v. Young, 573 F.3d 711, 720–21 (9th Cir. 2009) (warrant required for further search of backpack in the possession of law enforcement); United States v. Mulder, 808 F.2d 1346, 1348 (9th Cir. 1987) (limiting testing of pills lawfully in government possession to field testing for illegal drugs under a limited warrant exception, but requiring a warrant for further laboratory testing to determine their precise molecular structure).

497. *Ganias*, 755 F.3d at 128.

498. Warrant application, U.S. District Court for the District of Connecticut, Nov. 17, 2003.

499. *Ganias*, 755 F.3d at 135.

500. United States v. Ganias, No. 3:08 Cr. 224, 2011 WL 2532396 (D.Conn. June 24, 2011).

On appeal, the Second Circuit vacated Ganias's conviction on Fourth Amendment grounds. The Court noted that "[l]ike 18th Century 'papers,' computer files may contain intimate details regarding an individual's thoughts, beliefs, and lifestyle, and they should be similarly guarded against unwarranted Government intrusion."[501] Off-site review, while necessary, must still be subject to the rule of reasonableness. But the same reasons that make off-site review necessary (for example, storage capacity of media, difficulties created by encryption, and computer lab workload), do not "provide an 'independent basis' for retaining any electronic data" beyond that specified in the initial warrant.[502]

In June 2014, the Supreme Court issued an opinion in another case that similarly supports a Fourth Amendment use restriction on lawfully obtained information. In *Riley v. California*,[503] the Court held that law enforcement may not, without a warrant, search information on a cell phone that had been seized from an individual at the time of arrest. Police officers, scrolling through the suspect's address book, had found letters indicating gang membership next to a number of names. Further examination of the mobile device revealed photographs and videos tying the suspect to gang activity. The government subsequently introduced this information as evidence in connection with a shooting.

In a unanimous decision, the Supreme Court held that the search of digital data in the course of arrest fell outside the warrant exception.[504] While the police could seize the telephone, they could not simply scroll through the information without first obtaining a warrant.[505]

While the case derives from criminal law and not foreign intelligence law, it is significant for analysis of Section 702 because it

---

501. *Ganias*, 755 F.3d at 21.

502. *Id.* at 25 (citing United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1171 (9th Cir. 2010) (en banc)).

503. *See* Riley v. California, 134 S. Ct. 2473 (2014).

504. *Id.*

505. The Court was careful to note that exceptions to this might exist under the exigent circumstances exception, such as when a suspect may be in the midst of "texting an accomplice who, it is feared, is preparing to detonate a bomb . . . " *Id.* at 27. In such cases, a warrantless search of cell phone data may be justified. "The critical point is that, unlike the search incident to arrest exception, the exigent circumstances exception requires a court to examine whether an emergency justified a warrantless search in each particular case." *Id.*

recognized a privacy interest in the digital data (a privacy interest protected by the Fourth Amendment), and a distinction between search of such information and the seizure of the data in the first place. A critical question, of course, is whether the activity in question, undertaken consistent with Section 702, amounts to a search in the first place. In *Riley*, the Court reserved whether "the collection or inspection of aggregated digital information amounts to a search under other circumstances."[506] Setting aside for the moment arguments about whether the collection of certain types of information qualifies as a search, it is difficult to deny that the query of a database comprised of non-publicly-available information (obtained without the targets' consent), to try to find evidence of criminal activity, constitutes a search in the most basic sense of the term. Even though the government might have legally obtained the information at the front end, it could not search the information for evidence of criminal activity absent a warrant, supported by probable cause.

### *2. Database Construction*

There are a number of cases related to identification of individuals arrested for felonies, in which Fourth Amendment challenges to the search and seizure, and retention of information in databases that can subsequently be searched without a warrant, have failed.[507] In *Maryland* v. *King*, for instance, the Supreme Court ascertained that when law enforcement performs a felony arrest, supported by probable cause, obtaining DNA material is reasonable for Fourth Amendment purposes.[508] For the Court, detainees have "a reduced expectation of privacy."[509]

---

506. *Riley*, 134 S. Ct. at 2489 n. 1.

507. *See, e.g.*, United States v. Kimler, 355 F.3d 1132 (10th Cir. 2003); United States v. Kincade, 345 F.3d 1095 (9th Cir. 2003), *rev'd en banc*, 379 F.3d 813 (9th Cir. 2004); Roe v. Marcotte, 193 F.3d 72 (2d Cir. 1999); Doe v. Moore, 410 F.3d 1337 (11th Cir. 2005); Johnson v. Ogershok, 134 Fed. App'x 535 (3d Cir. 2005); United States v. Kraklio, 451 F.3d 922 (8th Cir. 2006); United States v. Conley, 453 F.3d 674 (6th Cir. 2006); United States v. Lujan, 504 F.3d 1003 (9th Cir. 2007). *See also* United States v. Diaz-Casteneda, 494 F.3d 1146, 1151–53 (9th Cir. 2007) (allowing for query of license plate databases on grounds that the information is already publicly available)—a case distinguishable from the interception of the content of communications where the courts have recognized a reasonable expectation of privacy.

508. Maryland v. King, 133 S. Ct. 1958 (2013).

509. *Id.* at 1978.

There are two problems with drawing parallels between the DNA database cases and NSA use of Section 702 to cache and subsequently search communications.

First, it is to the individual whose information is being collected—not to the purpose of the collection—that the Court gives priority. Suspects in felony cases and convicted criminals obtain a lower level of protection than others. This is the same rationale under which, in part, the Court found the exception for search incident to arrest to be acceptable: it is not just the context of a volatile arrest, but also "an arrestee's reduced privacy interests upon being taken into police custody."[510] The Supreme Court has repeatedly embraced Judge Cardozo's account of the historical underpinnings for the exception: "Search of the person becomes lawful when grounds for arrest and accusation have been discovered, and the law is in the act of subjecting the body of the accused to its physical dominion."[511]

Allowing for a similar search of U.S. persons' international communications treats them as though they have a reduced expectation of privacy, despite the fact that they have not been suspected of any wrongdoing. All individuals' communications may be monitored and intercepted, not just those with a lowered expectation of privacy related to suspicion of criminal activity.

Second, the use to which the information is being put matters. In the context of DNA collection, further search of the data can only be done to identify an individual, not to mine the information for further knowledge (for example, to determine relatives, look for genetic predispositions, etc.).

In *King*, the Court distinguished the DNA database search from "programmatic searches of either the public at large or a particular class of regulated but otherwise law-abiding citizens," which fell within the "special needs" category.[512] Such special needs searches relate to police stopping a motorist at a checkpoint,[513] or testing a political candidate for drug use.[514] In each case, the Court insists on something more than merely detecting evidence of or-

510. Riley v. California, 134 S. Ct. 2473, 2488 (2014) (Alito, J., concurring).

511. 414 U.S. at 232 (quoting People v. Chiagles, 237 N.Y. 193, 197, 142 N.E. 583, 584 (1923)).

