2014

Section 702 and the Collection of International Telephone and Internet Content

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

SECTION 702 AND THE COLLECTION OF INTERNATIONAL TELEPHONE AND INTERNET CONTENT

Laura K. Donohue*

* Professor of Law, Georgetown Law. Special thanks to William Banks, Orin Kerr, and David Kris for their comments on an earlier draft of this Article.

I. INTRODUCTION

On June 6, 2013, the *Washington Post* and *The Guardian* captured public attention with headlines claiming that the U.S. National Security Agency (NSA) was collecting large amounts of U.S. citizens' information.[1] The *Post* reported that the 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 it claimed came from the NSA, describing a program called "PRISM" (also known by its SIGAD, US-984XN).[3] The title 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 email, social network, and communications providers—making the type of information that could be obtained substantial: email, video and voice chat, videos, photos, stored data, VoIP, file transfers, video conferencing, notifications of target activity (e.g., 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 through 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 §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 PRISM and "upstream" collection of communications on fiber cables and infrastructure—i.e.,

---

[1] Barton Gellman and Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, Wash. Post, June 6, 2013; Glen Greenwald and Ewen MacAskill, NSA Prism Program Taps in to User Data of Apple, Google and Others, The Guardian, June 6, 2013, available at http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[2] Barton Gellman and Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, Wash. Post, June 6, 2013.

[3] PRISM/US-984XN Overview, April 2013, available at https://www.aclu.org/files/natsec/nsa/20130816/PRISM%20Overview%20Powerpoint%20Slides.pdf. 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 (such as connected to internet cables), sea-borne (such as intercept ships), or satellite intercept stations. SIGADs are use to identify SIGINT stations operated by the closely allied "Five-Eyes" (Australia, Canada, New Zealand, the United Kingdom, and the United States). According to documents published in June 2013 by the media as part of the Snowden document releases, as of March 2013 there were 504 active SIGADs. Glenn Greenwald and Ewen MacAskill, *Boundless Informant: the NSA's secret tool to track global surveillance data*, THE GUARDIAN, June 11, 2013, available at www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining. PRISM, in turn, is the name by which the program was known inside the NSA. Public remarks by Robert Litt, General Counsel Office of the Director of National Intelligence, Privacy and Civil Liberties Oversight Board, Hearings on §702, Washington, D.C., Mar. 19, 2014.

[4] *Id.*, slide 1.

[5] *Id.*, slide 2.

[6] *Id.*, slide 3.

[7] U.S. Foreign Intelligence Surveillance Court, Memorandum Opinion, Oct. 3, 2011, p. 29 https://www.aclu.org/files/assets/fisc_opinion_10.3.2011.pdf.

"[c]ollection directly from the servers of. . . U.S. Service Providers."[8] In contrast to PRISM, upstream collection allows the NSA to acquire Internet communications "as they transit the 'internet backbone' facilities."[9] The NSA could therefore potentially collect all traffic crossing particular Internet cables—not just information specifically targeted at particular Internet Protocol (IP) addresses or telephone number. This form of interception provides the intelligence community access to information that may be moving outside of the corporate partners employed in PRISM.[10] The slide urged analysts to use both methods to obtain information.[11] 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.[12]

Approximately two months after news of PRISM and upstream collection reached the public, the U.S. Director of National Intelligence, James Clapper, confirmed the existence of both collection programs, noting that PRISM had been in operation since Congress had passed the 2008 FISA Amendments Act.[13] Clapper declassified eight documents providing more details: two memorandum opinions issued by the Foreign Intelligence Surveillance Court, communication between the Administration and Congress on the existence and operation of the programs, and the §702 minimization procedures.[14] At the end of August 2013 Clapper announced that the intelligence community would release the total number of §702 orders issued, and targets thereby affected, on an annual basis.[15]

Although much of the information about PRISM remains classified, from what has been made public, via the press as well as declassification, suggests that the program pushes the statutory language to its limit, even as it raises critical Fourth Amendment concerns.[16] Almost no scholarship, however, has emerged since June

---

[8] James Ball, *NSA's Prism surveillance program: how it works and what it can do*, the Guardian, June 8, 2013, available at (including slide entitled FAA702 Operations,

[9] FISC Memorandum Opinion, Oct. 2011, at 26 (Bates, J.) Robert Litt, General Counsel of ODNI similarly explained, "Upstream collection refers to collection from the, for lack of a better phrase, Internet backbone rather than Internet service providers." Privacy and Civil Liberties Oversight Board, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the foreign Intelligence Surveillance Act, Washington, D.C., Mar. 19, 2014, remarks of Robert Litt, available at http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf.

[10] Public remarks by Raj De, National Security Agency General Counsel, Privacy and Civil Liberties Oversight Board, Hearing on §702, Washington, D.C., Mar. 19, 2014.

[11] *Id.*

[12] U.S. Foreign Intelligence Surveillance Court, Memorandum Opinion, Oct. 3, 2011, p. 30, https://www.aclu.org/files/assets/fisc_opinion_10.3.2011.pdf.

[13] Director of National Intelligence, *Press Release, DNI Declassifies Intelligence Community Documents Regarding Collection under Section 702 of the Foreign Intelligence Surveillance Act (FISA)*, Aug. 21, 2013 and DNI James Clapper's Cover Letter Announcing the document Release, Aug. 21, 2013, *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.

[14] *Id.*

[15] Director of National Intelligence, *Press Release, DNI Clapper Directs Annual Release of Information Related to Orders Issued Under National Security Authorities*, Aug. 29, 2013, *available at* http://icontherecord.tumblr.com/page/6.

[16] Some of the most important documents that have thus far been released in relation to this program include: 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 §702 of the Foreign Intelligence Surveillance Act of 1978, as amended, Jan. 8, 2007, available at http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document [hereinafter NSA Targeting Procedures]; Title VII, §702 of the Foreign Intelligence Surveillance Act (FISA) "Procedures for Targeting Certain Persons Outside the United States Other Than

2013 on the history of the legislative provisions and the questions that accompany the manner in which the intelligence community is interpreting and applying the statute—much less the profound Constitutional questions raised by the same.[17]

This Article begins by considering the origins of the current programs and the relevant authorities—particularly the shift of the content portions of the President's Surveillance Program, instituted just after 9/11, to the Foreign Intelligence Surveillance Act (FISA). It addresses the brief operation of the Protect America Act, before its replacement in 2008 by the FISA Amendments Act.

The Article then turns to statutory questions related to targeting, post-targeting analysis, and the retention and dissemination of information.

In the first statutory category, targeting, the Article argues that the NSA has sidestepped the statutory restrictions in three critical ways: by adopting procedures that allow analysts to acquire information not just to or from, but also "about" targets; by creating an assumption of non-U.S. person status; and by failing to construct procedures adequate to ascertain whether the target is located within domestic bounds. These interpretations undermine Congress' express inclusion of §§703 and 704 and open the door to the collection of U.S. persons' communications within domestic bounds. Looking beyond the statutory language, to the extent that the FAA is vague or ambiguous, different methods of interpretation raise concern. *Noscitur a sociis*, in this regard, offers little insight, but the doctrine of *ejusdem generis* suggests that the NSA's adherence to the to/from or about method goes beyond the authorities provided by Congress. Even if one rejects originalist interpretations as intellectually antediluvian, and assumes a more dynamic model, the recent passage of the statute places the NSA's interpretation on shaky ground.

FISC itself has confronted the problem of statutory language with regard to the FAA's prohibition of knowingly collecting entirely domestic communications. Although the NSA has stated to the Court that it does knowingly collect wholly domestic conversations, FISC has responded that because, in any one intercept, the NSA has not developed the technology to know the origins and destination of each packet intercepted, its actions are consistent with the FAA. This interpretation violates the plain language of the statute and calls into question how meaningful FISC's role is with regard to FAA targeting procedures.

In the second statutory category, post-targeting analysis, the Article draws attention to four areas, asking, first, whether the aim of the analysis conducted by the NSA elucidates (and generates further concern in relation to) the scope of information

---

United States Persons (50 USC §1881 a), available at https://www.fas.org/irp/news/2013/06/nsa-sect702.pdf. The July 2009 NSA Minimization Procedures (released by the Guardian in June 2013 and declassified/released by ODNI in November 2013), the June 2013 Fact Sheet on §702 (released in June 2013 by ODNI). Note that although the Administration has de-classified the Minimization Procedures, it has not, as of the time of writing, de-classified the Targeting Procedures.

[17] For thoughtful and 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); 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); Orin S. Kerr, *Updating the Foreign Intelligence Surveillance Act*, 75 U. CHI. L. REV. 225 (2010); 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 REV. 11 (2011). *See also* Jonathan D. Forgang, Student 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.

included at the collection phase. Second, it notes the failure of the NSA's prior minimization procedures to account for multi-communication transactions and raises question about the extent to which the statute adequately addresses situations in which the NSA collects information either in violation of FISC's direction or in a manner later found by FISC to be inconsistent with the statutory requirements. Third, the Article addresses the use of U.S. person information to query data, noting Congress's explicit prohibition of reverse targeting to prevent incursions into the use of §702 and asking whether then allowing such queries bypasses the statutory restrictions. Fourth, it looks at how what can be termed "recombinant" information changes the quality of information obtained under §702.

In regard to the third statutory category, the retention and dissemination of data, the Article notes that increasing consumer and industrial reliance on cryptography gives rise to questions about the NSA's automatic retention of encrypted data. This policy may soon become the exception that swallows the protections otherwise granted to U.S. persons' information. In addition, as a matter of statutory language (and not NSA implementation), the retention of all information under §702 implicating "foreign intelligence"—in light of the breadth of the statutory definition of the same—underscores the danger of looking to retention policies to delimit the type of information kept by the intelligence community. Finally, the use of the information obtained under §702 for criminal prosecution, while consistent with traditional FISA, fails to reflect the equivalent procedural protections at the collection stage.[18] This discussion leads naturally to Fourth Amendment considerations.

As a constitutional matter, outside of narrowly circumscribed exceptions (discussed, *infra*), a search in ordinary criminal law is presumptively unreasonable under the Fourth Amendment unless the government first obtains a warrant from a neutral, disinterested magistrate, based on a finding of probable cause of involvement in criminal activity. This applies to all searches within the United States. It does not apply to non-U.S. persons without a significant attachment to the country and who are outside domestic bounds. Between these book-ends is a considerably amount of grey area that takes account of questions such as whether the search centers on intelligence gathering or criminal prosecution, whether the target is a U.S. person or a non-U.S. person, where the search takes place, and the extent to which U.S. persons' privacy is implicated.

The Article briefly lays out this broader Fourth Amendment territory before turning to the government's argument that §702 collection takes place subject to a foreign intelligence exception to the warrant requirement. In the nearly four decades that have elapsed since the Court raised the possibility of such an exception—and in relation to which Congress responded by enacting FISA—not a single case has found a domestic foreign intelligence exception.

Pari passu, as a matter of the international intercept of U.S. persons' communications, practice and precedent prior to the FAA turned on a foreign intelligence exception to the warrant requirement that derived from the President's foreign affairs powers. Criminal investigations overseas similarly did not require warrants. (Nevertheless, the Courts required the search of U.S. persons overseas to be consistent with the Fourth Amendment requirement of reasonableness.) Through

[18] Minimization procedures published in June 2013 by the *Guardian*, dated from July 29, 2009, p. 2, §2, item (f), available at http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document. *See also* Government Fact Sheet on Section 702, June 2013, *available at* https://www.fas.org/irp/news/2013/06/nsa-sect702.pdf ("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.")

§§703 and 704 of the FAA, Congress has since introduced stronger safeguards for U.S. persons targeted for foreign intelligence purposes. By defaulting to §702, however, and "incidentally" collecting U.S. persons' international communications, the NSA is bypassing Congressional requirements. Acknowledging that the President and Congress share foreign affairs powers, the executive's persistent use of §702 may be regarded in Justice Jackson's third category under *Youngstown Sheet & Tube Co. v. Sawyer*.[19]

Even if one takes the position that the Warrant Clause is inapposite to collection of U.S. persons' information under §702, the FAA and NSA practice must still comport with the reasonableness requirements of the Fourth Amendment. To the extent that the target is a non-U.S. person based outside of domestic bounds, and the communications are to or from the target, the programs appear to be consistent with the constitutional mandate. But to the extent that the NSA interprets the statute to include information *about* such targets, in the process collecting the communications of wholly domestic communications, as well as conversations between U.S. persons, the practice fails to meet the totality of the circumstances test articulated by the Court with regard to reasonableness.

Although almost all of the public discussion of §702 has centered on the NSA's use of its authorities under the statute, almost no attention has been drawn to the role of the Central Intelligence Agency. The Article thus concludes by highlighting how little is currently known about the CIA's targeting, minimization, and retention and dissemination procedures—an omission which, in light of the significant statutory and constitutional questions accompanying the NSA's use of the same, and restrictions on CIA collection of information about U.S. persons within the United States, raises further concern.

II. CONTENT COLLECTION: SHIFT FROM ARTICLE II TO FISA

On October 4, 2001, President Bush authorized the National Security Agency (NSA) to collect two different types of bulk information: metadata and content.[20] The

[19] Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952).

[20] *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 GENERAL, NATIONAL SECURITY AGENCY CENTRAL SECURITY SERVICE, WORKING DRAFT ST-09-0002, Mar. 24, 2009, p. 1, 7-8, 11, 15, *available at* http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection [hereinafter WORKING DRAFT]. The Obama Administration has publicly confirmed the inclusion of Internet and telephony metadata, and telephony content, as part of the President's Surveillance Program (PSP), 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), *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 [hereinafter Declassification Press Release]; 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), *available at* https://www.eff.org/files/2013/12/21/fleisch2013jewelshubert.pdf (using language identical to DNI press release)[hereinafter Fleisch Declaration]. *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*

former gave the NSA the ability to identify terrorist-related activity through contact chaining—i.e., the process of building a network graph that modeled communication patterns of targets and their associates.[21] The latter provided raw intelligence.[22] The NSA focused on telephony and Internet sources for each kind of information, with four resultant categories: (1) telephony metadata, (2) Internet metadata, (3) telephony content, and (4) Internet content.[23]

The Administration initially based the President's authority to conduct the President's Surveillance Program (PSP) on three legal theories: the President's inherent authorities as Commander-in-Chief, the 2001 Authorization for the Use of Military Force, and the War Powers Resolution.[24] In March 2004, a classified review of the program by the Office of Legal Counsel determined that there was legal support for three of the four types of collection included in PSP [(1) bulk telephony metadata, and the contents of (3) telephone and (4) Internet communications]. OLC found that category (2), bulk Internet metadata collection, however, appeared to be prohibited by the terms of FISA and Title III.[25] The President thus rescinded the authority to collect bulk Internet metadata and gave the NSA one week to terminate the program.[26] DOJ and NSA subsequently transferred the process to FISA's Pen Register/Trap and Trace Provisions (PRTT), with the first order approved July 14, 2007 and renewed thereafter at 90-day intervals.[27] (This program operated until December 2011, when it was discontinued for failure to deliver sufficient operational value to the NSA.[28])

Although known to a small number of people within the executive branch, it was not until a *New York Times* article was published on December 16, 2005 that PSP reached the media.[29] As public concern increased, the Attorney General sent a five-

---

https://www.aclu.org/sites/default/files/pdfs/safefree/aclu_v_doj_2nd_declaration_steven_bradbury.pdf. Note that for purposes of this paper, I cite to the Working Draft of the NSA IG 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 time, and so I proceed, in part, on the assumption that the report is accurate, with the appropriate cautions in place.

[21] WORKING DRAFT, *supra* note 1, at 13.

[22] *Id.* at 15.

[23] Within a month, the President's Surveillance Program (PSP), renewed thereafter at 30-60 day intervals, became operational. WORKING DRAFT, *supra* note 1, at 11 ("Within 30 days, the PSP was fully operational . . . Private sector partners began to send telephony and Internet content to NSA in October 2001. They began to send telephony and Internet metadata to NSA as early as November 2001").

[24] *See, e.g.*, President's Radio Address, THE WHITE HOUSE, Dec. 17, 2005, *available at* http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051217.html; U.S. DEP'T OF JUSTICE, *LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT* (Jan. 19, 2006), *available at* http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf; Letter from William E. Moschella, Assistant Attorney General to The Hon. Pat Roberts, Chair, Senate Select Committee on Intelligence, The Hon. John D. Rockefeller, IV, Vice Chairman, Senate Select Committee on Intelligence, The Hon. Peter Hoekstra, Chairman, Permanent Select Committee on Intelligence, U.S. House of Representatives, and the Hon. Jane Harman, Ranking Minority Member, Permanent Select Committee on Intelligence, U.S. House of Representatives (Dec. 22, 2005), *available at* https://www.fas.org/irp/agency/doj/fisa/doj122205.pdf.

[25] OLC apparently issued three opinions on this matter: Mar. 15, 2004, May 6, 2004, and July 16, 2004. WORKING DRAFT, *supra* note 1, at 37.

[26] WORKING DRAFT, *supra* note 1, at 38.

[27] WORKING DRAFT, *supra* note 1, at 38, 39; Declassification Press Release, *supra* note 1; Fleisch Declaration, *supra* note 1.

[28] *See* Declassification Press Release, *supra* note 1; Fleisch Declaration, *supra* note 1.

[29] James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers without Courts*, N.Y. TIMES, Dec. 16, 2005, http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&_r=0 ("Months after the Sept. 11 attacks, President Bush secretly authorized the National Security Agency to eavesdrop

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.[30] At that time, only a narrow part of the program's contours became public: the NSA's interception of (some) telephone content between the United States and overseas.[31] 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.[32] Pressed for the legal rationale behind what became known as the Terrorism Surveillance Program (TSP), the Bush Administration cited the three legal theories: i.e., Article II, the 2001 AUMF, and the WPR.[33]

Following the appearance of information in the public domain and in the face of mounting pressure within and outside the government, the legal basis for the component parts of PSP gradually altered.[34] On May 24, 2006, the NSA transferred the bulk collection of telephony metadata to FISA's §501 tangible goods provisions (as amended by USA PATRIOT Act §215).[35] Then in July 2007 the NSA transferred

---

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 and 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 ("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.").

[30] *Administration Defends NSA Eavesdropping to Congress*, CNN.COM, Dec. 23, 2005, http://www.cnn.com/2005/POLITICS/12/23/justice.nsa/index.html. The leter was sent to Senators Pat Roberts (R-KS) and John Rockefeller (D-WV), as well as Representaties Peter Hoedstra (R-MI) and Jane Harman (D-CA).

[31] Lichtblau and Risen, *Spy Agency Mined Vast Data Trove*, *supra* note 10.

[32] *Administration Defends NSA Eavesdropping to Congress*, CNN.COM, Dec. 23, 2005, http://www.cnn.com/2005/POLITICS/12/23/justice.nsa/index.html.