512. *Id.*; *see, e.g.*, Chandler v. Miller, 520 U.S. 305, 314 (1997).

513. *See, e.g.*, Indianapolis v. Edmond, 531 U.S. 32 (2000).

514. *See Chandler*, 520 U.S. at 308.

dinary criminal wrongdoing to justify such searches in the absence of individualized suspicion.[515] In none of these cases is the information then fed into a giant database for future use.

### *3. Use of Data as Fourth Amendment Consideration*

Nearly twenty years ago, Professor Harold Krent proposed a use restriction for Fourth Amendment doctrine.[516] His thesis was that the reasonableness of the seizure extends beyond the immediate acquisition of the information to the use subsequently made of the data so obtained.[517] He argued that control over private information did not cease upon others' access to the data.[518] Reasonableness is not to be determined merely at one point in time, but at any time law enforcement authorities seek to make use of the property and information thus obtained. Use restrictions naturally follow.

Professor Orin Kerr questioned the practicality of Krent's argument under Supreme Court jurisprudence.[519] Specifically, he suggested that because third-party record collection constitutes neither a search nor a seizure, the doctrine would have to be radically overhauled to make all collection of data a seizure to then trigger a reasonableness analysis.[520]

Kerr's analysis predated the Court's recent movement with regard to third party data. In *United States* v. *Jones*, a shadow majority on the Court recognized a privacy interest in bulk collection and programmatic surveillance, despite the information being obtained from third parties.[521] Justice Sotomayor explained in her concurrence:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in infor-

---

515. Indianapolis v. Edmond, 531 U.S. 32, 38 (2000).

516. Harold J. Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEX. L. REV. 49 (1995).

517. *Id.* at 51.

518. *Id.* at 51–52.

519. Orin S. Kerr, *Use Restrictions and the Future of Surveillance Law, The Future of the Constitution*, BROOKINGS, 1, 9 (Apr. 19, 2011), *available at* http://www.brookings.edu/~/media/research/files/papers/2011/4/19%20surveillance%20laws%20kerr/0419_surveillance_law_kerr.pdf [http://perma.cc/E9HN-X2RS].

520. *Id.* at 10.

521. United States v. Jones, 615 F.3d 544 (2012). For detailed discussion of *United States v. Jones* in this context, *see* Donohue, *supra* note 33.

> mation 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. . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[522]

Sotomayor's words suggest that a use restriction may be relevant to Fourth Amendment analysis. A "limited purpose" for obtaining the information may cabin the use to which the data may then be put.

Justice Sotomayor's reasoning challenges the third party Athena that sprung from the Supreme Court in the 1970s. In *United States* v. *Miller*, the government subpoenaed bank records to convict Mitch Miller of running an illegal whiskey distillery[523] In a 7-2 decision, the Supreme Court determined that the defendant lacked a privacy interest in banking records.[524] Soon thereafter, in *Smith* v. *Maryland*, the Court found that a pen register placed on a suspect's telephone line did not implicate the Fourth Amendment.[525]

In *Riley*, the Court expressed a healthy skepticism towards a doctrine developed in the 1970s. It noted that modern cell phone technologies did not even exist in the 1990s; indeed, it found the term "cell phone" to be misleading: "They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[526] Their capacity dwarfs what one might previously have been able to transport, with a typical smart phone, at a capacity of 16 gigabytes, able to hold "millions of pages of text, thousands of pictures, or hundreds of videos."[527] The Court noted that these observations did not even begin to take into account cloud computing. For the Court, it is a new world. To the extent that search

---

522. *Id.* (internal citations omitted).
523. United States v. Miller, 425 U.S. 435 (1976).
524. *Id.*
525. Smith v. Maryland, 442 U.S. 735 (1979).
526. Riley v. California, 134 S. Ct. 2473, 2489 (2014).
527. *Id.*

might implicate "the privacies of life,"[528] the government must meet a higher standard.

### *4. Notice and Section 702-derived Evidence*

The FAA authorizes the government to use Section 702-obtained material for criminal prosecution, provided that the Attorney General provides advance authorization and that proper notice is given to the court or governmental entity involved as well as to individuals against whom the information will be used.[529] The obligation applies (1) "[w]henever the government intends to enter into evidence or otherwise use or disclose" (2) "in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States," (3) "against an aggrieved person" (4) "any information obtained or derived from" (5) an "electronic surveillance [or physical search] of that aggrieved person."[530] The government is required, *prior* to legal proceedings, to notify the aggrieved person and the court (or other authority), that information is to be disclosed or used.[531] The defendant may challenge the use of the information on the grounds that it was unlawfully obtained, or that it was not acquired consistent with an order of authorization or approval.[532] It is not clear that the government is abiding by the requirement that it reveal to defendants that information acquired under the FAA is being used in prosecution. This in turn demonstrates the importance of inserting judicial review into the process immediately once the inquiry turns criminal in nature.

---

528. *Id.* at 2495.

529. The FAA accomplishes this by folding the use of information obtained under Section 702 into the requirements for using information acquired via traditional FISA in criminal trials. Information obtained under Section 702 is "deemed to be" information acquired via Title I of FISA for purposes related to the applicability of the notice requirement and the suppression and discovery provisions contained in traditional FISA. 50 U.S.C. § 1881e(a) (2012).

530. *Id*. § 1806(c).

531. *Id.*

532. *Id.* § 1806 (f).

*a. Criminal Law Standard*

As a matter of criminal law, Title III does not forbid the interception of incidental or "nonpertinent" communications. Instead, the statute "requires that measures be adopted to reduce the extent of such interception to a practical minimum while allowing the legitimate aims of the [g]overnment to be pursued."[533] The government must minimize its interception of conversations that do not implicate predicate offenses.[534] The order may not authorize interception "for any period longer than is necessary to achieve the objective of the authorization," with an outside window of thirty days.[535] Courts keep a close eye on law enforcement to ensure that these steps are being followed.[536]

Even with these precautions, at times information relating to other criminal activity is intercepted. If the communications relate to offenses not specified in the original order, the extent to which information may be used is governed by statute.[537] The contents of incidental communications, and any evidence derived from them, may be disclosed in subsequent proceedings only after further authorization or approval by a judge, with the application having been made "as soon as practicable," and the judge having determined that the contents were obtained consistent with the statute.[538]

The law specifies neither the precise form of an application, nor the exact procedures that need to be followed by the judiciary in granting or denying the application.[539] Courts look to the legisla-

---

533. United States v. Turner, 528 F.2d 143, 156 (9th Cir. 1975); *see also* United States v. Ozar, 50 F.3d 1440, 1448 (8th Cir. 1995) (considering minimization requirements met in bank fraud case); Wayne R. LaFave et al., 2 CRIM. PROC. § 4.6(h) (3d ed. 2004).

534. 18 U.S.C. § 2518(5) (2012).

535. *Id.*

536. *See, e.g.*, Dennis K. Berman, *The Galleon Legacy: White-Collar Wiretaps*, WALL ST. J., May 12, 2011, http://online.wsj.com/news/articles/SB10001424052748704681904576317641529229136 [http://perma.cc/5R7D-C35Y] (quoting a federal judge who discovered that the FBI had listened in to personal details in phone calls between defendants in one case, calling it "nothing short of disgraceful").

537. Robert A. Morse, Annotation, Propriety, under 18 U.S.C.A. § 2517(5), of Interception or Use of Communications Relating to Federal Offenses Which Were Not Specified in Original Wiretap Order, 103 A.L.R. FED. 422, § 2[a] (1991).

538. 18 U.S.C. § 2517(5) (2012).

539. *See generally id*. § 2517 (absence therein of specific guidance of subsequent application or procedure to be followed).

tive history of the statute for the appropriate standard, requiring that the subsequent application "include a showing that the original order was lawfully obtained, that it was sought in good faith and not as a subterfuge search, and that the communication was in fact incidentally intercepted during the course of a lawfully executed order."[540]

The purpose behind requiring law enforcement to return to a court is to ensure that the executive branch does not evade the restrictions placed upon applications for original wiretap orders, such as the belief that the target is involved in the commission of a serious offense.[541] For incidental information to be admitted at trial, all of the statutorily required conditions for the intercept have to be present at the time of the original application for the wiretap order.[542] Absent such requirements, law enforcement could otherwise conduct a "subterfuge search," wherein the application appears to relate to a particular crime, but the applicant anticipates intercepting evidence of different crimes for which the prerequisites could not otherwise be satisfied.[543] It was to prevent such searches that Congress inserted the requirement that law enforcement return to a magistrate.[544] This was the compromise struck between protecting the Fourth Amendment right to privacy and the inadvertent discovery of criminal activity.[545]

Congress and the courts frown on the deliberate interception of incidental information. What law enforcement may *not* do is begin collecting U.S. citizens' communications generally, looking for any information that might be relevant to the target of their investigation. This would be an absurd interpretation of criminal law and roundly rejected by the judicial system. Instead, for every piece of information sought, such as records held by others, law

---

540. S. REP . NO. 90-1097, at 2189 (1968).

541. *See* United States v. Arnold, 773 F.2d 823, 829 (7th Cir. 1985); United States v. Marion, 535 F.2d 697, 700–01 (2d Cir. 1976); Morse, *supra* note 537, at § 9.

542. *Arnold*, 773 F.2d 829.

543. Morse, *supra* note 537, at § 9. *See also* United States v. Smith , 726 F.2d 852, 865 (1st Cir. 1984); United States v. Campagnuolo, 556 F.2d 1209, 1213 (5th Cir. 1977); *Marion*, 535 F.2d at 700–01.

544. *See, e.g.*, *Smith*, 726 F.2d at 856; *Campagnuolo*, 556 F.2d at 1213.

545. Morse, *supra* note 537, at § 10. There is some confusion about whether additional approval is required where the "other offense" not authorized by the original order includes the same elements as the offenses forming the basis for the original order. *See id.*

enforcement must demonstrate that the information is relevant to the target or specific investigation underway.

*b. Notice Under the FAA: Theory and Practice*

Information obtained under traditional FISA may be used in criminal prosecution. But acquisition of communications under Section 702 includes none of the procedural protections that mark Title III or traditional FISA.[546] At no point in the process is anything approximating a warrant obtained. The statute allows the intercepts to be used to prosecute crimes unrelated to the offense for which information was being sought. At no point must an application seek judicial approval for the use of electronic intercept information relating to "other offenses."[547]

Under the FAA, the government is required to provide notice to "aggrieved persons" that information obtained from Section 702 is to be used prior to trial.[548] Accordingly, in 2012 the Obama Administration informed the Supreme Court that

546. *But see In re* Directives [redacted] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1013 (FISA Ct. Rev. 2008) (addressing prior judicial review, probable cause, and particularity required under the Warrant Clause and finding that the safeguards in the PAA (such as targeting procedures, minimization procedures, procedure to ensure that a significant purpose of surveillance is to obtain foreign intelligence, procedures incorporated via Executive Order No. 12,222, § 2.5, and procedures outlined in affidavit supporting certifications) meet the standard).

547. *Cf.* 18 U.S.C. § 2517(5) (2012).

548. For cases considering whether FISA information is discoverable because of its importance to the defense, *see, e.g.*, United States v. Amawi, 695 F.3d 457, 474–75 (6th Cir. 2012); United States v. El-Mezain, 664 F.3d 467, 563–70 (5th Cir. 2011); United States v. Duggan, 743 F.2d 59, 78 (2d Cir. 1984); United States v. Belfield, 692 F.2d 141, 146–47 (D.C. Cir. 1982). For examples of cases considering whether information obtained from traditional FISA should be suppressed, *see, e.g.*, United States v. Aldawsari, 740 F.3d 1015, 1017–19 (5th Cir. 2014); United States v. Campa, 529 F.3d 980, 993–94 (11th Cir. 2008); United States v. Hammoud, 381 F.3d 316, 331–34 (4th Cir. 2004) (en banc), *reinstated in relevant part,* 405 F.3d 1034, 1034 (4th Cir. 2005). *See generally* ROBERT TIMOTHY REAGAN, FED. JUDICIAL CTR., FOREIGN INTELLIGENCE SURVEILLANCE ACT LITIGATION 25 nn.218–19 (2014). Note that although courts do not tend to provide FISA material information directly to defendants, we are beginning to see exceptions to this rule. *See, e.g.*, United States v. Daoud, No. 12 CR 723, 2014 WL 321384, at *3 (N.D. Ill. Jan. 29, 2014), *rev'd* 755 F.3d 479 (7th Cir. 2014) ("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 material.").

this was DOJ's practice.[549] In *Clapper v. Amnesty International*, Justice Samuel Alito relied in part on this claim to support the Court's holding.[550]

The question was whether plaintiffs had standing to challenge the constitutionality of Section 702. The Court underscored that other protections were in place: "[I]f the Government intends to use or disclose information obtained or derived from a [Section 702] acquisition in judicial or administrative proceedings, it must approve advance notice of its intent, and the affected person may challenge the lawfulness of the acquisition."[551] While this position was consistent with the statutory requirement, it did not reflect DOJ's actual practice. In December 2012, during FAA renewal debates, Senator Diane Feinstein credited the statute with providing information material to the prosecution of domestic terrorism cases.[552] She cited one hundred arrests between 2009 and 2012.[553] Feinstein went on to discuss cases related to charges of material support, use of weapons of mass destruction, and bombing and assassination plots.[554] Lawyers in two of the cases mentioned responded by asking prosecutors to confirm whether information obtained under the FAA had been used.[555] On May 21, 2013, months after the arguments in *Clapper*, prosecutors in Fort Lauderdale filed a document with the courts saying that they were under no obligation to disclose whether evidence used against defendants was derived from data authorized by Section

549. Reply Brief for the Petitioners at 15, Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2012) (No. 11-1025) ("[T]he government must provide advance notice of its intent to use information obtained or derived from [Section 702]-authorized surveillance against a person in judicial or administrative proceedings and that person may challenge the underlying surveillance."); *see also* Transcript of Oral Argument at 4, Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2012) (No. 11-1025) (recognizing "notice that the government intends to introduce information in a proceeding against" a defendant).

550. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1154 (2013).

551. *Id.*

552. See 158 CONG. REC. S8384-02 (daily ed. Dec. 27, 2012) (statement of Sen. Feinstein).

553. *Id.*

554. *Id.*

555. Eric Schmitt et al., *Administration Says Mining of Data is Crucial to Fight Terror*, N.Y. TIMES, June 7, 2013, http://www.nytimes.com/2013/06/08/us/mining-of-data-is-called-crucial-to-fight-terror.html?adxnnl=1&adxnnlx=1400077249-sDWgE37vt/sPPW0v8d+J7Q [http://perma.cc/5UU2-8NL6].

702.[556] According to the government, such notification would be "unwarranted and unprecedented."[557]

Solicitor General Donald B. Verrilli, Jr. questioned national security lawyers as to why he had not been informed of this policy prior to his submission of briefs to the Supreme Court or his preparation for oral argument in *Clapper*.[558] He was reportedly informed that it had been a misunderstanding, stemming from a narrow definition of what "derived from" meant.[559] In other words, a distinction could be drawn between information obtained, versus derived, from Section 702. The former equates to actual acquisitions, while the latter may be a product of subsequent searches of the data and further analysis.

A two-month debate within DOJ ensued as to whether prosecutors were required to provide information to defendants regarding information derived from Section 702.[560] Ultimately, the government changed its position to align with Verrelli's representation. In July 2013, DOJ filed a document with the Court saying, in a footnote, that while their prior filing in the Florida case might have been "construed to assert" that they did not need to disclose when such evidence had been used, "that is not the government's position."[561]

Dispute about the use of FAA-derived information in criminal cases continues. In October 2013, the ACLU filed a FOIA-related complaint in the Southern District of New York, seeking "records related to the government's use of evidence derived from surveillance authorized by" the FAA.[562] In light of settlement negotiations, Judge Robert W. Sweet held the case in abeyance.[563] And in

---

556. Devlin Barrett, U.S. Spy Program Lifts Veil in Court: Justice Department Says Prosecution in Terrorist Cases Must Tell Defendants When Surveillance Program Was Used, WALL ST. J., July 31, 2013, http://www.wsj.com/articles/SB10001424127887323854904578638363001746552 [http://perma.cc/5SDG-AW33].

557. *Id.*; *see also* Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. TIMES, Oct. 16, 2013, http://www.nytimes.com/2013/10/17/us/politics/us-legal-shift-may-open-door-for-challenge-to-secret-wiretaps.html?_r=0 [http://perma.cc/DT9G-DKQB]; Schmitt, *supra* note 555.

558. Savage, *supra* note 557.

559. *Id.*

560. *Id.*

561. Barrett, *supra* note 556.

562. Complaint, ACLU v. U.S. Dep't of Justice, No. 1:13-cv-7347 (S.D.N.Y. Oct. 17, 2013).

563. Order, ACLU v. U.S. Dep't of Justice, No. 1:13-cv-7347 (S.D.N.Y. Jan. 16, 2014).

a May 2014 letter to Verrilli, Senators Mark Udall of Colorado and Ron Wyden of Oregon accused DOJ as not being forthright about its misrepresentation to the Court in *Clapper*.[564] The government has not yet responded.

In the six months following DOJ's shift in policy, the government submitted Section 702 notices in just three cases.[565] Two of

---

564. Charlie Savage, *Justice Department Criticized on Spying Statements*, N.Y. TIMES, May 13, 2014, http://www.nytimes.com/2014/05/14/us/justice-dept-criticized-on-spying-statements.html [http://perma.cc/35LW-P7NK].

565. In the first case, involving charges of material support, U.S. Attorney Loretta Lynch informed the defendant that the government had used information from Section 702 to obtain an order under traditional FISA. Letter from Loretta E. Lynch, United States Attorney, E.D.N.Y., to Agron Hasbajrami (Feb. 24, 2014), *available at* https://www.documentcloud.org/documents/1028728-hasbajrami-supplemental-notice-2-24-2014.html [http://perma.cc/23W7-SABS]. In the government's view, however, because he had pled guilty in 2012, he had given up his right to appeal. *Id.* The defendant had been arrested in September 2011 at JFK as he was preparing to leave the United States. Accused of providing material support to a foreign terrorist organization, he faced 60 years in prison, but agreed to plead guilty in exchange for a limit of 15 years' imprisonment. Charlie Savage, *Justice Department Informs Inmate of Pre-Arrest Surveillance*, N.Y. TIMES, Feb. 25, 2014, http://www.nytimes.com/2014/02/26/us/justice-dept-informs-inmate-of-pre-arrest-surveillance.html [http://perma.cc/7ZE6-9FHW].

The second case involved a nineteen-year-old, Somali-born student at Oregon State, convicted in January 2013 of attempting to use a weapon of mass destruction. *See* United States v. Mohamud, 941 F. Supp. 2d 1303 (D. Or. 2013); *see also* Indictment, United States v. Mohamud, No. 3:10-CR-00475-KI (D. Or. Nov. 29, 2010), Docket No. 2. In 2009 the FBI intercepted Mohamud's emails with an individual suspected of recruiting for terrorist organizations. Colin Miner et al., *FBI Says Oregon Suspect Planned 'Grand' Attack*, N.Y. TIMES, Nov. 27, 2010, http://www.nytimes.com/2010/11/28/us/28portland.html?pagewanted=all&_r=0 [http://perma.cc/LC45-F7QU]. In November 2013, eleven months after his conviction, the government informed the defendant that information obtained or derived from traditional FISA might also have been related to prior Section 702 collection. Supplemental FISA Notification, United States v. Mohamud, No. 3:10-CR-00475-KI (D. Or. Nov. 19, 2013), Docket No. 486. The government acknowledged that the notice had been untimely. Government Discovery Opposition Brief at 9 n.5, 12, United States v. Mohamud, No. 3:10-CR-00475-KI (D. Or. Feb. 13, 2014), Docket No. 491. Efforts to challenge the use of Section 702 evidence on Fourth Amendment grounds failed. Opinion and Order, United States v. Mohamud, No. 3:10-CR-00475-KI (D. Or. Mar. 19, 2014), Docket No. 499.