[33] *See, e.g.*, President's Radio Address, THE WHITE HOUSE, Dec. 17, 2005, *available at* http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051217.html; U.S. DEP'T OF JUSTICE, *LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT* (Jan. 19, 2006), *available at* http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf; Letter from William E. Moschella, Assistant Attorney General to The Hon. Pat Roberts, Chair, Senate Select Committee on Intelligence, The Hon. John D. Rockefeller, IV, Vice Chairman, Senate Select Committee on Intelligence, The Hon. Peter Hoekstra, Chairman, Permanent Select Committee on Intelligence, U.S. House of Representatives, and the Hon. Jane Harman, Ranking Minority Member, Permanent Select Committee on Intelligence, U.S. House of Representatives (Dec. 22, 2005), *available at* https://www.fas.org/irp/agency/doj/fisa/doj122205.pdf.

[34] *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, available at http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm; Seymour M. Hersh, Listening In, New Yorker, May 29, 2006, available at http://www.newyorker.com/archiva/2006/05/29/060529ta_talk_hersh. 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 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

[35] USA PATRIOT Act, Sec.215, amending FISA Sec. 501, codified at 50 USC §1861 (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 (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

the Internet metadata program to FISA's Pen Register/Trap and Trace authorities.[36] It operated until December 2011, when it was discontinued for failure to deliver sufficient operational value to the NSA.[37]

The remaining PSP collection programs, 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.[38] The initial solution came in a re-definition of the language of FISA, subsequently, via statutory changes, and, finally, through broad understanding of the new provisions.

A. Re-definition of "Facility" under FISA

DOJ's immediate solution to finding a statutory basis for the content portion of PSP appears to have turned on a new definition of "facility" as that term was employed in FISA. From being understood narrowly in its traditional sense, i.e., 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

---

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 (Sept. 5, 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.

[36] In March 2004, a classified review of the program by the Office of Legal Counsel appears to have determined that legal support existed for three of the four types of collection included in PSP: (a) bulk telephony metadata, and the contents of (b) telephone and (c) Internet communications. Bulk Internet metadata collection, however, appeared to be prohibited by the terms of FISA and Title III. OLC apparently issued three opinions on this matter: Mar. 15, 2004, May 6, 2004, and July 16, 2004. WORKING DRAFT, *supra* note 1, at 37. The President rescinded the authority to collect bulk Internet metadata and gave the NSA one week to terminate the program. DOJ and NSA subsequently transferred the process to FISA's Pen Register/Trap and Trace Provisions (PRTT), with the first order approved July 14, 2007 and renewed thereafter at 90-day intervals. WORKING DRAFT, *supra* note 1, at 38, 39; Declassification Press Release, *supra* note 1; Fleisch Declaration, *supra* note 1.

[37] *See* Declassification Press Release, *supra* note 1; Fleisch Declaration, *supra* note 1. For detailed discussion of the legality and constitutionality of the §215 program and, by analogy, the transfer of Internet Metadata to PRTT, *see* Laura K. Donohue, *Bulk Metadata Collection*, Harv. J. L. Pub. Pol'y (2014).

[38] WORKING DRAFT, *supra* note 1, at 40.

information subject to acquisition by each device.[39]

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 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.[40]

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.[41] Congress explained the rationale behind adding the new language:

> The multipoint wiretap amendment to FISA in the USA PATRIOT Act (§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.[42]

---

[39] 50 USC §1805(c). [emphasis, in bold, added; underscore reflects changes made with the USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. 109-177, Mar. 9, 2006, §108, codified at 50 USC §1805(c)(3)].

[40] 50 USC §1805(c)(2)(B) [emphasis, in bold, added; underscore reflects changes made with the USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. 109-177, Mar. 9, 2006, §108, codified at 50 USC §1805(c)(3)].

[41] Intelligence Authorization Act for FY 2002, P.L. 107-108 (Dec. 28, 2001); USA PATRIOT Act of 2001, P.L. 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, Feb. 15, 2007, p. 24, available at http://www.fas.org/sgp/crs/intel/RL30465.pdf.

[42] Conference Report on H.R. 2338, the Intelligence Authorization Act for Fiscal Year 2002 (which became P.L. 107-108), H.Rept. 107-328, at 24. (Continuing, "Currently, FISA requires the court to "specify" the "nature and location of each of the facilities or places at which the electronic surveillance will be directed." 50 U.S.C. § 105(c)(1)(B). Obviously, in certain situations under current law, such a specification is limited. For example, a wireless phone has no fixed location and

The aim was to ensure that where a *particular* target (i.e., a foreign power or an agent thereof) 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.[43]

In 2005 Congress underscored the specificity for the facilities or places to be placed under surveillance, in relation to particular targets, 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.[44]

This language underscored the importance of the Executive Branch being able to articulate which, specific 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 specificity about the target and the facility itself. Facility was thus narrowly understood 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 PSP to a more secure legal footing,

---

electronic mail may be accessed from any number of locations. To avoid any ambiguity and clarify Congress' intent, the conferees agreed to a provision which adds the phrase, "if known," to the end of 50 U.S.C. § 1805(c)(1)(B). The "if known" language, which follows the model of 50 U.S.C. § 1805(c)(1)(A), is designed to avoid any uncertainty about the kind of specification required in a multipoint wiretap case, where the facility to be monitored is typically not known in advance.")

[43] *See also* 147 Cong. Rec. S10990-02 (statement of Senator Feinstein); Edward C. Liu, Amendments to the Foreign Intelligence Surveillance Act Extended Until June 1, 2015, CRS, R40138, June 16, 2011, available at http://www.fas.org/sgp/crs/intel/R40138.pdf.

[44] USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. 109-177, Mar. 9, 2006, §108, codified at 50 USC §1805(c)(3). [emphasis, in bold, added; underscore reflects changes made with the USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. 109-177, Mar. 9, 2006, §108, codified at 50 USC §1805(c)(3)].

from mid-2005 to January 2007, DOJ worked with NSA to re-define "facility."[45] The purpose, as aforementioned, was to shift PSP from an Article II basis to the FISA framework. Thus, instead of understanding facility in the traditional sense, (i.e., as a specific telephone number or email address), DOJ argued that it should be understood as a "general gateway" or "cable head."[46]

This change significantly expanded the amount of information that could be obtained by the government under FISA. The Internet essentially 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.

Re-defining "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 of "facility" 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."[47] On January 10, 2007, FISC signed two separate orders: the Foreign Content Order and the Domestic Content Order.[48] One week later, Attorney General Alberto Gonzales wrote to the Senate Judiciary Committee, indicating that a FISC judge had issued orders moving TSP to FISA.[49] According to

---

[45] *See* Working Draft *supra* note 1, 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 ("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.")

[46] WORKING DRAFT, *supra* note 1, 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.")

[47] WORKING DRAFT, *supra* note 1, at 41-42.

[48] Foreign Content Order, Jan. 10, 2007 and Domestic Content Order, Jan. 10, 2007, *cited in* WORKING DRAFT, *supra* note 1, at 41-42. For additional sources noting the ending of PSP in January 2007 *see also* S. REP. NO. 110-209, at 4 (2007); *See also* Letter from Attorney General Alberto Gonzales to Senate Judiciary Committee Chairman Patrick Leahy and Senator Arlen Specter (Jan. 17, 2007). Other documents, however, suggest that TSP transitioned to FISA in January 2007. *See, e.g.*, Declassification Press Release, *supra* note 1; Fleisch Declaration, *supra* note 1.

[49] 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.

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."[50]

The re-definition of "facility" and movement of PSP to the FISA framework met with mixed results. According to the NSA Inspector General, the domestic content order did not have an immediate or significant impact on collection.[51] The foreign content order, however, immediately and negatively affected the number of foreign selectors that could be used with regard to collection.[52] Each time the government wanted to include a new target, it was forced to return to FISC for an order. This, and the requirements that accompanied the resulting orders, placed a higher administrative burden on the NSA than the agency had been subject to under PSP.[53] 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.

B. 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.[54] 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.

The statute removed the Foreign Intelligence Surveillance Court (FISC) from supervising the interception of communications that began or ended in a foreign country. 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;

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 (2007), overturning ACLU v. NSA, 438 F.Supp.2d 754.

[50] *Id.*

[51] WORKING DRAFT, *supra* note 1, 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 significant attention has been paid post-June 2013 to §702, significantly less focus has been drawn to the domestic order.

[52] WORKING DRAFT, *supra* note 1, at 42.

[53] *See also* William C. Banks, *Responses to the Ten Questions: 9. Is the FISA Amendments Act of 2008 good policy? Is it constitutional?* WILLIAM MITCHELL L. REV., (2009), at 5012("[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.")

[54] Protect America Act of 2007, Pub. L. 110-55, § 2, 121 Stat. 553. (Aug. 5, 2007) (amending FISA, § 105B(a)(1)-(5)), codified at 50 U.S.C. § 1805b (2006)).

2. The acquisition did not constitute electronic surveillance (*i.e.,* 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. [55]

It therefore became easier to establish that the target of the intercepts was located outside the United States: no individualized showing was required. Instead, simply 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 solely on geography—not on whether the target was a foreign power, or an agent of a foreign power, as was previously required by 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.[56] Once certified, FISC was required to grant the order.[57] The statute gave retroactive immunity to service providers for their role in PSP, insulating them from civil liability.[58]

Efforts by a telecommunications company to challenge the PAA in the Foreign Intelligence Surveillance Court, on Fourth Amendment grounds, later failed.[59] FISC held that while the service provider had standing to challenge the directives, the PAA, as applied, satisfied the Fourth Amendment's reasonableness requirement.[60] Intended to operate for six months, the PAA expired in February 2008 when the executive and legislative branches reached an impasse over whether broad, retroactive immunity should be extended to businesses implicated in TSP.[61]

C. The FISA Amendments Act

After months of deadlock, Congress finally conceded on providing the telecommunications companies with blanket, retroactive immunity.[62] In July 2008 the legislature enacted a more permanent measure: the FISA Amendments Act (FAA).[63] Codified as Title VII of FISA, the legislation simultaneously strengthened and

---

[55] *Id*.

[56] Protect America Act of 2007, Pub. L. 110-55, § 3, 121 Stat. 552 (Aug. 5, 2007) (amending FISA § 105B(c), codified at 50 U.S.C. § 1805c (2006).

[57] Protect America Act of 2007, Pub. L. 110-55, § 3, 121 Stat. 552 (Aug. 5, 2007) (amending FISA § 105C). Twice a year the Attorney General would be required to inform the Intelligence and Judiciary Committees of the House and Senate of incidents or noncompliance with the directive issued by the Attorney General or Director of National Intelligence, incidents of noncompliance with FISC-approved procedures, and the numbers of certifications or directives issued during the reporting period. *Id.*

[58] Protect America Act of 2007, §6.

[59] In re Directives Pursuant to §105b of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1009-1016 (U.S. Foreign Intell. Surveil Ct. Rev. 2008).

[60] *Id.*

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

[62] 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 (2011; In re National Security Agency Telecommunications Records Litigation, 633 F.Supp.2d 949, denied reconsideration, 2009 WL 2171061.

[63] FISA Amendments Act of 2008, Pub. L. 110-261, 122 Stat. 2436 (July 10, 2008).

weakened protections for U.S. persons' international communications. A brief discussion of the statutory provisions helps to establish a basis for subsequent analysis of PRISM and upstream collection.

1. Section 702

Consistent with the PAA, FISA §702 empowers the Attorney General and the Director of National Intelligence jointly to authorize, for up to one year, "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[64] A number of limitations apply.

First, any such acquisition "may not intentionally target any person known at the time of acquisition to be located in the United States."[65] Second, such acquisition may not intentionally target an individual reasonably believed to be located outside the United States where the actual purpose of the acquisition is "to target a particular, known person reasonably believed to be in the United States."[66] Third, the acquisition may not intentionally target a U.S. person reasonably believed to be outside domestic bounds.[67] Fourth, the acquisition may not intentionally obtain domestic communications.[68] And fifth, such acquisition must be conducted consistent with the Fourth Amendment.[69]

Procedurally, three steps must be followed for acquisition to commence: it must be consistent with (a) targeting and (b) minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence and subject to review by the Foreign Intelligence Court; and it must be (c) certified by FISC.[70] The statute also requires that the targeting and minimization procedures be made available to the Congressional intelligence committees, as well as the Committees on the Judiciary of the Senate and the House of Representatives.[71]

FISC is limited in the role it can play with regard to reviewing the certification, as well as the targeting and minimization procedures.[72] 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, and minimization procedures are statutorily consistent, "the Court **shall** enter an order approving the certification and the use, or continued use. . ." of an acquisition.[73]

The head of each element of the intelligence community conducting an acquisition under §702 must annually review 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.[74] This review must then be provided to FISC, the Attorney

---

[64] "Procedures for Targeting Certain Persons Outside the United States Other Than United States Persons," Foreign Intelligence Surveillance Act, Pub. L. 110-261, § 702, 122 Stat. 2436, codified at 50 U.S.C. § 1881(a) (2006). 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 USC §1881(b)(1).
[66] 50 USC §1881 (b)(2).
[67] 50 USC §1881(b)(3).
[68] 50 USC §1881(b)(4).
[69] 50 USC §1881(b)(5).
[70] 50 USC §1881(c)-(e), (g).
[71] 50 USC §1881(f).
[72] *See* discussion, *infra*.
[73] 50 USC §1881(i)(3)(A) (emphasis added).
[74] 50 USC §1881(l)(3)(A)-(B).

General, the DNI, the Congressional intelligence Committees, and the Committees on the Judiciary of the House of Representatives and the Senate.[75]

The FAA created an opportunity for telecommunications companies served with orders to challenge the request for information.[76] FISC may only grant such petition where the request for information is unlawful.[77] Otherwise, the electronic communication service provider served with an order must provide the information or risk being held in contempt of court.[78] Either the government or the service provider may appeal to the Foreign Intelligence Surveillance Court of Review, with final review by the Supreme Court.[79]

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 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 U.S. persons overseas had been conducted under the auspices of Executive Order 12333.[80]

As a threshold matter, §704 prevents the intelligence community from targeting a U.S. person who is reasonably believed to be abroad unless authorized to do so by FISC or another provision in FISA.[81] The limit only applies where the target has a reasonable expectation of privacy and, if the activity were conducted within the United States for law enforcement purposes, a warrant would be required.[82]

Section 704 therefore appears to cover both physical searches as well as electronic intercepts. In U.S. jurisprudence, whether a "reasonable expectation of privacy" exists turns on both a subjective and an objective analysis: namely, whether an "individual manifested a subjective expectation of privacy in [a] searched object" and whether "society is willing to recognize that expectation as reasonable."[83] Accordingly, a report of the Congressional Research Service, subjecting international intercepts to this test explains, "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.'"[84]

As a practical matter, what this threshold consideration means is that where the NSA *knows* that a U.S. person is located overseas, *and that person is the target of the intercept* (an important provisio), in many foreign intelligence acquisitions, it must use FISA.

The legislation lays out the procedures under which FISC must then operate. The steps outlined in §703 only apply to electronic surveillance, or the acquisition of stored electronic communications or data, that would traditionally require an order

---

[75] 50 USC §1881(l)(3)(C).
[76] 50 USC §1881(h)(4)(A)("An electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition to modify or set aside such directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.")
[77] 50 USC §1881(h)(4)(C).
[78] 50 USC §1881(h)(4)(G).
[79] 50 USC §1881(h)(6).
[80] Exec. Order 12333, 46 FR 59941, 3 CFR, 1981 Comp., p. 200, §2.3, Dec. 4, 1981.
[81] 50 USC §1881c(a)(2).
[82] 50 USC §1881c(a)(2).
[83] Kyllo v. United States, 533 U.S. 27, 33 (2001)(citing California v. Ciraolo, 476 U.S. 207, 211 (1986)).
[84] Edward C. Liu, Reauthorization of the FISA Amendments Act, CRS Report R42725, Apr. 8, 2013.

under FISA. For all other situations, §704, whose standards are weaker than those of §703, applies.

The procedures to be followed generally reflect the structure employed by traditional FISA with regard to electronic surveillance and physical search. Namely, 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.[85] In addition, the Court must ascertain that there is probable cause to believe that the target is located outside the United States.[86]

The central difference between §§703 and 704 is that less specificity is required under the latter. The government need not assert that the information to be obtained cannot be garnered via normal investigative means. It also only requires minimization procedures with regard to the dissemination of acquired information[87]—as opposed to §703, which requires minimization procedures to be applied both with regard to acquisition and retention.

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, §§703 and 704 have no such equivalent.[88] In a further a departure from traditional FISA, which requires that U.S. persons to be targeted be linked either to international terrorism or clandestine intelligence activities, under §§703 and 704, neither linkage is required prior to targeting and acquisition.[89] Only the government is authorized to appeal the determination of FISC either to FISC-R or to the Supreme Court.[90]

III. PRISM AND UPSTREAM COLLECTION

Almost immediately after passage of the FAA, members of Congress, scholars, and others began criticizing §702, because of the potential for the government to use the authorities to engage in broad, "programmatic surveillance", implicating U.S. persons' right to privacy.[91] In voting against the legislation, Senator Russell Feingold explained,

> I sit on the Intelligence and Judiciary Committees, and I am one of the few members of this body who has been fully briefed on the warrantless wiretapping program. And, based on what I know, I can promise that if more information is declassified about the program in the future, as is likely to happen either due to the Inspector General report, the election of a new President, or simply the passage of time, members of this body will regret that we passed this legislation.[92]

---

[85] 50 USC §§1881b(b)-(c), §1881c(b)-(c). Note too that 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 USC §1881b(d), 1881c(d).
[86] *Id.*
[87] 50 USC §1881c(c)(1)(C).
[88] Compare 50 USC §1801 to Title VII.
[89] Compare 50 USC §1801(b) to Title VII.
[90] 50 USC §1881(f).
[91] *See, e.g.,* Banks (2009), *supra* note 53; William C. Banks, *Programmatic Surveillance and FISA: of Needles in Haystacks*, 88 Tex. L. Rev. 1633 (2009-2010); Forgang, *supra* note 17.
[92] Senator Russell Feingold, Remarks of U.S. Senator Russell Feingold in Opposition to the FISA Amendments Act (July 9, 2008), http://feingold.senate.gov/~faingold/statements/08/07/20080709.htm.

By removing probable cause that the target be a foreign power or an agent of a foreign power, and that the target be using particular facilities, and instead only loosely basing authorization on the geographic location of the target—even as it removed the Foreign Intelligence Surveillance Court from the process—the legislation opened the door to collecting significantly more citizens' communications. In 2009 prominent national security law Professor William Banks explained,

> [T]he FAA does not limit the Government to surveillance of particular, known persons reasonably believed to be outside the United States, but instead permits so-called "vacuum cleaner" surveillance and data mining. . . . [T]he 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. Surveillance might be directed at a terrorist organization, a telephone number or email address, or perhaps at an entire ISP or area code. . . [T]he surveillance permitted under the FAA does not require that the Government identify a particular known facility where the intercepted communications occur."[93]

Banks highlighted the concerns that attended programmatic surveillance, noting that the new language and the types of activities that it covered represented a sea change from how FISA had previously worked.[94] He 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. Nor do the minimization rules require the Government to discard communications of U.S. persons incidentally collected when the Government is targeting someone abroad. NSA may decide to retain any communications that constitute foreign intelligence...[95]

For Banks, part of the problem was that the nature of international information flows meant that it would be impossible to tell if an individual is located overseas or within

---

[93] Banks (2009), *supra* note 53, at 5013 - 5014.

[94] Banks (2009), *supra* note 53, at 5014 ("A few attributes of the programmatic surveillance authorized by the FAA mark stark changes in FISA. First, some of the intercepted communications will be to or from American citizens (only intentional targeting of Americans is prohibited), and the surveillance producing the intercepts will not have been reviewed under pre-existing FISA requirements that the target be an agent of a foreign power or a lone wolf terrorist. Even the TSP targeted communications only where one party was outside the United States and there was probable cause to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated organization. The FAA eliminates any showing of individualized suspicion, even where communications of American citizens are the foreseeable consequence of the program orders. ")

[95] Banks (2009), *supra* note 53, at 5014-5015.

domestic bounds.[96] 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.[97] Higher protections for personally-identifiable information, and its dissemination, and FISC review of the programs for First and Fourth Amendment implications proved equally important.[98] Other commentators similarly called for reform.[99]

Cases began to arise in the courts, challenging, on constitutional grounds, the language and the programs implemented under the statute. In *Clapper v. Amnesty International*, for instance, plaintiffs alleged that §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.[100] The Supreme Court ultimately dismissed the suit for failure to demonstrate standing—i.e., the existence of any concrete injury. It did not reach the merits of the Fourth Amendment claim.

Controversy about §702 and the lack of public discourse about how the provision was being used continued. A key consideration was NSA's inability to provide the number of how many U.S. citizens' communications had been intercepted under the statute's auspices. In 2012, for instance, Senators Ron Wyden and Mark Udall raised concerns about what they referred to as a "back door" in the statute.[101] In June 2012 the Senate Select Committee on Intelligence similarly noted numerous Senators' concern about the IC's inability to provide an estimate of the number of individuals whose communications had been intercepted.[102] Focus was drawn to the length of the extension, as well as that lack of information as to whether the NSA had attempted to search specific Americans' communications under the FAA without a warrant.[103] By the end of July 2012, more than a dozen senators 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 States whose communications may have been reviewed' under the FAA.'"[104]

---

[96] Banks (2009), *supra* note 53, at 5015.
[97] Banks (2009-2010), *supra* note 91, at 1637.
[98] Banks (2009-2010), *supra* note 91, at 1637.
[99] *See, e.g.,* citations listed in footnote 17, *supra*.
[100] Clapper v. Amnesty Int'l, 133 S.Ct. 1138 (2013).
[101] On May 4 Senators Wyden and Udall wrote a letter to the Inspector General (IG) of the National Security Agency 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 the Hon. Ron Wyden and the Hon. Mark Udall, to IG of the Intelligence community, May 4, 2012. 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 Comu8nity, to Senators Wyden and Udall, Washington, DC, June 15, 2012, available at http://www.wired.com/images_blogs/dangerroom/2012/06/IC-IG-Letter.pdf.
[102] FAA Sunsets Extension Act of 2012, SSCI Report together with Additional and Minority Views to accompany S. 3276, June 7, 2012, 112-174, Calendar No. 424, available at https://www.fas.org/irp/congress/2012_rpt/faa-extend.html.
[103] Udall Calls on Intelligence Director to Provide Answers before Senate Debate on FISA Amendments Act, July 26, 2012, available at http://www.markudall.senate.gov/?p=press_release&id=2586.
[104] Letter from 13 Senators to James R. Clapper, July 26, 2012, available at http://www.wyden.senate.gov/download/letter-to-dni. *But see* FAA Sunsets Extension Act of 2012, SSCI Report together with Additional and Minority Views to accompany S. 3276, June 7, 2012, 112-174,

Despite these concerns, two efforts to amend the legislation failed.[105] In December 2012 President Obama extended the FAA until 2017.[106] Six months later, the Snowden documents again forced §702 into the public discussion. The information that has since emerged raises serious statutory and constitutional concerns with regard to three areas: targeting, post-targeting analysis, and the use and dissemination of information.

A. Targeting

As aforementioned, §702 places four key limitations on acquisitions, all of which relate to targeting and each of which is meant to restrict the amount of information that can be obtained by the government. The government may not (a) target individuals known to be in the United States, (b) engage in reverse targeting (i.e., 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.[107] In addition, the statute requires that all acquisition be conducted in a manner consistent with the Fourth Amendment.[108]

The NSA has sidestepped the statutory restrictions related to targeting in three important ways: first, it has adopted procedures that allow analysts to acquire information "about" selectors (i.e., 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: i.e., if an individual is not *known* to be a U.S. person (and thus exempted from §702 and treated either under §§703 and 704 or under traditional FISA, depending on the location), then the NSA assumes that the individual is a non-U.S. person. Thus, despite the statutory restrictions that only non-U.S. persons be targeted under §702, the NSA is not bound by its procedures to a minimum due diligence level to ascertain the status of the target.

Third, the NSA has failed to adopt minimum standards that would require it to ascertain whether a target is located within domestic bounds. Instead, the agency assumes that the target is located internationally, absent evidence to the contrary.

These interpretations of the law work together to undermine Congress' addition of §§703 and 704, even as they open the door to more extensive collection of U.S. persons' communications within domestic bounds. They thus run contrary to the plain

---

Calendar No. 424, available at https://www.fas.org/irp/congress/2012_rpt/faa-extend.html (Senator Feinstein writing, "During the Committee's consideration of this legislation, several Senators expressed a desire to quantify the extent of incidental collection under §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 §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.")

[105] Jeff Merkeley of Oregon proposed an amendment that would have required FISC to disclose "important rulings of law." (Failed 37-54). Ron Wyden proposed an amendment that would have required the government to estimate the number of US citizens whose communications had been intercepted. Failed 43-52.

[106] Foreign Intelligence Surveillance Act Amendments Act Reauthorization Act of 2012, H.R. 5949, signed Dec. 30, 2012. Absent intervening legislation, Title VII will automatically sunset.

[107] 50 USC §1881(b).

[108] *Id.*

language of the statute. To the extent that they stem from ambiguity in the statute itself, the doctrine of *ejusdem generis* suggests that adherence to these interpretations takes the NSA outside statutory constraints. The case to move beyond originalist and textualist interpretations, to a more dynamic model—but five years after the statute's passage—to conclude otherwise, is weak.

In 2011 FISC realized the implications of the NSA's interpretation of to/from or "about." However, in light of the aim of the intelligence agencies, and the limitations imposed by the types of technologies being used (making it impossible to distinguish information at the point of interception), the Court read the statute in a manner that found the targeting procedures to be consistent with the statutory requirements. The Court's analysis violated one of the basic canon's of statutory construction—one rooted in the plain language of the statute—and raised the question of how meaningful FISC's role is with regard to §702.

1. Information To/From and About Targets

The FAA focuses on acquisitions with reference to the nature of the target itself. It is silent on whether only information held by the target, or communications to which the target is a party, may be obtained.

In the absence of explicit statutory language, the NSA has interpreted §702 to enable the agency also to obtain information about targets. The NSA's 2009 targeting procedures thus state that the NSA may seek "to acquire communications about the target that are not to or from the target."[109] The 2009 minimization procedures similarly acknowledge the acquisition of information related to persons or entities of interest.[110] 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."[111] The 2011 minimization procedures retain this focus.[112]

In scanning Internet traffic, the NSA uses IP filters to verify that the person from whom foreign intelligence information is being obtained is located overseas, or else it targets Internet links that terminate in a foreign country.[113] In this way, any international communication may be obtained, as long as it either originates or terminates outside the United States. Both methods ensure that acquisition is *directed*

---

[109] NSA Targeting Procedures, p. 1. The Targeting Procedures were published by The Guardian in June 2013. They have not, as of the time of writing, been declassified.

[110] The 2009 Minimization procedures were published by *The Guardian* in June 2013. They have not, as of the time of writing, been declassified.

[111] July 2009 Minimization Procedures, §3(b)(4), p. 3, available at http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document (emphasis added). *But see NSA Director of Civil Liberties and Privacy Office Report: NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*, Apr. 16, 2014, *available at* http://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf (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 email addresses or telephone numbers).

[112] *See, e.g.,* regarding segregated upstream collection information: 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)("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."); §3(b)(5)(b) ("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") [Document declassified by the DNI August 2013]

[113] *Id.*

at communications outside the US.[114] So, if a U.S. person is located within domestic bounds, and communicating with a person overseas, the NSA can intercept and scan the communication for links to a third party target.

One notable characteristic of the NSA's statutory interpretation is that, if the purpose of upstream collection is to ensure that information about targets is obtained (in the course of which further analysis of the information may commence), because of how the Internet is constructed, the NSA would have to collect significant amounts of data and then search the content for further reference to the selector or target in question.[115] In other words, if the NSA may collect not just email to or from the target's email account (e.g., badguy@ISP.com), but, in addition, other communications happening to mention badguy@ISP.com that pass through the collection point, then the NSA would have to be scanning all emails transiting the upstream collection point to filter out those of interest.[116]

The structure of the Internet is of note. Everything one does online involves packets of information. Every Web site, every email, 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.[117] Packet switched networks then 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. It may include routing even domestic messages through international servers, if that is the most efficient route to the final destination.

As a result, because of the NSA's TFA interpretation, not only will a significant amount of information be monitored via upstream collection, but such intercepts will inevitably include the interception of communications wholly domestic in nature. The potential insight generated in relation to domestic, international, and indeed, global communications, is remarkable. According to James Bamford, upstream interception on just domestic cables implicates "about 80% of the world's telecommunications."[118] And reports in foreign newspapers suggest that the program is not limited to domestic bounds.[119] FISC similarly raised concern about the amount and type of information

---

[114] NSA Targeting Procedures, pp. 1-2.

[115] *See also* Charlie Savage, *NSA Said to Search Content of Messages to and From U.S.*, New York Times, Aug. 8, 2013, available at http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?ref=todayspaper&pagewanted=all&_r=0 (discussing to/from or about collection and noting, "[T]o conduct the surveillance, the NSA 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.")

[116] *See* David Kris, 17:5 insert, cleared Feb. 25, 2014 (Illustrating to/from or about collection: "In other words, the government may collect at the upstream sites not only email to and from the target's email account, e.g., badguy@ISP.com, buy also other email (regardless of sender and recipient) that passes through the upstream collection points if it mentions badguy@ISP.com (and otherwise satisfies the legal requirements.")

[117] The data is contained in the Transmission Control Protocol/Internet Protocol (TCP/IP) used by the Internet. *What is a Packet?, How Stuff Works*, available at http://computer.howstuffworks.com/question525.htm.

[118] *Id. See also* JAMES BAMFORD, THE SHADOW FACTORY: THE NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA (2009).

[119] *See, e.g.,* Glenn Greenwald, Roberto Kaz E José Casado, *EUA espionaram milhões de e-mails e ligações de brasileiros*, O GLOBO, July 12, 2013, available at http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934; Laura Poitras, Marce Rosenbach, Fidelius Schmid, Holder Stark and Jonathan Stock, *How the NSA Targets Germany and Europe*, DER

obtained through TFA collection. Instead of finding statutory violation, however, the Court was driven to a Constitutional analysis. I return to this point, below.

The theory behind TFA is that "the user of the tasked facility was the 'target' of the acquisition, because the government's purpose is in acquiring such communications to obtain information about the user." [120] Parties to the communications only become targets once they are identified and verified through the targeting procedures.[121] The legal argument stems from the shift in interpretation of "facility" that occurred with the PAA. Namely, once the backbone facility becomes the target, then any data transiting that facility becomes fair game.

2. Burden of Proof Regarding "U.S. Person" Status

A second statutory interpretation that has allowed the NSA to push the statutory limits is the assumption that individuals not actually *known* to be U.S. persons are *assumed* to be non-U.S. persons, with no threshold burden of proof that must be met in order to ascertain whether the target is a non-U.S. person or not.

The statute is largely silent about what burden may be borne by the government to establish whether the target is a U.S. person. Instead, as aforementioned, §702 directs the Attorney General to adopt targeting procedures reasonably designed (a) to ensure acquisition is limited to persons reasonably believed to be outside US; and (b) to prevent the acquisition of domestic communications.[122] In other words, it only requires that the NSA not *know* (a) that the target is actually in US, 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.

Sections 703 and 704, in turn, which are designed to deal with U.S. persons, say nothing about the burden that may be required of the government in order to demonstrate whether a target either is—or is not—a U.S. person.[123] Instead, these provisions merely addresses situations where the applicant has probable cause to believe that the target is a person reasonably believed to be located outside the United States and is a foreign power, and agent of a foreign power, or an officer of employee thereof.[124]

In the absence of statutory guidance, and consistent with its statutory obligation to construct targeting procedures, the NSA has interpreted the statute as allowing the NSA, in the absence of concrete knowledge to the contrary, to *assume* that the target is a non-U.S. person.[125] The NSA's declassified minimization procedures explain,

---

SPIEGEL, July 1, 2013, available at http://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html (discussing Boundless Informant; noting, according to NSA documents, "alliances with over 80 major global corporations"; and publishing the global network of undersea cables); Phillip Dorling, *Snowden Reveals Australia's Links to U.S. Spy Web*, SYDNEY MORNING HERALD, July 8, 2013, available at http://www.smh.com.au/world/snowden-reveals-australias-links-to-us-spy-web-20130708-2plyg.html (noting the Australian Signals Directorate facilities and New Zealand Government Security Communications Bureau facility that participate in the X-Keyscore).

[120] FISC Memorandum Opinion, October 2011, at 42.

[121] Id.

[122] 50 USC §1881a(d).

[123] 50 USC §1881(b).

[124] 50 USC §1881b(b)(C) (for §703) and 50 USC §1881c(c)(B) (for §704).

[125] NSA Targeting Procedures, p. 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).

> 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.[126]

In light of the procedural recognition of the "absence of specific information," the immediate question that is raised is what action from the NSA is required in order to determine whether specific information to the contrary exists.

The answer, as understood by a close textual reading the targeting requirements, appears to be none. Throughout the targeting procedures, when referring to the databases or parallel surveillance systems that could be consulted to determine whether the target is a U.S. person or a non-U.S. person, the NSA uses the word "may." This word is 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 suggest what the NSA "must" do. This term, in contrast to "may", would suggest something that is formally required or necessary—i.e., a level of due diligence that is required prior to simply assuming that a target is a non-U.S. person.[127]

3. Burden of Proof Regarding Location

The NSA has similarly avoided being bound to a minimum level of due diligence with regard to establishing the location of the target. Section 702 requires that the information to be intercepted is limited to persons reasonably believed to be located outside the United States. As with the burden of proof regarding whether the target is a U.S. person, the statute is silent with regard to what steps the NSA or others must take to determine where the target is located.

As with the determination of whether a target is a U.S. person, the targeting procedures in reference for the location of the target come down on the side of greater flexibility for the NSA. The documents again make use of the auxiliary verb "may". Thus, the NSA "may review information in its databases" to ascertain if target is overseas.[128] 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."[129] It is under no procedural obligation to do so.[130]

---

[126] Minimization procedures published in June 2013 by the *Guardian*, dated from July 29, 2009, p. 2, §2, item (f), available at http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document.

[127] 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 Director of Civil Liberties and Privacy Office Report: NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*, Apr. 16, 2014, p. 4, *available at* http://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf.

[128] NSA Targeting Procedures, p. 2.

[129] NSA Targeting Procedures, p. 3.

[130] The minimization procedures appear to acknowledge the possibility: "In the event that the NSA determines that a person is reasonably believed to be located outside the United States and after targeting

4. Result of Statutory Interpretations

The three component statutory interpretations—namely, to/from or about (TFA), and the weak burdens of proof with regard to U.S. persons and the location of the target—undermine the protections created for U.S. persons in §§703 and 704 of the statute. They make it possible for the NSA to obtain significant amounts of American citizens' communications. .

The starting point for any statutory analysis is the language of the legislation itself. To the extent that the FAA controls access to U.S. persons' information, interpretations of the statute that allow broad access to the same run afoul of the procedures introduced by Congress. Where the FAA is vague or ambiguous, however, other methods of statutory interpretation may be applied.[131] While *noscitur a sociis* offers little insight in this regard, the doctrine of *ejusdem generis* suggests that the NSA's adherence to TFA extends well beyond the authorities introduced by Congress. Even if one rejects originalist interpretations as "intellectually antediluvian,"[132] and assumes a more dynamic model, the passage of the statute but five years past places claims of contextual alteration on rather shaky ground.

a. Protections Undermined

Congress introduced §§703 and 704 to increase the protections afforded to U.S. persons travelling outside of the United States. The previous framework, Executive Order 12333, authorized the intelligence community "to collect, retain or disseminate [foreign intelligence or counterintelligence] information concerning United States persons . . . in accordance with procedures established by the head of the agency and approved by the Attorney General."[133] 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."[134] Section 2.5 of the order states, in relevant part:

> The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each

---

this person learns that the person is inside the United States, or if NSA concludes that a 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." July 2009 Minimization procedures, §3(d)(1), p. 4, available at http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document. Such communications will be treated as "domestic communications." *Id.*

131 Traditional doctrine, for instance, requires reading statutes as static texts: i.e., by referencing the intent of the legislature in determining the meaning behind the words at the time of their enactment. William N. Eskridge, Jr., *Dynamic Statutory Interpretation*, 135 UNIV. OF PENNSYLVANIA L. REV., 1479 (1987), at 1479. *See also* Sutherland, Statutes and Statutory Construction, §45.05 (4th Ed. 1984); R. POSNER, THE FEDERAL COURTS: CRISIS AND REFORM 286-93 (1985); Easterbrook, *Statutes' Domains*, 50 U. CHI. L. REV. 533 (1983); William N. Eskridge, Jr., Philip P. Frickey, & Elizabeth Garrett, Cases and Materials on Legislation: Statutes and the Creation of Public Policy (3d ed. 2001). A modified version considers using the original purpose of the statute as a stand-in for the original intent of Congress—particularly where it may be difficult to ascertain the intention of the legislature in passing the statute. *Id.*, at 1480.

132 Eskridge, at 1482.

133 Exec. Order 12333, §2.3.

134 Exec. Order 12333, §2.3(b).

> case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power.[135]

For the government then to act on the certification, a determination first had to be made that probable cause existed to believe that the individual being targeted was a foreign power or an agent of a foreign power. Application to the Attorney General for this certification was informed by the contents of an application made consistent with DOD regulations.[136] *Pari passu,* these procedures 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.[137]

What this framework meant was that when a U.S. person was located overseas, he or she did not come within the stronger protections established in conjunction with traditional FISA—particularly in regard to a neutral, disinterested magistrate. Instead, the collection of foreign intelligence information was conducted consistent with procedures established by the head of the intelligence community entity in question, with the concurrence of the Attorney General. For DOD, this meant a statement of facts including both probable cause and necessity; but for each entity, potentially different guidelines applied.