The third case involved notification to Jamshid Muhtorov, whose case had not yet gone to trial—to date, the only case in which the government has provided prior notice of Section 702-derived information. Muhtorov was arrested at O'Hare airport on his way to Turkey on January 21, 2012. Complaint, United States v. Muhtorov, No. 1:12-cr-00033-JLK (D. Colo. Jan 19, 2012), Docket No. 1; Indictment, United States v. Muhtorov. No. 1:12-cr-00033-JLK (D. Colo. Jan. 23, 2012), Docket No. 5. In October 2013, the government filed a Section 702 notice. FISA Notice, United States v. Muhto-

the cases were already post-conviction. The failure to provide prior notice meant that defendants had not had the opportunity to challenge the FAA as unconstitutional either on its face or as applied. They had been unable to address whether the surveillance evidence tainted pretrial motions or defenses at trial, or whether the government had engaged in overreaching, misrepresentation, or misconduct during either pre-trial or trial proceedings. These cases are the only ones, as of the time of writing, to involve Section 702 notice. Even the two cases discussed by Feinstein, which spurred the debate, did not later result in notice being served.[566]

At a minimum, government practice appears to be conservative in informing defendants of the use of Section 702 information.[567] To the extent that, as a result of *Clapper*, only those so notified may have standing to challenge the constitutionality of Section 702, the pool of potential challengers to the FAA is limited. This underscores the importance of inserting judicial supervision into the procedure earlier in the process to protect important Fourth Amendment considerations.

### *D. Reasonableness Standard*

Courts have routinely recognized that regardless of whether the warrant clause applies, the domestic interception of electronic communications, and the international collection of communications involving individuals with a substantial connection to the United States, must still comport with the Fourth Amendment's

---

rov, No. 1:12-cr-00033-JLK (D. Colo. Oct. 25, 2013), Docket No. 457. The defendant's motion to suppress was filed in January 2014. Motion, United States v. Muhtorov, No. 1:12-cr-00033-JLK (D. Colo. Jan. 29, 2014), Docket No. 520. On May 9, 2014 the government filed both a classified and an unclassified memorandum in opposition to the defendant's motion. Response to Motion, United States v. Muhtorov, No. 1:12-cr-00033-JLK (D. Colo. May 9, 2014), Docket No. 559.

566. Prosecutors submitted documents to the court saying that they did not plan to use FAA-derived materials. A letter from a Senate lawyer, in turn, conveyed that Senator Feinstein "did not state, and did not mean to state" that the cases were linked to the warrantless surveillance program. Savage, *supra* note 564. Defense lawyers protested to the court that the references to their clients had not been random, but instead had been part of the debate over whether to renew authorities under the 2008 FAA. *Id.* Senator Feinstein declined comment. *Id.*

567. During her remarks, Feinstein noted that in 2012 alone there had been 16 domestic terrorism arrests. 158 CONG. REC. S8384-02 (daily ed. Dec. 27, 2012) (statement of Sen. Feinstein). However, only one person who had yet to go to trial had, between July 2013 and June 2014, received a Section 702 notice.

reasonableness requirement.[568] The NSA's use of "about" collection, and the interception of domestic conversations in MCTs, fall outside constitutionally acceptable bounds.

As a matter of domestic criminal law, in determining whether a search is reasonable under the Fourth Amendment, the Court looks to the totality of the circumstances.[569] This test amounts to a balancing test of the interests at stake.[570] It considers the nature of the government intrusion into privacy.[571] By looking at the manner in which the search is implemented, and weighing it against individual interests involved, the Court ascertains whether the action in question is reasonable. The greater the government interest that is involved, the greater the intrusion that may be permitted, as long as the privacy protections are sufficient in light of the stated governmental interest.[572]

In relation to searches conducted abroad, three circuit courts have considered how best to think about the reasonableness standard, creating in the process two different approaches. For the Ninth Circuit, the court looks to whether, in joint investigations conducted overseas, U.S. officials act in accordance with foreign law.[573] In 1987, then Judge (and now Justice) Kennedy explained that the exclusionary rule applies only where U.S. officials fail to act in good faith reliance on foreign law.[574] This approach has been adopted with regard to physical searches and wiretaps conducted overseas.[575]

Under the Ninth Circuit approach, constitutional rights depend in some form on foreign legal systems and relevant laws.

---

568. *See, e.g.*, United States v. Place, 462 U.S. 696 (1983).

569. Samson v. California, 547 U.S. 843, 848 (2006); Tennessee v. Garner, 471 U.S. 1 (1985). See *also* Scott v. United States, 436 U.S. 128 (1978) (finding the acquisition of virtually all conversations reasonable and underscoring that reasonableness depends on the facts and circumstances of each case).

570. *Samson*, 547 U.S. at 848–50; United States v. Knights, 534 U.S. 112, 118–19 (2001).

571. *Garner*, 471 U.S. at 8 (quoting *Place*, 462 U.S. at 703).

572. Michigan v. Summers, 452 U.S. 692, 699–701 (1981); *In re* Directives [REDACTED] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008).

573. United States v. Peterson, 812 F.2d 486 (9th Cir. 1987).

574. *Id.*

575. *See, e.g.*, United States v. Barona, 56 F.3d 1087, 1092–93 (9th Cir. 1995); United States v. Rosenau, No. CR06-157MJP, 2011 WL 4957357, at *2 (W.D. Wash. Oct. 18, 2011); Lau v. United States, 778 F. Supp. 98, 101 (D.P.R. 1991); United States v. Scarfo, CRIM.A. No. 88-00003-1-19, 1988 WL 115805, at *4 (E.D. Penn. Oct. 26, 1988).

Although this seems odd at the outside, it reflects Justice Kennedy's practical approach to the Fourth Amendment: for joint operations, it would be hard to proceed in a manner that constantly second-guesses the law of the jurisdiction in which the United States is operating.

The problem with applying the Ninth Circuit approach to the FAA is that in its global intercepts, the intelligence community is not operating solely according to one set of laws. Upstream collection may include the interception of packets that pass through dozens of different countries. It would be impossible to apply each law's contours as even one packet moves over the network—much less as all the packets that constitute a communication, or tens of thousands of communications. Even taking into account the Five Eyes, such operations could not properly be understood as joint operations of the sort considered by the Ninth Circuit in *Barona*.

Perhaps because of these difficulties, the FISA Court of Review has looked to the second approach—one that has been adopted only recently—and applied the balancing test to the international environment. In 2008 the Second Circuit became the first to employ the balancing test. In *In re Terrorist bombings of U.S. Embassies in East Africa*, the Court employed a reasonableness analysis that weighed governmental interests against the privacy intrusion involved.[576] In 2013 the Seventh Circuit largely followed course.[577]

This is the test to which the FISA Court of Review has appealed in considering the reasonableness of intercepts overseas. An important point to note at the outset, though, is the trouble with applying a criminal law approach to the foreign intelligence realm. The overwhelming nature of U.S. national security interests—which FISC considers "of the highest order of magnitude"[578] create a heavy burden to be overcome. National security, in other

576. *In re* Terrorist Bombings of US Embassies in East Africa, 552 F.3d 157, 167 (2d Cir. 2008).

577. United States v. Stokes, 726 F.3d 880 (7th Cir. 2013). Although Professor Kerr reconciles these two approaches, it is not necessary to do so in light of the types of questions presented by unilateral NSA surveillance overseas. *See* Kerr, *supra* note at 434.