In contrast to prior reliance on Executive Order 12333 and the operation of a less stringent regime, under the §703, government must submit an application to FISC identifying the target of the collection, and the facts and circumstances undergirding probable cause that the target is a foreign power or an agent of a foreign power.[138] The government must also establish probable cause that the target is located outside the United States.[139] The way in which §702 is being used, however, allows the NSA to bypass §703. Instead of having to go to a court to demonstrate probable cause, the NSA can simply assume that any U.S. person communicating internationally may be a foreign power or an agent thereof. It then uses its authority under §702 to scan the contents of the communications to determine whether this is, in fact, the case. The result—namely, the interception of U.S. persons' international communications—is the same.

This interpretation of §702 brings the NSA into conflict with Executive Order 12333, which restricts the FBI from using foreign intelligence collection as an excuse to acquire information about the domestic activities of U.S. persons. To the contrary, the TFA interpretation, combined with the low burden of proof required, means that information directly related to domestic activities is being collected. Even if it is not "targeted" as such, the result is the same.

b. Volume of Collection

For years, the volume of intercepts under §702 has been one of the principal concerns of legislators familiar with the program. Senators have consistently expressed unease about ODNI's claim that it is impossible to quantify how many Americans' communications have been implicated in the operation of §702. The

---

[135] Exec. Order 12333, §2.5, 46 Fed. Reg. at 59,951.
[136] DOD, Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons, DOD 5240.1-R, Proc. 5, Pt. 2C (Dec. 1982).
[137] *Id.*
[138] 50 USC §§1881b(b)-(c), §1881c(b)-(c). Note too that 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 USC §1881b(d), 1881c(d).
[139] *Id.*

information that has been released by the media suggests that massive information gathering is underway.

Following the initial release of the PRISM slides on June 6, 2013, on June 18, the NSA issued a Fact Sheet on the program, stating that FISA "allows only the targeting, for foreign intelligence purposes, of communications of foreign persons who are located abroad."[140] 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, for instance, 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.[141] 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.[142] General Alexander quickly replied, publishing a letter the following day.[143] He agreed with the senators that the fact sheet "could have more precisely described the requirements for collection under Section 702."[144] He then went on to provide more detail, quoting the statute in full.[145]

As to Wyden and Udall's second concern—namely, 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.[146] The *Guardian* followed this claim by a release on June 27, 2013 of a draft NSA inspector general report reviewing PSP and its transfer to §702.[147] From

---

[140] The Fact Sheet, which does not have a date on it, was released June 18, 2013. (See https://www.aclu.org/nsa-documents-released-public-june-2013) The document was quickly withdrawn from the DNI's website; however, a copy of the Fact Sheet can be found online at http://www.wyden.senate.gov/news/blog/post/wyden-and-udall-to-general-alexander-nsa-must-correct-inaccurate-statement-in-fact-sheet.

[141] 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 §702 of the Foreign Intelligence Surveillance Act of 1978, as amended, Jan. 8, 2007, available at http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document [hereinafter §702 Targeting Procedures]; Exhibit B: Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to §702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, available at https://www.aclu.org/files/natsec/nsa/20130816/FAA%20Minimization%20Procedures.pdf [hereinafter §702 Minimization Procedures].

[142] Letter from Ron Wyden and Mark Udall, to General Keith Alexander, Washington, DC, 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

[143] Letter from General Keith B. Alexander, to the Hon. Ron Wyden and the Hon. Mark Udall, Fort Meade, Maryland, June 25, 2013, available at https://www.aclu.org/files/natsec/nsa/20130816/General%20Alexander%20Letter%20re%20NSA%20Fact%20Sheet%20Inaccuracy.pdf.

[144] *Id.,* at 1.

[145] *Id.*

[146] *Id.*

[147] Working Draft, Office of the Inspector General, National Security Agency Central Security Service, Mar. 24, 2009, available at https://www.aclu.org/files/natsec/nsa/20130816/NSA%20IG%20Report.pdf.

this and subsequent releases, it became clear that the program was significantly more extensive than first envisioned.[148]

The collection of massive amounts of information about U.S. persons undermines the intent of Congress in enacting not just §702, but §§703 and 704. The entire point of adding these sections was to circumscribe the NSA's ability to collect data and, in the process, to offer U.S. persons a greater degree of privacy.[149] Yet TFA, combined with the lower burdens of proof with regard to U.S. person status and the location of the target, have allowed significantly broader front-end collection.

c. Statutory Interpretation: Ejusdem Generis

In interpreting a statute, courts first look to the language of the statute itself. The Supreme Court explained, "Absent a clearly expressed legislative intention to the contrary, that language must ordinarily be regarded as conclusive."[150]

To the extent that the FAA clearly states the procedures under which U.S. persons' communications overseas must be collected (in accordance with §§703 and 704), an interpretation of §702 that allows the intelligence community to bypass the restrictions introduced by Congress violates the express language of the statute.[151] This reading is reinforced by the preamble to the act,[152] which states in relevant measure that the *purpose* of the Act was "to amend the Foreign Intelligence Surveillance Act of 1978 to establish a procedure for authorizing certain acquisitions of foreign intelligence."[153] The point of adding the new sections to FISA was thus, in part, to create new procedures (as outlined in §§703 and 704)—making problematic any interpretation by the intelligence community that allows the Executive to bypass these restrictions to a meaningful degree. In light of the volume of communications thereby obtained, as well as substantive nature of the content intercepted, the NSA's interpretations may thus be said to fall outside statutory constraints.

Perhaps the best objection to this point, at least as regard to TFA, emphasizes relativity. Namely, the statute itself does not specify what can be collected *relative* to a particular target. And although under traditional FISA, only information to or from a target was included, the comparison between traditional FISA and the FAA may be one of apples and oranges. Traditional FISA related to the domestic collection of international communications—not to the interception of international communications generally.

When statutes are vague or somehow ambiguous, courts must turn to a method of statutory interpretation. One of the most common approaches, *noscitur a sociis*, offers

---

[148] *See, e.g.,* PRISM slides released by the *Guardian*, June 29, 2013, available at https://www.aclu.org/files/natsec/nsa/20130816/PRISM%20Powerpoint%20Slides%20re%20Data%20Acquisition.pdf.

[149] *See, e.g.,* Statement of Senator Rockefeller, 154 Cong. Rec. S6465 (2008) ("[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."); Statement of Ms. Harman, 154 Cong. Rec. H5762 (2008)("[This bill] expands the circumstances for which individual warrants are required, by including Americans outside the U.S.").

[150] Consumer Product Safety Commission et al v. GTE Sylvania, Inc. et al, 447 U.S. 102 (1980). *See also* Connecticut Nat'l Bank v. Germain, 503 U.S. 249, ("[I]n interpreting a statute a court should always turn to one cardinal canon before all others. We have stated time and again that courts must presume that a legislature says in a statute what it means and means in a statute what it says there.").

[151] This approach is consistent with the whole act rule—i.e., that legislatures draft statutes in a manner that is internally consistent in how the relevant provisions work together. *See* Eskridge et al, 2001, at 830.

[152] Eskridge, 2001, at 832.

[153] FAA, at 1.

little in recompense, since, in the statute, there is only discussion of the target itself, and not of the relationship between the communications to be intercepted and the target. It is thus difficult to ascertain from the placement of the words within the broader context the extent of the communications anticipated by the legislature—indeed, there are no words so placed.

In contrast, the doctrine of *ejusdem generis* offers greater insight. This approach comes to the fore when one looks at whether people, things, or situations not explicitly included in the statutory language belong to the class otherwise denoted. Here, the NSA's interpretation—namely, adding "about"—takes us rather far afield from Congress' consideration of intercepts and targets. In passing the FAA, Congress focused on the target of the surveillance: i.e., whether the target itself was a U.S. person or not, and where the target was located, mattered greatly in whether the executive could exercise its intercept function.

It seems at least a stretch to interpret the statute to read that although the targets themselves could not be a U.S. person, or located inside the United States (on the grounds of which their communications could be intercepted), communications *not hinging on the target's identity or location*, could be included.

Like the doctrine of *expression unius*, this doctrine does assume that the legislature thought through possible variations in language; but the legislative history of the FAA suggests that Congress was acutely aware of the status of the target and the target's location as a necessary condition for the interception of communications. If, therefore, under §§703 and 704, a U.S. person's communications could not be intercepted, under the doctrine of *ejusdem generis*, it runs at counter-purposes to the statutory language to read §702 as allowing *precisely* these communications to be collected.

Even if one rejects an originalist and/or textualist reading and instead asks what the FAA ought to mean "in terms of the needs and goals of our present day society[?]"[154] It would be rather extraordinary to state that over the past five years the surrounding context had changed so radically as to require us to read the statute differently. Congress recently introduced the statute. It did so to update FISA itself. It thus represents Congress' effort to update a 1978 structure to the current context. There have been no major events or political upheavals that might lead us to conclude a radically altered situation.

5. FISC Oversight of Targeting Procedures

The FAA created an exception to traditional FISA, removing FISC from reviewing specific orders. Instead, the Attorney General, in consultation with the Director of National Intelligence, is responsible for determining whom to target, as well as the contours of the targeting and minimization procedures. FISC, in turn, has jurisdiction only to review certification, targeting procedures, and minimization procedures.[155] Its role in regard to each of these functions is narrowly circumscribed.

The statute empowers FISC to "determine whether the certification contains all the required elements."[156] This means that the court merely confirms that the government has included the required elements—namely, that:

(1) the certifications have been made under oath by the AG and the DNI,[157]
(2) the certifications contain each of the attestations statutorily required,[158]

---

[154] Phelps, *Factors Influencing Judges in Interpreting Statutes*, 3 VAND. L. REV., 456, 469 (1950).
[155] 50 USC §1881a(i)(1)(A).
[156] 50 USC §1881a(i)(2)(A).
[157] 50 USC §1881a(g)(1)(A).

(3) each of the certifications is accompanied by the applicable targeting and minimization procedures,[159]
(4) each of the certifications is supported by the affidavits of appropriate national security officials,[160] and
(5) each of the certifications has an effective date for the authorization.[161]

FISC reviews targeting procedures to "assess whether the procedures are reasonably designed to – (i) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and (ii) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States."[162]

The minimization procedures must "meet the definition of minimization procedures under [50 U.S.C. §§] 1801(h) or 1821(4). . . "[163] That definition, in turn, requires "specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular [activity], to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[164] Finally, Court must assess whether targeting and minimization procedures are consistent with the Fourth Amendment.[165]

Once approved for a particular program, the way in which FISC carries out its duties in practice appear to be somewhat *pro forma*. (The Court, for instance, pointed out in its October 2011 opinion that the targeting and minimization procedures were simply copies of the procedures filed July 29, 2009.)[166] The Court's ability, moreover, to challenge even what appears to be a violation of the statute on its face appears similarly limited.

FISC first became aware of the implications of the NSA's interpretation of to/from and about in 2011.[167] The court was surprised by the government's admission that it would have to intercept significantly more content in order to scan it for

---

[158] 50 USC §1881 a(g)(2)(A).
[159] 50 USC §1881 a(g)(2)(B).
[160] 50 USC §1881a(g)(2)(c).
[161] 50 USC §1881a(g)(2)(D).
[162] 50 USC §1881a(i)(2)(B).
[163] 50 USC §1881a(e)(1).
[164] 50 U.S.C. §§1801(h) and 1821(4).
[165] 50 USC §1881a(i)(2)(c).
[166] U.S. Foreign Intelligence Surveillance Court, Memorandum Opinion, Oct. 3, 2011, (J. Bates), (Part 2), pp. 18-19, available at http://www.dni.gov/files/documents/October%202011%20Bates%20Opinion%20and%20Order%20Part%202.pdf.
[167] U.S. Foreign Intelligence Surveillance Court, Memorandum Opinion, Oct. 3, 2011, (J. Bates), (Part 2), pp. 15-16, available at http://www.dni.gov/files/documents/October%202011%20Bates%20Opinion%20and%20Order%20Part%202.pdf. This document was declassified by the Director of National Intelligence August 21, 2013, along with a series of other documents, including, *inter alia*, U.S. Foreign Intelligence Surveillance court Memorandum Opinion and Order, Nov. 30, 2011, (J. Bates), U.S. Foreign Intelligence Surveillance Court Memorandum Opinion, Sept. 25, 2012 (J. Bates), and the 2011 Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to §702 of the Foreign Intelligence Surveillance Act, as amended, Oct. 31, 2011.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.

relevant information. According to FISC, misrepresentation played a role in the Court's prior failure to understand the scope of the program. In its first §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 Section702 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.[168]

In reviewing and granting the application for an order, the Court had not taken into account the NSA's acquisition of Internet transactions, which "materially and fundamentally alter[ed] the statutory and constitutional analysis."[169]

FISC was troubled by the government's revelations regarding the NSA's acquisition of Internet transactions—marking this the third time in less than three years in which the NSA had disclosed a "substantial representation" on "the scope of a major collection program."[170] Either the Court was particularly slow, or the government had ben lying: "The government's submissions make clear not only that NSA has been acquiring Internet transactions since before the Court's approval of the first §702 certification in 2008, but also that NSA seeks to continue the collection of Internet transactions."[171]

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."[172] Yet this appeared to be precisely what had happened with regard to the scope of the NSA's upstream collection.[173]

---

[168] U.S. Foreign Intelligence Surveillance Court, Memorandum Opinion, Oct. 3, 2011, (Part 2), pp. 15-16, available at http://www.dni.gov/files/documents/October%202011%20Bates%20Opinion%20and%20Order%20Part%202.pdf.

[169] U.S. Foreign Intelligence Surveillance Court, Memorandum Opinion, Oct. 3, 2011, (Part 2), p. 16, available at http://www.dni.gov/files/documents/October%202011%20Bates%20Opinion%20and%20Order%20Part%202.pdf.

[170] U.S. Foreign Intelligence Surveillance Court, Memorandum Opinion, Oct. 3, 2011, (Part 2), p. 16, fn 14, available at http://www.dni.gov/files/documents/October%202011%20Bates%20Opinion%20and%20Order%20Part%202.pdf. The Court goes on to cite the NSA's bulk acquisition of telephone metadata under §215; the second incident is entirely redacted.

[171] U.S. Foreign Intelligence Surveillance Court, Memorandum Opinion, Oct. 3, 2011, (Part 2), p. 17, fn 14, available at http://www.dni.gov/files/documents/October%202011%20Bates%20Opinion%20and%20Order%20Part%202.pdf

[172] 50 USC §1809(a).

[173] The Court stated that it would address the potential criminal violation in a separate order. U.S. Foreign Intelligence Surveillance Court, Memorandum Opinion, Oct. 3, 2011, (Part 2), p. 17, fn. 15, available at http://www.dni.gov/files/documents/October%202011%20Bates%20Opinion%20and%20Order%20Part

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—i.e., "discrete communications between or among the users of telephone and Internet communications facilities that are to or from a facility tasked for collection."[174] As in the past, it found the targeting procedures in 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 transactions.[175] Remarkably, despite the acknowledgement by the government that it knowingly collected tens of thousands of messages of a purely domestic nature, the Court found the procedures consistent with the statutory language that prohibited the intentional acquisition of domestic communications.[176]

The Court's analysis of the targeting procedures focused on upstream collection.[177] 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."[178] 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."[179] 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.[180] The number of purely domestic communications alone was in the tens of thousands.[181]

Despite this finding, the Court 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 certification] is limited to targeting persons reasonably believed to be located outside the United States" and (2) "prevent

---

%202.pdf. As of the time of writing, the order referenced in the October 2011 opinion has not been declassified.

[174] U.S. Foreign Intelligence Surveillance Court, Memorandum Opinion, Oct. 3, 2011, (Part 2), p. 17, available at http://www.dni.gov/files/documents/October%202011%20Bates%20Opinion%20and%20Order%20Part%202.pdf

[175] U.S. Foreign Intelligence Surveillance Court, Memorandum Opinion, Oct. 3, 2011, (Part 3), p. 29, available at http://www.dni.gov/files/documents/October%202011%20Bates%20Opinion%20and%20Order%20Part%203.pdf.

[176] U.S. Foreign Intelligence Surveillance Court, Memorandum Opinion, Oct. 3, 2011, (Part 4), p. 33, available at http://www.dni.gov/files/documents/October%202011%20Bates%20Opinion%20and%20Order%20Part%204.pdf.

[177] U.S. Foreign Intelligence Surveillance Court, Memorandum Opinion, Oct. 3, 2011, (Part 3), p. 29, available at http://www.dni.gov/files/documents/October%202011%20Bates%20Opinion%20and%20Order%20Part%203.pdf.

[178] U.S. Foreign Intelligence Surveillance Court, Memorandum Opinion, Oct. 3, 2011, (Part 4), p. 31, available at http://www.dni.gov/files/documents/October%202011%20Bates%20Opinion%20and%20Order%20Part%204.pdf.

[179] *Id.*

[180] *Id.,* at 31-32.

[181] *Id.,* at 33. *See also* U.S. Foreign Intelligence Surveillance Court, Memorandum Opinion, Oct. 3, 2011, (Part 5), pp. 42-43, 46 available at http://www.dni.gov/files/documents/October%202011%20Bates%20Opinion%20and%20Order%20Part%205.pdf.

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."[182]

The Court employed extraordinary logic to reach this conclusion. In short, it 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 States."[183] Since 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."[184] 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.[185] The Court concluded that, as far as the targeting procedures were concerned, at least with regard to multi-communication transactions (MCTs), the NSA had circumvented "the spirit" but not the letter of the law. [186]

As a method of statutory interpretation, the Court's conclusion runs contrary to one of the most important canons in the law: namely, that where the language of a statute is plain and unambiguous, it must be given effect.[187] The only exception to this is where a literal interpretation would lead to absurd or mischievous results, or thwart the manifest purpose of the statute. Here, however, it is FISC's interpretation of the statutory language that leads to an extraordinary result. The statute bans the knowing interception of entirely domestic conversations. The NSA says that it knowingly intercepts entirely domestic conversations. And yet the Court finds its actions consistent with the statute.

This judicial finding also raises question about whether FISC plays a meaningful role in regard to §702. The court's role, as aforementioned, is already significantly circumscribed. The Court's position in regard to the knowing collection of entirely domestic conversations stemmed from the NSA's apparent lack of technical capabilities. In other words, because the NSA had not developed the technology to abide by the statutory provisions, it was thus excused from abiding by the statutory provisions. It is far from clear how this amounts to any sort of a meaningful check on the exercise of surveillance authorities under §702.

Beyond the immediate question of law, this interpretation raises important policy questions about the incentives created by the governing statute: i.e., willful ignorance. If the intelligence community wants more information, then, consistent with the FISC opinion, it is in the IC's interests never to develop the technology to identify whether it is actually violating the statute.

---

[182] 50 U.S.C. 1881a(d)(1); and 50 USC §1881a(i)(2)(B).
[183] 50 U.S.C. 1881a(d)(1)(B), quoted and cited at *Id.,* pp. 46-47.
[184] *Id.,* at 48.
[185] *Id.*
[186] *Id.* The Court distinguished between single communication transactions (SCTs) and multi-communications transactions (MCTs). *See* U.S. Foreign Intelligence Surveillance Court, Memorandum Opinion, Oct. 3, 2011, (Part 3), p. 28, available at http://www.dni.gov/files/documents/October%202011%20Bates%20Opinion%20and%20Order%20Part%203.pdf; and (Part 5), pp. 42-43, available at http://www.dni.gov/files/documents/October%202011%20Bates%20Opinion%20and%20Order%20Part%205.pdf.
[187] Eskridge et al, 2001, at 824.

B. Post-Targeting Minimization and Analysis

The NSA keeps and analyzes the content of international intercepts.[188] Analysts use computer selection terms and other information ("such as telephone numbers, key words or phrases, or other discriminators") to scan the content to determine whether there is information of value for either foreign intelligence or criminal law purposes.[189] Four matters here deserve attention: the purpose of the analysis, the scope of the minimization procedures, the use of U.S. person information to query the data, and recombinant information.

1. Purpose of the Post-Targeting Analysis

Although the statutory premise for the acquisition of information under §702 is that the target is outside the United States, NSA documents suggest that it uses the subsequent analysis to determine if and when the target entered the United States—suggesting that information is obtained at the front end and *then* analyzed based on location. The NSA, for instance, notes that it takes into account sources like telecommunications logs showing movement [e.g., Global System for Mobiles (GSM) Home Location Registers (HLR)], as well as all available Internet communications databases.[190] The NSA may also analyze the substantive information itself "for indications that a target has entered or intends to enter the United States."[191]

These procedures indicate that communications to or from the target or held by the target will be collected, based on the assumption that the target is outside the United States, and will then be analyzed to see if any of the target is actually located in domestic bounds. Similarly, all information *relating to* targets will be collected, on the assumption that the target is outside the United States. It will then be analyzed to see if the target with reference to whom the content of communications are being analyzed, is actually within U.S. borders.

To the extent that the use of the analytical function in this capacity supplants the front-end calculations prior to the collection of information, the NSA may be bypassing statutory constraints. This interpretation is supported by the default assumption (discussed above) that the individual is located overseas. While it may offer some protection, its occurrence after the information is collected suggests that Congressional intent in setting standards prior to the collection is not being met.

To the extent, however, that the subsequent analysis to determine target status and location merely operates as a second layer of protection, the criticism falls away. The real question is the extent to which it supplants the front-end determination. In light of the highly classified nature of the PRISM and upstream collection programs, it is difficult to know how much work this analytical function is performing, post-collection.

---

[188] The targeting procedures document released in June 2013 explains, "After a person has been targeted for acquisition by NSA, NSA will conduct post-targeting analysis." Targeting Procedures, p. 6. *See also NSA Director of Civil Liberties and Privacy Office Report: NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*, Apr. 16, 2014, p. 6, *available at* http://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf (Communications provided to NSA under Section 702 are processed and retained in multiple NSA systems and data repositories. One data repository, for example, might hold the contents of communications such as the texts of emails and recordings of conversations, while another, may only include metadata. . . such as the time and duration of a telephone call, or sending and receiving email addresses.")

[189] §3(b)(5), pp. 3-4, available at http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document.

[190] Targeting Procedures, p. 6.

[191] Targeting Procedures, p. 7.

2. Scope of the Minimization Procedures: MCTs

In October 2011 FISC found that the NSA's minimization procedures violated the statute.[192] The key issue was the failure of the procedures expressly to contemplate the acquisition of multi-communication transactions (MCTs). They referenced "domestic communication" and "foreign communication", but they failed to take account of communications constructed of smaller packets of information.[193] The omission influenced the amount and type of information retained by the NSA.

The proposed minimization procedures focused only on the discrete communications within MCTs that analysts might decide to use; they did not require analysts to do anything with other portions of the MCT.[194] The information was not marked in any way (e.g., whether or not they contained wholly domestic communications, related to U.S. persons, etc.). The Court explained,

> The net effect is that thousands of wholly domestic communications (those that are never reviewed and those that are not recognized by analysts as being wholly domestic), and thousands of other discrete communications that are not to or from a targeted selector but that are to, from, or concerning a United States person, will be retained by the NSA for at least five years, despite the fact that they have no direct connection to a targeted selector and, therefore, are unlikely to contain foreign intelligence information.[195]

The NSA had failed to address myriad options (such as limiting access to a small group of specially-trained analysts, applying minimization procedures to each discrete communication, marking the MCT or its discreet parts to identify the type of information obtained, reducing the retention time for MCTs and unreviewed upstream communications, etc.) in the minimization procedures.[196]

The NSA subsequently rectified the deficiency: by November 2011, FISC was satisfied that the problems had been addressed.[197] Like the July 2009 minimization procedures, the October 31, 2011 minimization procedures have been declassified by the Director of National Intelligence.[198] Exactly how the problem has been addressed is not publicly clear.

---

[192] *Id.,* at 49 ("[T]he Court concludes that NSA's minimization procedures, as applied to MCTs in the manner proposed by the government, do not meet the statutory definition in all respects.")

[193] U.S. Foreign Intelligence Surveillance Court, Memorandum Opinion, Oct. 3, 2011, (Part 6), p. 50, available at http://www.dni.gov/files/documents/October%202011%20Bates%20Opinion%20and%20Order%20Part%206.pdf.

[194] *Id.,* at 59.

[195] U.S. Foreign Intelligence Surveillance Court, Memorandum Opinion, Oct. 3, 2011, (Part 7), pp. 60-61, available at http://www.dni.gov/files/documents/October%202011%20Bates%20Opinion%20and%20Order%20Part%207.pdf.

[196] As far as dissemination went, the Court noted that FISA imposes a stricter standard than applicable with regard to minimize: i.e., the procedures here must be reasonably designed to "prohibit" the dissemination of U.S. persons' information, consistent with the foreign intelligence needs of the United States. *Id.,* at 63. The Court determined that the measures adopted by the government were sufficient. *Id.,* at 66-67.

[197] U.S. Foreign Intelligence Surveillance court Memorandum Opinion and Order, Nov. 30, 2011, (J. Bates), at 2, available at http://www.dni.gov/files/documents/November%202011%20Bates%20Opinion%20and%20Order%20Part%201.pdf ([T]he Court concludes that . . . the government has adequately corrected the deficiencies identified in the October 3 Opinion, and the request for approval is therefore granted.")

[198] *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*

It is worth noting here that, as a matter of statutory weakness (and not NSA implementation thereof), the FAA does not impose any meaningful consequences for government-initiated surveillance using procedures either not approved by FISC or subsequently found to be unlawful.[199] In the case of the MCT concern, it appears that in the intervening seven months between the government's request for an order approving the certification in April 2011 until resolution of the matter in November 2011, FISC did not allow collection to proceed.[200] From the publicly-available documents, though, it is not clear how the Court has subsequently treated information collected during periods of noncompliance, once the Court became aware of the problem.

3. Queries using U.S. Person information and Reverse Targeting

Section 702 forbids U.S. persons from being targeted under its auspices. It also makes it illegal to target someone outside the United States, where the purpose of the acquisition is to obtain information about a particular person known to be within domestic bounds. This practice, known as "reverse targeting," was central to Congressional debates on the legislation.[201] As Representative Langevin explained in the House during passage of the FAA, the insertion of FISC in the process proved an important protection: "This will 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 inadvertently intercepted, it is dealt with in a manner that guarantees legal protections."[202]

Despite Congress' concern about reverse targeting and insertion of protections to prevent this from happening, the NSA instituted a rule change in October 2011 to make it possible to query communications obtained under §702 using U.S. person names and identifiers as query terms.[203] The relevant definition in the 2011 minimization procedures is largely consistent with its predecessor:

> Identification of a United States person means (1) the name, unique title, or address of a United States person; or (2) other personal identifiers of a United States person when appearing in the context of activities conducted by that

---

Surveillance Act of 1978, as Amended, Oct. 31, 2011, available at http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf. [hereinafter 2011 Minimization Procedures]

[199] Statement of Senator Feingold, Cong. Rec, Senate, July 9, 2008, S6458 ("Say, for example, the FISA Court determines that the procedures were not even reasonably designed to wiretap foreigners outside the United States rather than Americans at home. Under this bill, all that illegally obtained information on Americans can be retained and used.")

[200] Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications for DNI/AG 702(g), cited in October 2011 Memorandum Opinion (Bates, J.).

[201] *See, e.g.,* 154 Cong. Rec. H5757 (2008)(Letter from the Administration regarding FAA, to Hon. Nancy Pelosi, Speaker, House of Representatives, June 19, 2008, read into the record); 154 Cong. Rec. H5740 (2008)(statement of Representative McGovern); 154 Cong. Rec. H5762 (2008)(statement of Ms. Harman "[This bill] protects Americans from so-called reverse targeting.").

[202] 154 Cong. Rec. H5766 (2008).

[203] *See* James Ball and Spencer Ackerman, *NSA Loophole Allows Warrantless Search for U.S. Citizens' Emails and Phone Calls*, THE GUARDIAN, Aug. 9, 2013, available at http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls. ("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 implement any USP queries until an effective oversight process has been developed by NSA and agreed to by DOJ/ODNI. . . . (702 data is contained in MARINA, MAINWAY, NUCLEON, PINWALE (Sweet* and Sour* partitions) and other databases).")

> 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.[204]

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

Although glimmers of this change appeared in August 2013, it was not until March 2014 that the Director of National Intelligence, James Clapper, confirmed in a letter to Senator Ron Wyden that the NSA had queried §702 data "using U.S. person identifiers."[205] The following month the NSA's privacy and Civil Liberties Officer confirmed use of the same.[206]

FISC has upheld this reading of the statute.[207] 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 §3(b)(5) to allow NSA to query the vast majority of its §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 §702 collection, queries using United States-person identifiers would be limited to those reasonably likely to yield foreign intelligence information. NSA Minimization Procedures, Sec. 3(b)(5).[208]

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."[209]

---

[204] 2011 Minimization Procedures, p. 2 (compare to 2009 Minimization Procedures, p. 2). This definition appears to be consistent with the legislative history of FISA. *See, e.g.,* Conference Report Filed in House, Oct. 5, 1978, H11673 ("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.")

[205] Letter from James R. Clapper to the Hon. Ron Wyden, U.S. Senate, Washington, DC, Mar. 28, 2014, available at https://www.documentcloud.org/documents/1100298-unclassified-702-response.html.

[206] *NSA Director of Civil Liberties and Privacy Office Report: NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*, Apr. 16, 2014, p. 7, *available at* http://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf ("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.")

[207] U.S. Foreign Intelligence Surveillance Court, Memorandum Opinion, Oct. 3, 2011, p.p. 22-24, https://www.aclu.org/files/assets/fisc_opinion_10.3.2011.pdf.

[208] FISC Memorandum Opinion, pp. 22-23.

[209] FISC Memorandum Opinion, p. 24.

As a practical matter, what this rule change means is that U.S. person information that is incidentally collected via §702 can now be mined using U.S. person information as part of the queries. Together with the NSA's acknowledged collection of tens of thousands of wholly domestic conversations, the result is that U.S. person information can be collected and queried solely in relation to U.S. persons. This circumvents Congress' requirement that prior to U.S. person information being obtained or analyzed, the government be required to appear before a court to obtain a document approximating the warrant requirement as understood to be consistent with the Fourth Amendment.

4. Recombinant Information

A final point to draw out with regard to the back-end analysis of §702 data centers on how the information is subsequently used. Much of this information remains classified, so comment is necessarily cabined.

Documents leaked to the press suggest extremely sophisticated back-end analytical capabilities. XKeyScore, for instance, mentioned in one NSA training presentation, claims to deliver "real-time target activity." The system appears to be a sort of search engine, involving a complex set of software interfaces, database, and servers, to allow analysts to find the online activities of anyone in the world, real time.[210] PRISM and upstream collection, as well as other intelligence sources, appear to feed into this system.[211] Because the program is being run under the FAA, analysts must select "foreign factors" to search the massive data repository.[212]

According to the slides, published in the *New York Times*, but as of the time of writing not declassified by the U.S. government, the power of this data is substantial. Analysts can look for anomalous events (e.g., individuals in Germany speaking Farsi), or search entire regions (e.g., all encrypted word documents generated in Iran) and then trace the communications backwards to a strong selector. XKeyScore uses HTML language tags to identify relevant data, it looks at users' activities on Google maps, and it identifies machines open to exploitation.[213]

If one accepts the premise that significant amounts of information are being obtained via the way in which the NSA and other elements of the IC have implemented §702, then the implications of new knowledge generated by mining this data and combining it with other information are considerable. What is "incidental" in one context may become central to subsequent analysis. Further concerns exist about the dissemination of information to other government entities. That the collection and use of such information is taking place absent the insertion of any judicial warrant in the process, particularly in light of the potential introduction of the information for criminal prosecution, gives rise to Fourth Amendment concerns.

---

[210] Brett Max Kaufman, *A Guide to What We Now Know About the NSA's Dragnet Searches of Your communications*, Free Future, American Civil Liberties Union, Aug. 9, 2013, available at https://www.aclu.org/blog/national-security/guide-what-we-now-know-about-nsas-dragnet-searches-your-communications.

[211] *Id.*

[212] Brett Max Kaufman, *A Guide to What We Now Know About the NSA's Dragnet Searches of Your communications*, Free Future, American Civil Liberties Union, Aug. 9, 2013, available at https://www.aclu.org/blog/national-security/guide-what-we-now-know-about-nsas-dragnet-searches-your-communications.

[213] Charlie Savage, *NSA Said to Search Content of Messages to and From U.S.*, N. Y. TIMES, Aug. 9, 2013, *available at* http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?ref=todayspaper&pagewanted=all. *See also* https://www.aclu.org/files/natsec/nsa/20130816/NSA%20XKeyscore%20Powerpoint.pdf

C. Retention and Dissemination of Data

Additional concerns relates to the retention and dissemination of data collected under §702. The NSA automatically retains all encrypted communications. Paired with increasing public and private use of encryption, this presents concerns about the extent to which the exception may swallow the rule and result 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.[214] While the former category may be broad, it is anchored in traditional FISA and critical for U.S. national security. The latter category is also 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 §702 for criminal prosecution raises important constitutional questions.

1. Retention of Encrypted Communications

The NSA automatically retains all encrypted communications, information that contains technical data base information, or information necessary to assess a "communications security vulnerability".[215] This information is stored for five or more years, as considered necessary by CYBERCOM. Encrypted material in particular may be retained for "any period of time during which encrypted material is subject to, or of use in, cryptanalysis."[216]

The reason this matters is that 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 email. 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.[217] 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 between you and Gmail's servers, but also as they

---

[214] Minimization procedures published in June 2013 by the *Guardian*, dated from July 29, 2009, p. 2, §2, item (f), available at http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document. *See also* Government Fact Sheet on Section 702, June 2013, *available at* https://www.fas.org/irp/news/2013/06/nsa-sect702.pdf ("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.")

[215] July 2009 Minimization Procedures, §5(3), p. 5.

[216] July 2009 Minimization procedures, §6(a)(1)(a), p. 6.

[217] Nicolas Lidzborski, Gmail Security Engineering Lead, 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. *See also* Lily Hay Newman, *Now Gmail Encrypts Every Email. Other Services Should, Too*, SLATE, Mar. 21, 2014, 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.

> move between Google's data centers—something we made a top priority after last summer's revelations.[218]

The irony of Google's actions in light of the NSA's retention policies is hard to miss: because the NSA was intercepting Gmail and reading it (at which point the NSA 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, [219] it seems that this practice may become standard.

Not only are we seeing greater individual use of encryption, but companies are increasingly 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.[220] 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), has encouraged industry to make greater use of encryption.[221] According to a recent market research report, the hardware encryption market is expected to reach some $166.67 billion by 2018, growing at an incredible CAGR of 62.17% 2013 to 2018.[222] These trends call attention to the NSA's back-end retention policies with regard to encrypted materials.

---

[218] *Id.*

[219] Lily Hay Newman, *Now Gmail Encrypts Every Email. Other Services Should, Too*, SLATE, Mar. 21, 2014, 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.

[220] Marketsandmarkets.com, 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), SE 1876, July 2013, available at http://www.marketsandmarkets.com/Market-Reports/hardwar.e-based-encryption-systems-market-1115.html.

[221] Verizon, for instance, documented 198 data breaches in 2013 in retail, accommodation and food industry. 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, available at http://www.crn.com/news/security/300072595/despite-prominent-retail-breaches-pos-system-attacks-decline-report-finds.htm. *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-breaches-in-security-are-hotels.html?_r=0; 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.

[222] Marketsandmarkets.com, 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), SE 1876, July 2013, available at http://www.marketsandmarkets.com/Market-Reports/hardwar.e-based-encryption-systems-market-1115.html.

2. Breadth of "Foreign Intelligence information"

The term "foreign intelligence information" is not itself defined in §702's minimization procedures.[223] It is, however, found in traditional FISA, where it is understood as:

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
> (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
> (2) information with respect to a foreign power or 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.[224]

The items listed under (1) appear to be consistent with FISA and, in particular, the criminal aspects of behavior that the statute is meant to address. They key directly 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 (i.e., 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.[225] As such, they are legitimate interests to be pursued under the exercise of §702 authorities, as applied overseas to non-U.S. persons.

To the extent that surveillance targeting may raise international relations concerns, such as heightened sensitivity to economic espionage, both the execution of the surveillance and the response to other countries' representations lays firmly in the hands of the political branches—not the judiciary.[226] As a statutory matter, Congress has given the executive broad room for movement.

3. Criminal Prosecution

Outside of encrypted communications (and technological difficulties), and foreign intelligence, 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

---

[223] The minimization procedures, however, define "foreign communications" broadly to mean "a communication that has at least one communicant outside the United States." (2009 Minimization Procedures, §2, p. 2)

[224] 50 USC §1801(e).

[225] *See, e.g.,* Laura Poitras, Marcel Rosenbach and Holger Stark, *Ally and Target: US Intelligence Watches Germany Closely*, DER SPIEGEL ONLINE INTERNATIONAL, Aug. 12, 2013, available at http://www.spiegel.de/international/world/germany-is-a-both-a-partner-to-and-a-target-of-nsa-surveillance-a-916029.html (citing an April 2013 NSA document as highlighting these intelligence priorities for U.S. surveillance of the European Union).