578. *In re* Directives [redacted] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008); *see also* Haig v. Agee, 453 U.S. 280 (1981); *In re* Sealed Case, 310 F.3d 717, 746 (FISA Ct. Rev. 2002).

words, is a powerful trump card. As soon as a foreign intelligence purpose is introduced, the standards for reasonableness shift.

While the targeting procedures and the interception of information to or from non-U.S. persons located outside the United States meet the Fourth Amendment's standard of reasonableness, when looked at in relation to Section 702, the inclusion of communications "about" targets or selectors and the knowing interception of entirely domestic conversations shift the program outside constitutional bounds.

### *1. Criminal Law Versus National Security Law*

In *In re Sealed case*, in which the FISA Court of Review held that traditional FISA did not require the government to demonstrate that the primary purpose of electronic surveillance was not criminal prosecution, and that the shift in language to a "significant purpose" was consistent with the Fourth Amendment, the Court drew attention to six categories to flesh out whether the protections afforded to targets are reasonable: prior judicial review, the presence (or absence) of probable cause, particularity, necessity, duration, and minimization.[579]

Six years later, the FISA Court of Review, responding to a telecommunication service provider's challenge to the PAA, was careful to note that the test from *In re Sealed Case* should not be treated as a rigid framework on the grounds that it would contradict the "totality of the circumstances test".[580]

The test derives from criminal law, in the context of which the Supreme Court, like the FISA Court of Review, has enumerated factors that must be taken into account to determine whether the procedures followed in minimization are reasonable. In *Scott v. United States*, the Court considered the month-long surveillance of a telephone used in a narcotics conspiracy, in the course of which only some 40% of the conversations were related to the crime in question.[581] In finding the minimization procedures (or lack thereof) reasonable, the Court explained,

> [B]lind reliance on the percentage of nonpertinent calls intercepted is not a sure guide to the correct answer. Such percent-

579. *In re Sealed Case*, 310 F.3d at 737–41.

580. *In re Directives*, 551 F.3d at 1012–13.

581. Scott v. United States, 436 U.S. 128 (1978).

> ages may provide assistance, but there are surely cases, such as the one at bar, where the percentage of nonpertinent calls is relatively high and yet their interception was still reasonable. The reasons for this may be many. Many of the nonpertinent calls may have been very short. Others may have been one-time only calls. Still other calls may have been ambiguous in nature or apparently involved guarded or coded language. In all these circumstances agents can hardly be expected to know that the calls are not pertinent prior to their termination.[582]

The Court's position is worth considering at length:

> In determining whether the agents properly minimized, it is also important to consider the circumstances of the wiretap. For example, when the investigation is focusing on what is thought to be a widespread conspiracy more extensive surveillance may be justified in an attempt to determine the precise scope of the enterprise. And it is possible that many more of the conversations will be permissibly interceptable because they will involve one or more of the co-conspirators. The type of use to which the telephone is normally put may also have some bearing on the extent of minimization required. For example, if the agents are permitted to tap a public telephone because one individual is thought to be placing bets over the phone, substantial doubts as to minimization may arise if the agents listen to every call which goes out over that phone regardless of who places the call. On the other hand, if the phone is located in the residence of a person who is thought to be the head of a major drug ring, a contrary conclusion may be indicated.[583]

The Court noted that other factors may play a significant role, such as the point at which law enforcement intercepted the communications. During the initial phase of surveillance, officers may be expected to collect more information than at the later stages, by which point categories of nonpertinent communications will have been established and identification of nonpertinent discussions more efficiently made. The Court contemplated a learning curve for law enforcement, where the standards applied may shift based on the evolution and maturity of the electronic surveillance.[584]

---

582. *Id.* at 140.
583. *Id.*
584. *See id.* at 141.

In *Scott*, most of the nonpertinent calls were either "very short," "ambiguous in nature," or one-time conversations.[585] Therefore they did not amount to a violation of the minimization requirement. The subjective intent of law enforcement in *Scott* was of little consequence. Even though, as the district court had found, the officers had made "no attempt to comply" with the statutory requirement, the Supreme Court looked to the broader context. Resultantly, courts have considered similar charges on a case-by-case basis.[586]

In translating the totality of the circumstances test to national security law, the unique nature of foreign intelligence gathering matters. As the FISA Court of Review explained in *In Re Sealed Case*, "[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."[587] Therefore, it is common practice in FISA surveillance to leave devices on, with the emphasis on minimization occurring at the back end, in the process of indexing and logging the relevant communications.[588] For the FISA Court of Review, the possibility that the government might, in this process, make a mistake, was not sufficient to invalidate the surveillance in question.[589]

In defense of its practices with regard to the PAA, the government emphasized the protections embedded in the statute, as well as those incorporated in the certifications and directives.[590]

---

585. 436 U.S. at 141–42.

586. United States v. Quintana, 508 F.2d 867, 873–74 (7th Cir. 1975); *see also* United States v. Dumes, 313 F.3d 372, 380 (7th Cir. 2002); United States v. McGuire, 307 F.3d 1192, 1200–01 (9th Cir. 2002); United States v. Mansoori, 304 F.3d 635, 647 (7th Cir. 2002); United States v. Brown, 303 F.3d 582, 603–06 (5th Cir. 2002); United States v. Bennett, 219 F.3d 1117 (9th Cir. 2000); United States v. Uribe, 890 F.2d 554, 557 (1st Cir. 1989); United States v. Adams, 1115 759 F.2d 1099 (3d Cir. 1985).

587. *In re Sealed Case*, 310 F.3d at 741.

588. *Id.* at 740.

589. *In re Directives*, 551 F.3d at 1015.

590. *Id.* at 1013 (listing 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 12,333, Section 2.5, and procedures outlined in an affidavit supporting the certifications).

FISCR accepted the government's position.[591] Arguments regarding particularity and prior judicial review fell short in light of how the PAA had been applied. While the statute did not require a particularized showing, the "pre-surveillance procedure" (which remains classified) established steps "analogous to and in conformity with the particularity showing" considered by FISCR in *In re Sealed Case*.[592]

The particularity requirement contemplated by the FISA Court of Review in *In re Sealed Case* related to the probable cause standards in traditional FISA.[593] Applied to the PAA, FISCR found in *In re Directives* that the procedures incorporated via Executive Order 12,333, Section 2.5, as applied via certifications and directives, offset the probable cause concern. That section states, in pertinent part, that the Attorney General is given the authority to approve any techniques within the United States or against a U.S. person overseas, where "a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is *probable cause* to believe that the technique is directed against a foreign power or an agent of a foreign power."[594]

What this requirement means is that for the intelligence community to act upon a certification, the Attorney General first has to establish probable cause that the U.S. person being targeted is a foreign power or an agent thereof.[595] Combined with other protections, such as minimization, the procedures offered sufficient compensation for any encroachments into individual privacy, bringing the PAA within the bounds of the Fourth Amendment.[596]

---

591. *Id.* ("Notwithstanding the parade of horribles trotted out by the petitioner, it has presented no evidence of any actual harm, any egregious risk of error, or any broad potential for abuse in the circumstances of the instant case. Thus, assessing the intrusions at issue in light of the governmental interest at stake and the panoply of protections that are in place, we discern no principled basis for invalidating the PAA as applied here.").