[226] *See* Laura K. Donohue, *U.S.-EU Cloud Industry and Privacy Protections*, AM. BUS. L. REV. (2014).

the NSA would like to retain the information.[227] In light of front-end considerations (i.e., the inclusion of information "about" selectors/targets, and the assumption of non-U.S. person and overseas status), a significant amount of U.S. persons' information can be obtained—and the individual's life or freedom forfeit—without any individualized suspicion of that person's involvement in wrongdoing. Similarly, further query of databases using U.S. person identifiers may implicate U.S. persons in criminal activity. But, again, no judicial process is required prior to further inquiries.

As a result, NSA procedures may uncover evidence of criminal activity, which can then be used in a court of law, without ever having particularized suspicion of that individual having ever engaged in wrongdoing—and without the involvement of a neutral, third-party magistrate, to protect the rights of the individual. Courts have in the past found applications under traditional FISA sufficient for this purpose.[228] But §702 includes none of these protections, giving rise to Fourth Amendment concerns.

4. Dissemination

Part of the rationale for the inclusion of minimization procedures in the original Foreign Intelligence Surveillance Act was to limit the dissemination of non-publicly available information concerning non-consenting U.S. persons.[229] The House amendments required that any information obtained under FISA not be disseminated in a manner that identified an individual, absent that person's consent, unless their identity was central to understanding the foreign intelligence information or assessing its importance (outside of criminal activity). In addition, no contents of any communication to which a U.S> person was party would be disclosed, disseminated, used, or retained for more than 24 hours, absent court order. During conference, the House version was slightly modified to require minimizations procedures to be reasonably designed to minimize acquisition and retention—but to prohibit the dissemination—of specified information. The rationale was that "the standard for dissemination should be higher than for acquisition and retention". Simultaneously, there should be a reasonableness component to the prohibition, to ensure that U.S. foreign intelligence needs were met.[230]

IV. THE ACQUISITION OF 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

[227] July 2009 Minimization procedures, §6(1)(3), p. 6.

[228] But note limitation recognized by Congress at the introduction of FISA to limit subsequent use of incidental information to instances involving potential threats to human life or serious bodily harm: "The Senate bill prohibited any use of the contents of unintentionally acquired domestic radio communications, if there is a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, except where the contents indicate a threat of death or serious bodily harm to any person. The House amendments contained a comparable provision, with an exception if the contents may indicate a threat of death or serious bodily harm to any person. The conference substitute adopts the Senate provision which omits the word "may": the conferees agree that an exception for any indication of such a threat is sufficient.[228]

[229] Conference Report Filed in House, Oct. 5, 1978, H11673.

[230] Conference Report Filed in House, Oct. 5, 1978, H11673.

> affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[231]

As a matter of criminal law, outside of a limited number of exceptions,[232] the search of an individual's home, office, briefcase, electronic communications, or post, is presumptively "unreasonable", and therefore unconstitutional, unless the government first obtains a warrant from a neutral, disinterested magistrate, 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.[233]

The Fourth Amendment applies to criminal searches within the United States of individuals located within domestic bounds—regardless of their citizenship. It does not apply to non-U.S. persons, who do not have a strong attachment to the United States, for searches conducted by the United States abroad.[234]

Between these two book-ends is a considerable amount of nuance, stemming from (a) whether the search in question is focused on criminal prosecution or foreign intelligence gathering; (b) whether the target of the surveillance is a U.S. person or a non-U.S. person; (c) whether the search takes place within the United States, outside the country, or across U.S. borders; and (d) the extent to which U.S. persons' privacy is implicated as part of incidental intelligence-gathering.[235] These questions all push on the warrant requirement, as well as the reasonableness of the search in question.

In this analysis the unique nature of foreign intelligence matters. Valuable information may (or may not) have anything to do with ordinary criminal activity.[236] A wiretap, for instance, between two foreign powers or their plenipotentiaries may reveal information critical for U.S. foreign policy, such as the likelihood of the overthrow of a foreign ruler, or the outcome of elections in another country. It may also uncover criminal activity, like international drug trafficking or complicity in the same.

With this dual role in mind, traditional FISA explicitly allows for information obtained from wiretaps to be used in criminal prosecutions.[237] The statute thus creates higher protections for U.S. persons, requiring some level of criminal activity, and the insertion of a third-party judicial determination, prior to the introduction of domestic wiretaps. Courts have repeatedly upheld traditional FISA as consistent with the Fourth Amendment.[238]

---

[231] U.S. Const., 4th Amend.

[232] *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).

[233] 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.")

[234] U.S. v. Verdugo-Urquidez, 494 U.S. 259, 274-275 (1990).

[235] A critical consideration in this regard is whether, when, and to what extent the government can tell whether a target is outside the United States. *See* Banks & Kris.

[236] *See also* U.S. v. Belfield, 692 F.2d 141, at 144 n. 8 ("Much valuable intelligence information . . . has nothing to do with the contemplated commission of a crime.")

[237] 50 USC §§1806(k) and 1825(k).

[238] *See, e.g.,* U.S. v. Cavanagh, 807 F.2d 787 (1987) (finding traditional FISA consistent with the Fourth Amendment); 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, 1010-1014 (C.D. Cal. 1985) (holding that traditional FISA does not violate the Fourth Amendment), aff'd. 788 F.2d 566 (9th Cir. 1986); United States v. Megahey, 553 F.Supp. 1180, 1185-92 (E.D.N.Y. 1982) (holding that traditional FISA does not violate the Fourth Amendment); U.S. v. Falvey, 540 F.Supp. 1306, 1311-14 (E.D.N.Y. 1982) (holding that traditional FISA does not violate the Fourth Amendment); US v. Duggan, 743 F.2d

Unlike traditional FISA, §702 allows for surveillance without any particularized suspicion or demonstration of probable cause. The targets need not satisfy traditional FISA's requirements that the targets be foreign powers or agents thereof; instead, *any* non-U.S. person located outside the United States may be monitored, as long as the programmatic purpose is to acquire foreign intelligence information.

In addition, unlike traditional FISA, the court's role is extremely limited.[239] FISC neither reviews nor approves of individual targeting determinations. Neither does it consider the specific facilities to be placed under surveillance. The FAA exempts the government from having to provide the court with a description of the "facilities, places, premises, or property" where surveillance will be conducted.[240] Instead, the court merely verifies that the government has submitted the appropriate certifications, at which point it is required to grant the application. Further searches or "queries" of the data are shielded from judicial oversight: they are conducted solely at the discretion of the intelligence community.

Despite the lack of substantive and procedural safeguards, information obtained from §702 may (with notice to the "aggrieved party") be used in criminal prosecution. Such information may include individuals' thoughts, beliefs, and relationships—arguably some of the most intimate information about individuals. In light of the privacy interests implicated by the interception of content, question exists about the constitutionality of §702.

The executive branch attempts to circumvent Fourth Amendment concerns by pointing to the foreign intelligence components of the surveillance underway. It cites in support the Supreme Court's recognition in 1972 that the domestic surveillance of foreign powers and their agents may merit a different Fourth Amendment standard, as well as circuit courts' efforts to implement the Supreme Court's approach. These arguments are not persuasive.

As an expression of a domestic foreign intelligence exception to the warrant requirement, these cases, without exception, predated traditional FISA. In the thirty-six years that have since elapsed, not a single case has found a domestic foreign intelligence exception.

Pari passu, as a matter of the international intercept of U.S. persons' communications, practice and precedent prior to the FAA turned on a foreign intelligence exception to the warrant requirement that derived from the President's foreign affairs powers. (Criminal investigations overseas also did not require warrants.) This exempted such searches from the warrant requirement. Nevertheless, the courts required the search of U.S. persons overseas to be consistent with the Fourth Amendment requirement of reasonableness.

Congress has since introduced more stringent safeguards for U.S. persons targeted for foreign intelligence purposes via §§703 and 704 of the FAA. With regard to the targeting of U.S. persons overseas, the situation is thus analogous to that which pre-dated FISA: i.e., while the practice prior to the FAA may have recognized an exception with regard to U.S. persons overseas, Congress' determination in 2008 altered the calculus.

Further concerns are raised by the incidental collection of U.S. persons' domestic communications. In defaulting to §702 and, in the process, knowingly obtaining "tens

---

59, 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.");

[239] *See* In re Proceedings Required by §702(I) of the FISA Amendments Act of 2008, No. Misc. 08-01, 2008 WL 9487946, at *2 (FISC Aug. 27, 2008) (describing FISC's role as "narrowly circumscribed.")

[240] 50 USC §1881a(g)(4).

of thousands" of entirely domestic conversation, a colorable argument can be raised that the executive is bypassing Congress's statutory requirements. Although statutorily required, the extent to which notice actually enters the picture is exceedingly limited. As a constitutional matter, acknowledging that the President and Congress share foreign affairs powers, the executive branch's persistent use of §702 with regard to both the international and domestic intercept of U.S. persons' communications may be regarded in Justice Jackson's third category under *Youngstown Sheet and Tube Co. v. Sawyer*.[241] In its exercise of §702, the NSA is purposefully interpreting the statute in a manner that undermines Congress' inclusion of §§703-704.

A. Criminal Prosecution and the Collection of Foreign Intelligence

The criminal law standard for electronic intercepts derives from *Katz v. United States*, 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."[242] 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.[243]

The "presence or absence of a physical intrusion" mattered naught.[244] Wiretapping transgressed the reasonable expectation that the government would not intercept telephone calls. Thus, in order to act within the contours of the Fourth Amendment, the government must first obtain a warrant, based on a judicial finding of probable cause.

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 (e.g., criminal law, domestic security, foreign intelligence, and military), the legal status of the individuals whose conversations are being intercepted (i.e., U.S. person v non-U.S. person), or the location of the search and seizure (i.e., whether the interception takes place wholly within the United States, between the United States and overseas, or entirely overseas).

1. Criminal law and Domestic Security within the United States

Following *Katz*, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act to govern domestic telephone wiretaps for ordinary criminal investigations.[245] 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 for the belief that the facilities to

---

[241] Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952).
[242] Katz v. United States, 289 U.S. 347 (1967).
[243] Katz v. United States, 389 U.S. 347, 351 (1967) (citation omitted).
[244] *Id.* at 353.
[245] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III § 802, 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510-20 (2000)).

be placed under surveillance are to be used in conjunction with the enumerated offense or by the individual suspected of criminal wrongdoing. [246] The officer applying for the warrant must establish that normal investigative procedures have been tried and have failed, or reasonably appear to be unlikely to succeed if tried or to be too dangerous.[247] The applicant must specify the person, location, and type of communications, as well as the length of the interception (with a 30 day limit).[248]

The legislation restricts wiretaps to the investigation of twenty-six specified crimes, including, *inter alia*, espionage, sabotage, treason, murder, kidnapping, extortion, and counterfeiting—all of which, incidentally, are associated with terrorism and threats posed to public safety. The statute, however, does not claim jurisdiction over questions of national security:

> Nothing contained in this chapter 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.[249]

Questions about what standard, exactly, should govern national security (as opposed to ordinary criminal law) arose both in *Katz* and during Congress' passage of Title III.

Justice Byron White, in his concurrence in *Katz*, suggested that the presumption against warrantless searches could be overcome by pressing need. He wrote,

> 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.[250]

Justice William O. Douglas, joined by Justice William J. Brennan, strongly objected, pointing to a certain conflict of interest: "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." [251] For Douglas, to the executive branch was given the responsibility of "vigorously investigat[ing] and prevent[ing] breaches of national security and prosecut[ing] those who violate pertinent federal laws."[252] This hardly qualified for neutral observation. Such a structural, or interest-based analysis did not change in the face of the different types of challenges potentially faced by the government:

> 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

---

[246] *Id. See also* Wayner LaFave, Jerold H. Israel, Nancy J. King, and Orin S. Kerr, *Overview of Obtaining and Executing Wiretap Orders*, 2 Crim. Proc. 4.6(c)(3d ed.).
[247] *Id.*
[248] *Id.*
[249] 18 U.S.C.A. §2511(3).
[250] *Katz*, 389 U.S. at 358, 363-64 (White, J., concurring).
[251] *Id.* at 359 (Douglas, J., concurring).
[252] *Id.* at 359-60 (Douglas, J., concurring).

> rights is assured when the President and Attorney General assume both the position of adversary-and-prosecutor and disinterested, neutral magistrate.[253]

Dicta notwithstanding, *Katz* did not settle the question of the Fourth Amendment standard for surveillance by the intelligence community. When it passed Title III, Congress, in turn, specifically excepted "national security" from the statute's remit.[254]

In 1972, the Supreme Court addressed the question of how to treat national security in relation to the warrantless wiretapping of three individuals suspected of conspiring to bomb the Central Intelligence Agency.[255] In *U.S. v. U.S. District Court*, the Supreme Court held that government officials were required to obtain a warrant prior to engaging in electronic surveillance even where national security was on the line. 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 surveillance.[256]

Justice Powell, writing for the Court, noted that new technologies presented a double-edged sword: while the government had the responsibility of ensuring the safety of the people—and it would be "contrary to the public interest" for the Government to deny itself the use of new technologies that could be used against it, neither was it in the people's best interest to give the government untrammelled access to technology.[257] There may be some exceptions to the warrant requirement, but this was not one of them.

Powell's arguments echoed those of Douglas in *Katz*: the duty of the state to protect itself has to be weighed against "the potential danger posed by unreasonable surveillance to individual privacy and free expression."[258] Nevertheless, "Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch."[259]

The Court was careful to limit its decision to cases involving "the domestic aspects of national security", adding, "We 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."[260] The showing necessary under the Fourth Amendment to justify surveillance in the context of national security may not be analagous to the cirminal investigation standard of probable cause.[261] Powell wrote,

---

[253] *Id.* at 360 (Douglas, J., concurring).
[254] Omnibus Crime Control Act, § 802 (codified as amended at 18 U.S.C. §2511(3)); *see also* PHILIPPA STRUM, PRIVACY: THE DEBATE IN THE US SINCE 1945 141-44 (1998).
[255] United States v. U.S. District Court, 407 U.S. 297 (1972).
[256] United States v. United States Dist. Court, 407 U.S. 297, 308 (1972).
[257] 407 U.S. at 312. (Powell, J., writing, "The marked acceleration in technological developments and sophistication in their use have resulted in new techniques for the planning, commission, and concealment of criminal activities. It would be contrary to the public interest for Government to deny to itself the prudent and lawful employment of those very techniques which are employed against the Government and its law-abiding citizens." The most basic function of the government is to provide for the security of the individual, "But a recognition of these elementary truths does not make the employment by Government of electronic surveillance a welcome development. . . There is, understandably, a deep-seated uneasiness and apprehension that this capability will be used to intrude upon cherished privacy of law-abiding citizens.")
[258] *Id.* at 314-15.
[259] *Id*. at 316-17. *See also* Abel v. United States, 362 U.S. 217, 219-220 (1960) ("[T]he nature of the case, the fact that it was prosecution for espionage, has no bearing whatever upon the legal considerations relevant to the admissibility of evidence.")
[260] *Id.,* at 321-322.
[261] *Id.,* at 322.

> [A] [d]ifferent srtandard[] [of probable cause] may be compatible with the Fourth Amendment if [it is] reasonable both in relation to the legitimate need of Government for intellignece information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be ienforced and the nature of citizen rights deserving protection.[262]

In this calculus, probable cause was to be weighed against the Fourth Amendment's reasonableness standard.[263]

2. Foreign Intelligence Gathering within the United States

Congress responded to *US v. US District Court* by enacting FISA.[264] The legislature sought to balance the government's legitimate interest in protecting national security against the individual right to privacy protected by the Fourth Amendment.[265] The statute thus premised surveillance gathering on the targeting of foreign powers or their agents—terms synonymous with foreign governments and individuals working on behalf of foreign countries.[266] To the extent that U.S. persons came within the definition, Congress required the government to demonstrate some level of criminality and to submit to procedural protections that approximated the Fourth Amendment warrant requirement.

Traditional FISA defines "foreign power" as:

> (1) a foreign government or any component thereof, whether or not recognized by the United States;
> (2) a faction of a foreign nation or nations, not substantially composed of United States persons;
> (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
> (4) **a group engaged in international terrorism or activities in preparation therefor**;

---

[262] *Id.,* at 322-23.

[263] *Id.,* at 323 ("In cases in which the Fourth Amendment requires that a warrant to search be obtained, 'probable cause' is the standard by which a particular decision to search is tested against the constitutional mandate of reasonableness." (Quoting Camara v. Municipal Court, 387 U.S. 523, 534 (1967)).

[264] *See, e.g.,* remarks by Mr. Kastenmeier, House Consideration and Agreement Conference Report on FISA, Oct. 12, 1978, H. 12534 "Mr. Speaker, it has now been over 6 years since the Supreme Court in the famous Kieth 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. . . 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. . .")

[265] S. Rep. No. 604 (Part I), 95th Cong., 2d Sess. 7-9, *reprinted in* 1978 U.S. Code Cong. & Ad. News 3904, 3908-10.

[266] National Security Communications Intelligence Directive 9 defined "foreign communications" as "all communications and related materials . . . of the government and/or their nationals or of any military, air, or naval force, faction, party, department, agency, or bureau of a foreign country, or of any person or persons acting or purporting to act therefor." NSCID No. 9 (Jul. 1, 1948) (National Archives and Records Administration, RG 59, Records of the Department of State, Records of the Executive Secretariat, NSC Files: Lot 66 D 195)

(5) a foreign-based political organization, not substantially composed of United States persons;
(6) an entity that is directed and controlled by a foreign government or governments; or
(7) an entity not substantially composed of United States persons that is **engaged in the international proliferation of weapons of mass destruction**.[267]

What this definition means is that, outside of actual foreign entities, some element of criminal activity is required for individuals or groups to be considered within the reach of foreign intelligence gathering. "International terrorism", for instance, means activities that:

(1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;
(2) appear to be intended—
  (A) to intimidate or coerce a civilian population;
  (B) to influence the policy of a government by intimidation or coercion; or
  (C) to affect the conduct of a government by assassination or kidnapping; and
(3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.[268]

For a U.S. entity to be considered a foreign power within the meaning of (4), above, it must be engaged in international, violent acts indended to intimidate civilians or the government. Similarly, the proliferation of WMD, which captures U.S. persons in its remit under (7), above, is a criminal act.

An "agent of a foreign power", in turn, refers to any person *other than a United States person*, who –

(a) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;
(b) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities. 50 USC §1801(b) (2006 & Supp. V 2011).

[267] 50 USC §1801 (emphasis added).
[268] 50 USC §1801(c).

This first part of the definition of an agent of a foreign power tracks the traditional understanding of foreign powers and their intermediaries as non-U.S. persons.

The second part of the definition includes *any* individual—including a U.S. 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; 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 knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or C).[269]

The acts that qualify U.S. persons as agents of foreign powers, highlighted in bold, like those that fold U.S. persons into the definition of foreign powers, are criminal in nature. The first and second sections [(a) and (b)] require a violation of a criminal statute. Language in the statute referring to "sabotage" is defined as a crime—i.e., "activities that involve a violation of [18 USC 105], or that would involve a violation if committed against the United States."[270] Section (c), above, would also require individuals to assume a false or fraudulent identity upon entering the United States—which will almost always be a crime because of the statutory regime governing customs and border entry.