592. *In re Directives*, 551 F.3d at 1013–14.

593. *In re Sealed Case*, 310 F.3d at 740.

594. Exec. Order 12,333, § 2.5, 3 C.F.R. 200, 212 (1982) (emphasis added).

595. *In re Directives*, 551 F.3d at 1014.

596. *Id.* at 1013.

This analysis makes sense in light of the Court's Fourth Amendment jurisprudence and the manner in which traditional FISA has operated. Where the target is a U.S. person based overseas, or within the United States, the Attorney General (under the PAA), or the FISA Court of Review (under the FAA) must verify probable cause of wrongdoing prior to the interception of communications to or from the target.

In October 2011 Judge John Bates considered the reasonableness of the NSA's targeting and minimization procedures. The court had previously found the targeting and minimization procedures to be constitutionally sufficient on the grounds that the procedures reasonably confined acquisitions to targets who were non-U.S. persons located outside the United States and thus outside the protections of the Fourth Amendment.[597] In October 2011 Bates concluded that, to the extent that the targeting procedures, as applied to the acquisition of information *other than* Internet transactions (meaning, telephone and Internet communications) still reflected the Court's previous assumptions, they were consistent with the Fourth Amendment reasonableness requirement. The problem, for Judge Bates, was the interception of Internet transactions involving either single discrete communication (Single Communication Transactions, or SCTs) or multiple discrete communications (Multi-Communication Transactions, or MCTs).[598] Here, Fourth Amendment reasonableness questions loomed large. The reason these communications changed the picture is because they allowed for the collection of wholly domestic conversations, as well as communications between U.S. persons. As a matter of statutory interpretation, the only way in which such conversations could be intercepted is by interpreting the statute to include not just communications to or from a target, but also communications *about* the target or selector.

### *2. Incidental Interception*

In its October 2011 opinion, FISC confronted the fact that the number of wholly domestic communications being intercepted was much higher than the Court had previously understood.[599]

---

597. [Redacted], 2011 WL 10945618 at *25 (FISA Ct. Oct. 3, 2011).
598. *Id.* at *9.
599. *Id.* at *11.

The FISA Court of Review explained, "NSA's upstream collection devices will acquire a wholly domestic 'about' SCT if it is routed internationally."[600] The interception of incidental information created constitutional concerns.[601]

Judge Bates underscored the importance of evaluating the government's targeting and minimization procedures in light of the communications actually acquired.[602] The problem was that the sheer volume of information obtained by the NSA via upstream collection made it difficult, as Judge Bates explained, to conduct "any meaningful review of the entire body of the transactions . . ."[603] Only a statistical sampling was possible. ISPs might change their services, giving users greater latitude in customizing services. "As a result, it is impossible to define with any specificity the universe of transactions that will be acquired by NSA's upstream collection at any point in the future."[604]

Actual practice also figured large in FISC's approach to incidental information in *In re Directives*:

> The petitioner's concern with incidental collections is overblown. It is settled beyond peradventure that incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful. *The government assures us that it does not maintain a database of incidentally collected information from non-targeted United States persons*, and there is no evidence to the contrary. On these facts, incidentally collected communications of non-targeted United States persons do not violate the Fourth Amendment.[605]

The problem with the FISA Court of Review's analysis is that, regardless of whether one database exists that is dedicated to incidentally collected information, it is of little moment if the NSA can feed information incidentally collected under Section 702 into other databases. Section 702 data appears to be stored in multiple places.[606] Information is also forwarded to other agencies, such as

---

600. *Id.*

601. *See id.* at *11–12.

602. *Id.* at *9.

603. *Id.* at *10.

604. *Id.*

605. *In re Directives*, 551 F.3d at 1015 (emphasis added) (citations omitted).

606. *See, e.g.*, James Ball & Spencer Ackerman, *NSA loophole allows warrantless search for U.S. citizens' emails and phone calls*, GUARDIAN (Aug. 9, 2013, 12:08 PM),

the National Counterterrorism Center (NCTC), at which point it is no longer associated with the specific authority under which it was collected.[607] For datasets acquired pursuant to Track 3 (where the agency replicates the data sets obtained from other agencies), "NCTC may conduct (i) queries that do not consist of, or do not consist exclusively of, terrorism data points, and (ii) pattern-based queries and analyses."[608]

Although Judge Bates concluded in October 2011 that the 2009 minimization procedures did not pass constitutional muster, the following month he approved new procedures as consistent with the Fourth Amendment.[609] Insofar as "about" communications are monitored, retained, and mined for further information, and entirely domestic conversations captured and used in subsequent criminal prosecution, the procedures do not comport with constitutional requirements.

Returning to the six categories for reasonableness laid out by FISA Court of Review, there is no prior judicial review approving the targeting of individuals whose communications are being intercepted.[610] There is neither the presence (nor absence) of probable cause—indeed, there is no standard applied (collection under

---

http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls [http://perma.cc/B5FN-SEGN] (containing screen shot of classified document). *See also* James Risen & Laura Poitras, *N.S.A. Gathers Data on Social Connections of U.S. Citizens*, N.Y. TIMES, Sept. 28, 2013, http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?pagewanted=all&_r=0 [http://perma.cc/RGE7-PQYD].

607. While it is thus important that agencies like NCTC adopt safeguards to ensure the integrity of datasets and access to the information contained therein, such protections do not reach the front-end collection considerations entailed in Section 702 programs. *See, e.g.*, NAT'L COUNTERTERRORISM CTR., ATTORNEY GENERAL GUIDELINES FOR ACCESS, RETENTION, USE AND DISSEMINATION BY THE NATIONAL COUNTERTERRORISM CENTER AND OTHER AGENCIES OF INFORMATION IN DATASETS CONTAINING NON-TERRORISM INFORMATION, ANNUAL REPORT ON THE ACCESS, RETENTION, USE, AND DISSEMINATION OF UNITED STATES PERSON INFORMATION, *available at* http://www.nctc.gov/docs/2012-2013_NCTC_AGG_Annual_Report_(redacted).pdf [http://perma.cc/73CR-H9L3]; NAT'L COUNTERTERRORISM CTR., OVERVIEW OF THE BASELINE SAFEGUARD PROTECTIONS UNDER NCTC'S 2012 ATTORNEY GENERAL GUIDELINES, *available at* http://www.nctc.gov/docs/NCTCWhitePaperOverviewofNCTC2012AGGBaselineSafeguards050114.pdf [http://perma.cc/VAJ7-Q4Y2].

608. NAT'L COUNTERTERRORISM CTR., ATTORNEY GENERAL GUIDELINES, *supra* note 607, at 7.

609. [Redacted], 2011 WL 10945618 at *1 (FISA Ct. Oct. 3, 2011).

610. *In re Sealed Case*, 310 F.3d at 737–41.

Section 702 being outside the confines of either Executive Order 12,333, Section 2.5 or FAA Sections 703–704). There is no particularity involved (the target being another individual, entity, or selector and the collection broad). The argument that targeting and minimization procedures satisfy this requirement may hold for to or from communications, but neither of these procedures limits the universe of communications that could be monitored and intercepted as an aspect of "about" collection in any meaningful way. The interception of communications, programmatic in nature, is not required to be of limited duration. And the minimization procedures, far from rectifying the problem, require the NSA to retain and to pass on information for subsequent criminal prosecution. Even if one follows the direction of the FISA Court of Review in *In re Directives* and looks at these not as strict categories to be satisfied but rather,as a general balancing test, that none of them are actually satisfied is probative of the constitutionality of using incidentally collected information in prosecution.

In *In re Directives*, the government pointed to a series of non-statutory documents: targeting and minimization procedures, an internal procedure adopted to ensure that a significant purpose of the surveillance is to obtain foreign intelligence information, procedures incorporated via Executive Order 12,333, and procedures outlined in an affidavit supporting the certifications.[611] But the Court's discussion focused on the targeting of certain customers (as applied), under the PAA. It did not address incidentally-obtained information under Section 702 (as derived from the to, from, or about interpretation) and its subsequent use in criminal prosecution.

Nor did the Court consider the query of data using U.S. identifier information. As with TFA and incidental collection, this practice falls outside the Fourth Amendment's reasonableness requirement. At no point has the collection of the information in question been subjected to prior judicial review with anything even approaching particularity. Instead, one order suffices for nearly 90,000 targets on the grounds that some sort of foreign intelligence information may be obtained.[612] This is then used to

611. *In re Directives*, 551 F.3d at 1013.

612. Although Sections 703–704 require a statement of the basis of the certification that the information sought is the type of foreign intelligence information designated, Section 702 does not.

monitor U.S. persons' international communications, some of which may be collected, despite the absence of any contact between the U.S. person and the targets approved by the FISA Court of Review. The FBI may then query this data to attempt to find evidence of criminality unrelated to foreign affairs. It may use U.S. person information to probe the information, without any prior judicial oversight or subsequent accountability. Information about who can access the database, what they use as a query, what information is obtained, and how it is used is not even tracked, much less subjected to oversight. This practice falls outside acceptable constitutional bounds.

## IV. CONCLUSION

As a matter of public discourse, much remains unknown about how elements of the intelligence community are making use of Section 702 authorities.[613] What is clear is that there are many difficult questions associated with the NSA's exercise of the FAA. This Article has sought to explain the evolution of Section 702, to analyze the statutory framework, and to address constitutional concerns raised by the legislation and the manner in which it has been applied.

The most concerning aspect of the NSA's targeting practices under the FAA is the inclusion of TFA. Together with generous assumptions with regard to foreignness and the vague requirements embedded in the foreign intelligence determination, TFA has allowed the NSA to collect data beyond what might otherwise be considered incidental. Congress may not have anticipated this possibility in 2008. But by 2012 the information had been made available to any Members inclined to read it. The legislature, however, did not take steps to end programmatic collection. Nor

613. The CIA and FBI receive raw data from PRISM. 2011 MINIMIZATION PROCEDURES, *supra* note 171, at, § 6(c). *See also* PCLOB REPORT, *supra* note 2, at 34. Redacted, declassified FISC opinions report that the Court has approved of their minimization procedures. *E.g.*, *In re DNI/AG Certification 2008-A*, No. 702(j)-08-01 (FISA Ct. Aug. 19, 2010), *available at* http://cryptome.org/2013/06/nsa-fisa-certification.pdf [http://perma.cc/DW2M-UT45]. But the documents remain classified. The only semiannual compliance report that has been made public almost entirely redacts the "Trends in CIA Minimization" and the "Review of Compliance Incidents related to CIA minimization procedures." DEC. 2011 SEMIANNUAL ASSESSMENT, *supra* note 245, at 20–22, 35.

did FISC play a strong role with regard to the legality of knowingly collecting entirely domestic conversations. The court's decision encouraged willful blindness: as long as the NSA did not develop sophisticated technologies, it could collect more information and fit within the statutory bounds.

Critique of these developments could be read as simply a complaint that the law went the other way. After all, three branches of government appear to have given the NSA their blessing: Congress through renewal of the FAA, the FISA Court of Review via its approval of certification, targeting, and minimization procedures, and the AG and DNI in their oversight capacities. But the burden borne by the government in the realm of national security is one that requires the public authorities to be consistent with practice. It is concerning that what is being done in practice looks very different than what the law says on its face.

As a matter of post-targeting analysis, despite Congress's concern about reverse targeting, the intelligence community is using U.S. person identifiers to query Section 702 data, potentially accomplishing much the same effect in practice. In regard to data retention and dissemination, the NSA's automatic retention of encrypted material has strong arguments in its favor. But increasing consumer and industrial reliance on encryption may prove to overwhelm the exception, with retention becoming the rule.

As a constitutional matter, Congress and the Executive share foreign affairs powers. Courts acknowledge foreign intelligence gathering as a concomitant of this realm, in which separation of powers doctrine stands in tension with the Fourth Amendment.[614] The domestic foreign intelligence exception to the warrant requirement ended with Congress's enactment of FISA.

One could argue that, following the FAA, the requirements for intercepting U.S. persons' international communications were similarly altered. Bypassing Sections 703 and 704 via incidental collection absent a warrant procedure could thus be challenged on constitutional grounds. The problem with this argument is that following the 2012 renewal of the FAA, the Administration acted not at its weakest, but at its strongest.

---

614. *See, e.g.*, *In re Directives*, at *3 ("At its most elemental level, the petition requires us to weigh the nation's security interests against the Fourth Amendment privacy interests of United States persons.").

The real issue is where foreign intelligence morphs into criminal law. The best example of practice beyond the pale is in the query of Section 702 data using U.S. person information for potential violations of criminal law. It is the very definition of reasonableness under the Fourth Amendment that when a search is conducted, outside of any exceptions, it must be supported by a warwarrant granted by a neutral, disinterested magistrate, upon a finding of probable cause.

Even where the warrant clause does not apply, the statute and programs introduced under its auspices must meet the reasonableness requirements of the Fourth Amendment, as applied within a domestic realm and to U.S. persons based overseas. The targeting procedures and the interception of information to or from non-U.S. persons outside the United States meet the appropriate standard. However, the inclusion of "about" targets or selectors, and the knowing interception of entirely domestic conversations, pushes the NSA's actions beyond constitutional boundaries.

Without doubt, technology has altered the balancing equation, raising the question of how best to protect the privacy of U.S. persons in the context of digitization and international communication flows. The use of information obtained through national security surveillance for law enforcement purposes, though, alters what protections are necessary for Fourth Amendment purposes. What is required is an effort to re-draw the line between national security and criminal law, to ensure that foreign intelligence collection can continue in a manner consistent with the right to privacy.