Under traditional FISA, Congress thus requires not only that some level of criminality be involved for U.S. persons to be targeted, but that the government demonstrate probable cause that U.S. persons come within one of the above categories. The standard is slightly different than, but has largely the same effect as, the standards required under Title III, also known as the Wiretap Act.[271]

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. These definitions are central to traditional FISA: the definition of "foreign power", for instance, anchors

---

[269] 50 USC §1801(b) (2006 & Supp. V 2011) (emphasis added).
[270] 50 USC §1801(c).
[271] Title III, at the time of its passage, regulated government interception of the contents of oral and wire communications involving the human voice (i.e., 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* Wiretap Act, 18 USCA §§2510-22; Stored Communications Act 18 USC §§2701-11; and Pen Register Statute, 18 USC §§3121-27.

"foreign intelligence information". [272] The legislation also requires that the government establish probable cause that the target is likely to use the facilities to be placed under surveillance. For Congress, the requirement of an application to an independent magistrate, supported by probable cause, met the Fourth Amendment warrant requirements for foreign intelligence.

In criminal prosecution cases the Courts have consistently upheld FISA orders as constitutional. In *U.S. v. Cavanagh*, for instance, a defendant was indicted for attempting to deliver defense information to a foreign government.[273] His effort to suppress the fruits of the search, conducted under traditional FISA, met with zero success: the 9th 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 probable cause and particularity.[274] Similar challenges have met with the same result.[275]

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), FISC 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*, FISCR 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.[276]

B. The Domestic Foreign Intelligence Exception to the Warrant Requirement

Prior to Congress' introduction of traditional FISA, the lower courts, looking to the language in *U.S. v. U.S. District Court*, carved out a foreign intelligence exception to the warrant requirement for domestic surveillance applied to foreign powers and their agents. Most of 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.

Congress, however, shares foreign affairs authorities with the executive branch. In enacting FISA the legislature made it clear that the statute would serve as the sole means via which the executive branch would be allowed to conduct domestic foreign intelligence surveillance. In the thirty-six years that have since elapsed, not a single case has found a domestic foreign intelligence exception to the warrant requirement.

---

[272] 50 USC §1801(e).

[273] U.S. v. Cavanagh, 807 F.2d 787 (1987).

[274] *Id.*

[275] *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, 1010-1014 (C.D. Cal. 1985) (holding that traditional FISA does not violate the Fourth Amendment), aff'd. 788 F.2d 566 (9th Cir. 1986); United States v. Megahey, 553 F.Supp. 1180, 1185-92 (E.D.N.Y. 1982) (holding that traditional FISA does not violate the Fourth Amendment); U.S. v. Falvey, 540 F.Supp. 1306, 1311-14 (E.D.N.Y. 1982) (holding that traditional FISA does not violate the Fourth Amendment); US v. Duggan, 743 F.2d 59, 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."); U.S. v. Rosen, 447 F.Supp. 2d 538 (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).

[276] In re Sealed Case, 310 F.3d 717 (Foreign Intell. Surveillance 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.")

1. U.S. v Truong

One of the most important cases to arise prior to FISA 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.[277] 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.[278] 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.[279] Surveillance conducted outside of either Title III or FISA subsequently revealed that Truong was receiving the classified materials from Ronald Humphrey, an American citizen working at the United States' Information Agency.[280] Truong and Humphrey were convicted, *inter alia*, of espionage, as well as acting as agents of a foreign government without prior notification to the Secretary of State.[281]

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 intelligence. At the point where the investigation turned criminal in nature, however, any information obtained without a warrant could be suppressed.[282]

The court, distinguishing its holding from *U.S. v. U.S. District Court*, 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." [283] The 4th 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."[284]

The warrant exception thus stemmed from the foreign affairs component of executive power, outwardly directed at protecting U.S. national security.[285] Not only did the executive have the expertise, but, as a constitutional matter, it was the "pre-eminent authority in foreign affairs." [286] Flexibility, practical experience, and constitutional competence worked together to carve out an exception where foreign intelligence matters were concerned.

---

[277] U.S. v. Truong, 629 F.2d 908 (4th Cir.), 1980.
[278] *Id.*
[279] *Id.*
[280] *Id.*
[281] Criminal violations included 18 U.S.C. §§371, 641, 793(e), 794(a), (c), 951-952; and conspiracy to violate 50 U.S.C. §§783(b), (c).
[282] U.S. v. Truong, 629 F.2d 908 (4th Cir.), 1980.
[283] *Id.*, internal citations omitted.
[284] *Id.*, internal citations omitted.
[285] *Id.*, ("The executive branch, containing the State Department, the intelligence agencies, and the military, is constantly aware of the nation's security needs and the magnitude of external threats posed by a panoply of foreign nations and organizations. On the other hand, while the courts possess expertise in making the probable cause determination involved in surveillance of suspected criminals, the courts are unschooled in diplomacy and military affairs, a mastery of which would be essential to passing upon an executive branch request that a foreign intelligence wiretap be authorized.")
[286] *Id.*

The 4th Circuit was careful to limit its holding "to those situations in which the interests of the executive are paramount." [287] This meant that the object of the search or surveillance must be a foreign power or its agents. In other words, the foreign connection was critical. Similarly important was the point at which the surveillance moved to the criminal realm—in this case, the point 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." [288]

2. Precedent, History, and Practice

Other circuit courts, applying *U.S. v. U.S. District Court* ("*Keith")* prior to Congress' enactment of FISA, similarly affirmed the existence of a domestic foreign intelligence exception to the warrant clause.[289] These cases all involved individuals with a nexus to foreign countries. They grounded the exception in the President's foreign affairs powers. And, like *Truong*, even as the courts found an exception, they nevertheless considered the Fourth Amendment's reasonableness requirement to apply.

In *United States v. Butenko*, the 3rd Circuit recognized that the Constitution accorded the President foreign affairs powers.[290] It simultaneously recognized the danger of allowing the Fourth Amendment analysis "to be abandoned whenever the President asserts that a particular search and seizure is incident to the conduct of foreign affairs." [291] 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." [292]

The Court read the Fourth Amendment as (a) requiring that all searches and seizures, even if authorized by a warrant, meet the reasonableness requirement. At a minimum, this meant that some form of probable cause for the search and seizure must exist. Even if a search was thus deemed reasonable, failure to have secured a warrant may still make a search unlawful.[293]

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.[294] The executive branch's decision in the first instance to wiretap the two men stemmed from the President's foreign affairs power:

---

[287] *Id.*
[288] *Id.*
[289] *See, e.g.,* United States v. Butenko, 494 F.2d 593, 606 (3d Cir. 1974) (finding a foreign intelligence exception); United States v. Clay, 430 F.2d 165, 171 (5th Cir. 1970) (upholding warrantless foreign intelligence surveillance); United States v. Brown 484 F.2d 418, 426 (5th Cir. 1973) ("restrictions 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. Buck, 548 F.2d 871, 875 (9th Cir. 1977) (Foreign security wiretaps are a recognized exception to the general warrant requirement."). Note also that the 2nd Cir. and DC Circuit commented on the foreign intelligence exception but did not themselves decide the question.
[290] *Id.* ("The Constitution contains no express provision authorizing the President to conduct surveillance, but it would appear that such power is similarly implied from his duty to conduct the nation's foreign affairs.")
[291] *United States v. Butenko*, 494 F.2d 593, 606 (3d Cir. 1974). See also United States v. Curtiss-Wright, 299 U.S. 304 (1936)(holding as constitutional Congress' delegation to the President of the authority to prevent the sale of weapons to countries engaged in hostilities).
[292] *Id.*
[293] *Id.*
[294] *Id.*

> 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 at uncovering American secrets, and the policy positions of foreign states on a broad range of international issues. [295]

Because the targets in question were tied to foreign powers, they fell within a foreign intelligence exception to the warrant requirement under the Fourth Amendment.

The domestic foreign intelligence exception at issue in *Butenko* finds support in history and practice. The language of Article II and its assignation of (at least some) foreign affairs powers to the executive, as considered by the 1787 Constitutional Convention, centered on the Founders' understanding of institutional competence and national interest. In *Federalist No. 64*, John Jay distinguished between the powers of the Senate in treaty adoption and those of the executive branch in treaty formation on grounds of the latter's ability to "manage the business of intelligence", ensure "secrecy", and act with "dispatch."[296] The power of making treaties was, for Jay, particularly important for foreign relations purposes, "as it relates to war, peace, and commerce."[297] The necessity of giving the executive branch access to the information requisite for negotiating international instruments followed.

Alexander Hamilton, in turn, emphasized the importance of a vigorous, unitary executive: "Energy in the Executive is a leading character in the definition of good government. It was essential to the protection of the community against foreign attacks.[298] In *Federalist No. 74* Hamilton elaborated,

> Of all the cares or concerns of government, the direction of war most peculiarly demands those qualities which distinguish the exercise of power by a single hand. The direction of war implies the direction of the common strength; and the power of directing and employing the common strength, forms a usual and essential part in the definition of executive authority.[299]

It is not just in the service of forming international compacts that foreign intelligence comes into play. It is equally crucial for avoiding conflict and prosecuting war—powers afforded to the President through the Commander-in-Chief authorities.[300]

In 1936, the Supreme Court recognized the power of the federal government generally over foreign affairs, and the inherent authorities of the President, in particular, with regard to U.S. international relations.[301]

> In view of the delicacy of foreign relations and of the power peculiar to the President in this regard, Congressional legislation which is to be made effective in the international field must often accord to [the President] a

---

[295] *Id.*
[296] John Jay, The Federalist No. 64, The Powers of the Senate, Independent Journal, Wed., Mar. 5, 1788.
[297] Id.
[298] Alexander Hamilton, The Federalist No. 70, The Executive Department Further Considered, Independent Journal, Sat., Mar. 15, 1788.
[299] Alexander Hamilton, The Federalist No. 74, The command of the Military and Naval Forces, and the Pardoning Power of the Executive, from the New York Packet, Tues., Mar. 25, 1788.
[300] U.S. CONST., Art. II(1)(1), (2)(1).
[301] United States v. Curtiss-Wright Export Corp, 299 U.S. 304 (1936).

> degree of discretion and freedom which would not be admissible were domestic affairs alone involved.[302]

It was precisely in the realm of foreign affairs, as deeply embedded in the country's external relations, that the President found increased scope of action. For the courts, the Executive's power in the field of foreign affairs includes the power to collect foreign intelligence.[303]

3. FISA and the Elimination of the Domestic Foreign Intelligence Exception

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.[304] It falls to the legislature to declare war.[305] Congress may raise and support armies, provide and maintain a navy, and make rules for the government and regulation of the same.[306] It may call forth and organize the militia.[307] And it may "make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers."[308]

With the constitutional allotment of power in mind, the courts have traditionally recognized executive and legislative preeminence in the field of foreign affairs and afforded the other two branches deference with regard to related questions.[309] This does not mean that foreign affairs powers are unlimited.[310] But it does suggest that on certain matters the judiciary will withdraw from the field to allow the political branches to determine how to proceed. The introduction of the Foreign Intelligence Surveillance Act marks one such moment.

FISA, recognizing the concurrent authorities of the executive and Congress with regard to some aspects of foreign affairs, drew a sharp line at the border of the United States. FISA was to be the sole means via which the executive henceforward conducted domestic foreign intelligence surveillance. During passage of the bill, the House wanted the statute to state that the procedures established under its auspices

---

[302] 299 U.S. 305-306.

[303] United States v. Totten, 92 U.S. 105 (1875)(acknowledging President's power to conduct intelligence gathering operations and to employ spies); Webster v. Doe, 486 U.S. 592 (1988) (O'Connor, J., concurring in part, dissenting in part)(noting that "the functions performed by the Central Intelligence Agency and the Director of Central Intelligence" are "at the core" of the Executive's foreign relations authority).

[304] U.S. CONST., Art. I, §8 (1), (3), (10).

[305] U.S. CONST., Art. I, §8 (11).

[306] U.S. CONST., Art. I, §8 (12), (13), (14).

[307] U.S. CONST., Art. I, §8 (15), (16).

[308] U.S. CONST., Art. I, §8 (18). In light of changing technologies, the traditional reliance on foreign and domestic as an aspect of foreign intelligence collection is proving inapposite for Constitutional analysis. More work needs to be done on this front to understand the Constitutional implications of the global communications infrastructure.

[309] *See, e.g.,* Chicago & Southern Air Lines, Inc. v. Waterman S.S. Corporation, 333 U.S. 103 (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"); U.S. v. Curtiss-Wright, 299 U.S. 304 (1936) (noting the "very delicate, plenary and exclusive power of the President as the sole organ of the federal government in the field of international relations.")

[310] *See, e.g.,* U.S. 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); United States v. Curtiss-Wright, 299 U.S. 304, 320 (1936) (foreign affairs powers of the President "must be exercised in subordination to the applicable provisions of the Constitution").

represented the "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 Sheet & Tube Co. v. Sawyer*.[311] The Senate view carried.[312]

Concurrent authorities meant that the scope of action available to either party in some sense rested on the actions of the others. This lay at the heart of the Founders' concept of separation and balance of powers. Accordingly, Jackson's third category contemplates the potential for the President to undertake measures "incompatible with the expressed or implied will of Congress."[313] 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."[314] 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.[315]

In *Dames & Moore v. Regan*, the Court went on to identify a three-part test based on Jackson's analysis in *Youngstown*.[316] In 1978 Congress went even further: FISA repealed the limitation previously noted in Title III, suggesting that Congress did not intend to limit the President's constitutional authorities.[317]

---

[311] Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952).

[312] *See also* Conference Report Filed in House, Oct. 5, 1978, at H 11683 ("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.'")

[313] Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635 - 638 (1952).

[314] Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 638 (1952).

[315] Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635 - 638 (1952).

[316] Dames & Moore v. Regan, 453 U.S. 654, 668-669 (1981).

[317] See FISA, § 201, repealing 18 U.S.C.A. § 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."; FISA Senate Judiciary Report at 17 ("Most importantly, the disclaimer in 18 U.S.C.A. § 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* U.S. v. Torres,

In order, then, for the Courts to overturn FISA, they must disavow a significant amount of foreign affairs powers to Congress—a step the judiciary would be highly reluctant to take. Accordingly, in the 36 years that have elapsed since the introduction of FISA, the Courts have not once upheld a domestic foreign intelligence exception to the warrant requirement. Instead, it is to FISA itself that the Courts look to establish the Fourth Amendment standard for the warrant requirement when domestic foreign intelligence collection is of moment. Every challenge to traditional FISA on Fourth Amendment grounds has failed.

Many of the protections in traditional FISA are absent from §702. Judicial decisions upholding the constitutionality of traditional FISA, moreover, center on the *targeting* of U.S. persons and non-U.S. persons within the United States. They do not involve the *incidental* collection of U.S. and non-U.S. persons domestic communications; nor do they contemplate the subsequent use of incidentally-collected material in criminal prosecution. I return to this point, below.

C. Application of the Fourth Amendment Overseas

The Supreme Court has held that 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.[318] The reasoning underlying this decision raises difficult issues with regard to §702 authorities. While the court has provided little guidance on the nature of the connection, an appropriate approach would be to require a valid legal relationship indicating membership in the political community. Either physical contact or a virtual presence are insufficient to satisfy the test. On the flip side, where U.S. persons are in contact with non-U.S. persons, the courts should recognize that individuals do not, merely by engaging in global communications, waive their right to the protections of the Fourth Amendment. That is, virtual connectivity does not divest U.S. persons of their rights under the Constitution.

1. *Verdugo-Urquidez*

In *United States v. 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.[319] Rehnquist's reading stemmed from a deeply Aristotelian approach: i.e., one that emphasizes membership in the polis (πόλις), or political community, as a concomitant of forming a structure of government.[320] As the politas (πολίτης), 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."[321]

---

751 F.2d 875, 882 (7th Cir. 1984); U.S. v. Biasucci, 786 F.2d 504, 508, n. 4 (2d Cir. 1986) (noting exclusivity intent of Congress).

[318] U.S. v. Verdugo-Urquidez, 494 U.S. 259 (1990).

[319] U.S. v. Verdugo-Urquidez, 494 U.S. 259, 265 (1990) (Rehnquist, C.J.)

[320] ARISTOTLE, POLITICS, Book I (350 BC), trans. by Benjamin Jowett, available at http://classics.mit.edu/Aristotle/politics.1.one.html; available in the original Greek at http://www.perseus.tufts.edu/hopper/text;jsessionid=91A85450747C74DF609D266E0A8DF8E5?doc=Perseus%3atext%3a1999.01.0057.

[321] 494 U.S. at 265 (Rehnquist, C.J.).

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."[322] Instead, Kennedy relied on a more practical argument to find 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.[323]

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.[324] Beyond this confusion, very few cases address precisely what constitutes sufficient connections to the United States to satisfy the "substantial connections" aspect of the majority's decision. Those that do point in seemingly different directions.[325]

In *Martinez-Aguero v. Gonzalez*, for instance, a Mexican national, with an expired visitor's visa to the United States, went to the U.S. consulate in Mexico to obtain a new visa.[326] Directed to treat the visa as sufficient until the new one arrived, the woman came to the United States to visit her mother. Searched at the border, the Fifth Circuit determined that she had sufficient connections to the United States to benefit from the protections of the Fourth Amendment.[327] In contrast, another 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 to the United States 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.[328]

At the outside, the conclusion that a foreign national who lives *external* the United States, and who *enters* the United States 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.[329] In both cases, the aliens' connections with the U.S. 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

---

[322] U.S. v. Verdugo-Urquidez, 494 U.S. 259, 278 (1990) (Kennedy, J.).

[323] *Id.* See also discussion in Orin Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. (forthcoming 2015), p. 8.

[324] *Compare, 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 (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).

[325] Kerr, *supra* note 323, at 8-9.

[326] Martinez-Aguero v. Gonzalez, 459 F.3d 618 (5th Cir. 2006).

[327] *Id.*

[328] United States v. . Esparza-Mendoza, 265 F.Supp.2d 1254 (D.Utah 2003).

[329] 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.*

unlawfulness been, for instance, 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 to the United States, then geographic location may prove the most critical question.

The lack of clarity at the margins has implications for targets of surveillance under §702. To the extent that the connections to the United States are lawful in regard to citizenship or residency (i.e., the target is either lawfully present in domestic bounds 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 §§703-704 addresses U.S. persons overseas.[330]

A critical gap in Constitutional jurisprudence, and in understanding the application of §702, lies with a third class of individuals, who may have a substantial connection to the United States 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 country—indeed, their actions may be critical to U.S. 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.[331] For him, online contacts with U.S. servers amount merely to a "'fortuitous' circumstance of where the Internet provider happens to locate the servers."[332] Customers may 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."[333] It was not meant to prevent the Federal Government from acting against aliens outside the United States.[334] The community that formed "the people" are not just accidental members of the *politas*. Indeed, they rely on the Constitution to protect them from the state.[335]

This reading of "the people" appears to be right. But unlike Kerr, at least insofar as one considers Fourth Amendment protections as a threshold matter, I would

---

[330] 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 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).

[331] Kerr, *supra* note 323, at 18-21.

[332] Kerr, *supra* note 323, at 21.

[333] 494 U.S. at 266.

[334] Id., at 266-27. *See also* Kerr, *supra* note 323, at 20.

[335] *See also* Kerr, *supra* note 323, at 21.

consider the legal relationship paramount, and I would limit it to a legal relationship establishing the relationship between the individual and the political community. That is, an individual constituting "the people" may or may not be present within the country; but it is the legal framing, stemming from constitutional tenant of organization of the political entity, that creates the right.

The difficulty, for §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.[336] "[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."[337] 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 §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.[338] Foreign persons could become avid Amazon.com users, communicate with associates in the United States via Verizon, and take online 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 possible 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.

There is a *real politic* argument to be made as well: namely, U.S. failure to ensure privacy protections will 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 §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.[339] 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.[340] 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.[341]

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

---

[336] 494 U.S. at 276 (Kennedy, J., concurring). *See also* Kerr, *supra* note 323, at 21.
[337] *Id*., at 277.
[338] Kerr, *supra* note 323, at 22.
[339] *IT Industries Set to Lose Billions Because of Privacy Concerns*, UPI, Dec. 17, 2013, available at http://www.upi.com/Business_News/Security-Industry/2013/12/17/IT-industries-set-to-lose-billions-because-of-privacy-concerns/UPI-30251387333206/. (""Information technology companies stand to lose billions of dollars of business because of concerns their services are neither secure nor private.")
[340] *Id. See also* Mary DeRosa, *Tech Insider* (reporting estimates of losses of $22 billion over the next three years).
[341] *Id.*

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 thus 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, both the rationale of the Rehnquist opinion and the Kennedy concurrence can be read as compatible with not extending Fourth Amendment rights to individuals lacking a legal relationship (i.e., those stemming directly from the individual's status as a member of the political community).[342]

This was the crux of President Obama's effort to reassure the international community in January 2014 that the U.S. would not use its (legal) authority to collect trade secrets simply to advantage U.S. corporations.[343] In PPD-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.[344]

But 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' concern about reverse targeting—namely, that the intelligence community will use §702 to target non-U.S. persons overseas, as a back door to gaining access to U.S. persons' communications. (See discussion, *infra)*.

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-end, U.S. persons are entitled to protections.[345] 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. That is, it does not hinge constitutional protections

---

[342] *See also* Kerr, *supra* note 323, at 23 ("To ensure that the role of the Fourth Amendment maintains its preexisting balance as technology changes, the courts should hold that purely virtual contacts with the United States cannot establish Fourth Amendment rights.")

[343] *See, e.g.,* PPD-28, §1(c) (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.")

[344] PPD-28, §4.

[345] For lengthy discussion of the question of search and seizure in light of *Verdugo-Urquidez*, *see* Kerr, *supra* note 323, at 21. pp. 27-32.

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. In the first place, this rule assumes that individuals have control over whether their communications leave domestic bounds. They do not. The Internet, for instance, for purposes of email, is constructed to find the most efficient route between two ISP addresses. This means that even wholly domestic communications may be routed internationally. Individuals have no control over how their messages are conveyed. In the second place, 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, he or she loses constitutional protections in the content of those communications. This would simply eviscerate the meaning of the Fourth Amendment. That is, virtually no communications would benefit from the protections of the Fourth Amendment.

The Court can avoid this conclusion by underscoring the status of the individual as Rehnquist articulated for the majority in *Verdugo-Urquidez*: i.e., by emphasizing membership in the political community. Where established, the protection of the Fourth Amendment applies. At least insofar as the individual with the substantial connection to the United States are concerned, such protections come into play.

2. 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.[346] 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 12333 provided for the same for U.S. persons.

Accordingly, prior to the FAA, lower Courts found the absence of a prior warrant for electronic intercepts conducted abroad for criminal investigations to be consistent with the Fourth Amendment.[347] There were no statutes on point. Title III has no extraterritorial force.[348] The Federal Rules of Criminal Procedure (F.R.C.P.), in turn, limit the jurisdiction of federal magistrates.[349] While 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

---

[346] William F. Brown and Americo R. Cinquegrana, Warrantless Physical Searches for Foreign Intelligence Purposes: Executive Order 12333 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. ")

[347] *See, e.g.,* U.S. v. Peterson, 812 F.2d 486, 492 (9th Cir. 1987).

[348] 18 U.S.C. §2518. See also 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); U.S. v. Peterson, 812 F.2d 486, 492 (9th Cir. 1987).

[349] F.R.C.P., Rule 41(a)(governing domestic law enforcement investigations).

Amendments to the F.R.C.P. noted that, "it was unclear how federal officers might obtain warrants authorizing searches outside the district of the issuing magistrate.[350] In the absence of statutory guidance, Courts relied upon a constitutional analysis.

In *U.S. v. Barona*, the 9th Circuit recognized that U.S. persons based overseas are covered by the Fourth Amendment—but only insofar as the search in question meets the standard for reasonableness. The warrant clause proved inapposite.

Barona stemmed from a Drug Enforcement Agency operation ("Operation Pisces"), conducted at the height of the war on drugs, 1985-1987.[351] Wiretaps led to the eventual conviction of individuals for involvement in the worldwide distribution of cocaine. The Court noted that neither the Fourth Amendment "nor the judicially created exclusionary rule applies to acts of foreign officials."[352] Only two "very limited exceptions"[353] might apply: first, "if the circumstances of the foreign search and seizure are so extreme that they 'shock the [judicial] conscience,'" [354] (a consideration stemming from the judiciary's supervisory powers, employed to ensure "the integrity of the criminal justice system"[355]); and, second, where U.S. agents' participation "is so substantial that the action is a joint venture between United States and foreign officials."[356] 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.[357]

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.[358] Like *Barona*, the decision pre-dated the FAA. In *U.S. v. Bin Laden*, the Southern District of New York 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.[359] (The intercepts had been approved by the Attorney General in 1997.)[360] The Court considered the costs of imposing a warrant requirement on surveillance conducted overseas—a consideration akin to exceptions to the warrant requirement in domestic criminal law.[361] The Court

---

[350] U.S. v. Peterson, 812 F.2d 486, 492 (9th Cir. 1987). *See also* U.S. v. Toscanino, 500 F.2d 267, 280-81 (2d Cir. 1974); Berlin Democratic Club v. Rumsfeld, 410 F.Supp. 144 (D.D.C. 1976).
[351] U.S. v. Barona, 56 F.3d 1087 (9th Cir. 1995).
[352] United States v. LaChapelle, 869 F.2d 488, 489 (9th Cir. 1989), quoting U.S. v. Maher, 645 F.2d 780, 782 (9th Cir. 1981).
[353] 869 F.2d at 489.
[354] 869 F.2d at 490, quoting Rose, 570 F.2d at 1362.
[355] U.S. v. Barona, 56 F.3d 1087, 1090 (9th Cir. 1995).
[356] 869 F.2d at 490.
[357] U.S. v. Barona, 56 F.3d 1087, 1090 (9th Cir. 1995).
[358] U.S. v. Bin Laden, 126 F.Supp. 2d 264 (S.D.N.Y. 2000).
[359] *Id.*
[360] *Id.*
[361] *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); 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); Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 619 (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."); 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.") Cf. Terry v. Ohio, 392 U.S. 1 (1968) (upholding patdowns for weapons to protect officer safety during stops).

reasoned by analogy that a similar "special needs" exception existed with regard to foreign intelligence conducted overseas.[362] 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.[363] The Court further recognized the potential for breaches of security in requiring a warrant prior to foreign intelligence collection overseas.[364]

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' communications.[365] Thus, just as in *Truong* and *Butenko*, in the absence of direction from Congress, the executive, in its exercise of foreign affairs powers, had greater leeway to decide whether and to what extent it engaged in overseas foreign intelligence gathering.[366] 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*.[367]

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

---

[362] U.S. v. Bin Laden, 126 F.Supp. 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; Hon. Peter Hoekstra, Chairman, Permanent Select Committee on Intelligence U.S. House of Representatives, Hon. John D. Rockefeller, Vice Chairman, Senate Select Committee on Intelligence, Hon. Jan Harman, Ranking Minority Member, Permanent Select Committee on Intelligence, U.S. House of Representatives, Washington, D.C., Dec. 22, 2005, p. 4, available at http://www.justice.gov/ag/readingroom/surveillance6.pdf .

[363] U.S. v. Bin Laden, 126 F.Supp. at 274-275,

[364] U.S. v. Bin Laden 126 F.Supp. at 275.

[365] U.S. v. Bin Laden 126 F.Supp. at 275 ("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.")

[366] *See, e.g.,* Truong, 629 F.2d at 915 and Butenko, 494 F.2d at 606.

[367] U.S. v. Bin Laden, 126 F. Supp. at 277 (emphasis in original).

Like *Truong*, *U.S. v. 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, however, 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."[368]

In 2008 the Foreign Intelligence Court of Review found a similar foreign intelligence exception to the warrant requirement.[369] 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 AG 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.)[370] In one of the few challenges in FISC to §702 or its antecedents (as publicly known), a telecommunications provider challenged the PAA on Fourth Amendment grounds.

Although the telecommunications 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.[371] 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.[372] 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.[373]

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.[374]

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

---

[368] U.S. v. Bin Laden, 126 F.Supp. at 278.
[369] In re: Directives [REDACTED] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, Aug. 22, 2008 (Selya, C.J.), available at http://www.fas.org/irp/agency/doj/fisa/fiscr082208.pdf.
[370] Compare the Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (repealed July 10, 2008) and the FISA Amendments Act of 2008, Pub. L. No. 110-261, Section 403, 122 Stat. 2436, 2473 (2008). *See also* discussion, *infra*.
[371] The statute had been "applied to the petitioner in a specific setting." *In re Directives*, p. 11.
[372] 310 F.3d at 741-42.
[373] In re Directives, pp. 14-15 ("The question, then, is whether the reasoning of the special needs cases applies by analogy to justify a foreign intelligence exception to the warrant requirement for surveillance undertaken for national security purposes and directed at a foreign power or an agent of a foreign power reasonably believed to be located outside the United States.")
[374] In re Directives, p. 15.

> [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.[375]

Since the executive branch stated that the programs in place were to protect against 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."[376]

In re Directives, like *U.S. v. Bin Laden*, was decided prior to the FAA and Congress' introduction of §§703-704. 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 the question of the incidental collection of information.

D. To/From or About and Incidental Collection

The foregoing case law centers on the targeting of U.S. persons and non-U.S. persons within the United States and overseas. The NSA's interpretation of the statutory language, however (to include information to/from, or about the target) allows the agency to collect the communications of individuals not themselves the target of foreign intelligence gathering, and, where criminal behavior is found, to use information in subsequent third-party prosecution.

Three important constitutional concerns in relation to the warrant clause follow. First, the practice results in the *de-facto* targeting of U.S. persons at home and abroad in a manner that runs contrary to the constitutional standards set by the courts and by Congress. Second, the use of information incidentally obtained through foreign intelligence collection in criminal prosecution, absent further judicial involvement, risks creating a way to bypass carefully-constructed restrictions in criminal law. Third, further query of the data obtained through §702 amounts to a search. Even if the information is obtained at the front end in a manner consistent with the Fourth Amendment, constitutional questions may still be still entailed in how the information is accessed and analyzed.

1. *De-facto* targeting and Criminal Prosecution

Criminal law and traditional FISA reflect the view shared by Congress and the Courts that wiretapping represents a particularly intrusive form of surveillance. Resultantly, both statutes include a necessity requirement. For the former, prosecutors must address "whether or not other investigative procedures have been tried and failed

[375] In re Directives, p. 16.
[376] In re Directives, p. 17.

or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous."[377] Under traditional FISA, certification accompanying the application for an order must attest that the information being sought is foreign intelligence and that such information could not reasonably be obtained by normal investigative means.[378] Both statutes raise the bar for who may obtain an intercept. Unlike an ordinary search warrant application, which can be submitted by any law enforcement officer, Title III requires that the application be authorized by a high-level official.[379] Traditional FISA also requires that the application be approved by a high-ranking official.[380] Both statutes demand that the government obtain authorization from a judge of a U.S. district court or a U.S. court of appeals prior to collecting information.[381] For both Title III and traditional FISA, inquiry is conducted on a case-by-case basis, with the courts approving the individual to be targeted. In addition, the standard applied in both contexts is one of probable cause (albeit with different objects to which the standard is applied).

In addition to the foregoing considerations, and reflective of the highly intrusive nature of the interception of the contents of communications, both statutes limit the government's actions to the interception of communications directly tied to the target. Title III thus requires that an interception be executed "in such a way as to minimize the interception of communications not otherwise subject to interception."[382] This requirement echoes the Court's holding in *Berger v. New York*, a case that invalidated a state wiretapping statute in part because it allowed the government to seize "the conversations of any and all persons coming into the area covered by the device . . . indiscriminately and without regard to their connection to the crime under investigation."[383]

Traditional FISA approaches wiretaps in much the same manner as criminal law: the applicant must demonstrate to FISC probable cause that the individual is a foreign power or an agent thereof, and likely to use the particular facilities to be placed under surveillance. The government may not simply begin casting about for information related to the target of an order under traditional FISA by scanning domestic communications. The purpose behind FISA in 1978 was to prevent precisely this type of search from occurring. Traditional FISC also ensures that minimization procedures are in place. Where evidence of criminality is found, FISA may lead to criminal prosecution. At this point, however, particularized suspicion, insertion of a neutral magistrate, and demonstration of probable cause has already been inserted into the process, making referral for prosecution constitutional.

The addition of §§703 and 704 indicate that in 2008 Congress continued to emphasize the importance of particularized targeting and use of third party judicial intervention. Where the target is a U.S. person, an order from FISC must be obtained *prior* to the interception of the target's communications. The statute is silent on the standard that must be applied in determining whether the target is a U.S. person and/or based overseas—an omission that has led the NSA, as noted above in relation to §702, to assume, absent information to the contrary, that a target qualifies for inclusion in §702. Where, however, the NSA is aware that the individual is a U.S. person, the agency must proceed under §§703 or 704.

---

[377] 18 USC §2518(1)(i).
[378] 50 USC §1804(a)(6).
[379] 18 USC §2516(1).
[380] 50 USC §§.
[381] *Compare* 18 USC §2510(9)(a) *and* 50 USC §§.
[382] 18 USC §2518(5).
[383] Berger v. New York, 388 U.S. 41 (1967).

By interpreting §702 to include any information "about" the target, (together with the assumption that the target is not located in the United States), the NSA has created a loophole that results in the *de facto* targeting of U.S. persons and non-U.S. persons in the United States and overseas without ever meeting anything even approximating a warrant requirement. Significant amounts of information appear to be at stake.

Consider, for instance, XKeyscore.[384] In 2007, an NSA report estimated that the NSA had collected and stored approximately 850 billion "call events" and 150 billion Internet records.[385] The document claimed that on a daily basis another one to two billion records were added.[386] In 2010 the *Washington Post* reported that the NSA intercepted and stored 1.7 billion emails, phone calls, and other communications per day.[387] In 2012, William Binney, a mathematician who previously worked at the NSA, estimated that the agency had obtained approximately 20 trillion email and telephone transactions just between U.S. citizens.[388] *The Guardian* reported that during one 30-day period in 2012, at least 41 billion total records were collected and scored in XKeyscore.[389] Volume is key to the program's success: part of the power of the digital network intelligence (DNI) program is that it allows analysts to search based on patterns, instead of particular individuals.[390]

Or consider PRISM and Upstream collection more generally. The NSA and FISC both acknowledge that tens of thousands of entirely domestic communications are being collected as part of these programs.[391] Assuming, *arguendo*, that none of those privy to the communications are themselves targets of the collection (based on the theory that the target must be located outside the United States and the communications in question are entirely domestic), what the NSA's interpretation is doing is allowing the government to collect information about U.S. persons' domestic communications, without any prior showing to a judicial body. This *de facto* result runs contrary to traditional FISA's requirement that the only way in which such surveillance can occur is when at least one person involved in the communications is a foreign power or an agent thereof, as demonstrated to a judicial body. The interpretation of targeting as any information *about* a target (again, assumed to be outside the United States), allows the NSA to collect significant amounts of international communications.

Unlike Title III, traditional FISA, or §§703 or 704, §702 does not require the government to obtain an order prior to the collection of non-U.S. persons'

---

[384] Since much of the information about XKeyscore remains classified, it is not clear how much of the data included in the program includes information obtained under Executive Order 12333, §2.5, and how much derives from §702. It is thus used here as an example, but further information is required to confirm its basis in §702.

[385] Glenn Greenwald, *XKeyscore: NSA tool collects "nearly everything a user does on the internet",* THE GUARDIAN, Jul. 31, 2013, available at http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

[386] *Id.*

[387] Dana Priest and William M. Arkin, *Top Secret America: A Washington Post Investigation*, WASH. POST, Sept. 16, 2010, available at http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/1/.

[388] Glenn Greenwald, *XKeyscore: NSA tool collects "nearly everything a user does on the internet",* THE GUARDIAN, Jul. 31, 2013, available at http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

[389] Id.

[390] Laura Poitras, Marcel Rosenbach and Holger Stark, *Ally and Target: US Intelligence Watches Germany Closely*, DER SPIEGEL ONLINE INTERNATIONAL, Aug. 12, 2013, available at http://www.spiegel.de/international/world/germany-is-a-both-a-partner-to-and-a-target-of-nsa-surveillance-a-916029.html.

[391] *See* August 2013 FISC opinion.

communications. Instead, the authority to do so derives from the President's Article II authorities. For U.S. persons, however, §§703 and 704 make it clear that the government must first obtain an order. By reading §702 in such an expansive manner, the government is bypassing the requirements of §§703-704.

The NSA's 2011 minimization procedures do not rectify the problem. To the contrary, the minimization procedures, as aforementioned, allow for all encrypted communications to be retained, and for information of foreign intelligence interest (itself a broad category) or of use in criminal prosecution, to be retained. They do not create a higher barrier to subsequent prosecution than that presented in the mere collection of foreign intelligence. To the extent that traditional FISA, or §§703-704 are predicated upon a constitutional requirement that the warrant clause be satisfied, the *de facto* result absent previously satisfied constitutional requirements raises concern.

2. Use of Wiretap Evidence in Investigation and Prosecution

The FAA authorizes the government to use §702-obtained material for criminal prosecution, provided that (a) the Attorney General provides advance authorization, and (b) proper notice is given to the court or governmental entity involved, as well as to individuals against whom the information will be used. The FAA accomplishes this by folding the use of information obtained under §702 into the requirements for using information acquired via traditional FISA in criminal trials.

More specifically, information obtained under §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.[392] The notice obligation applies (1) "whenever 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", (3) "against an aggrieved person" (4) "any information obtained or derived from" (5) an "electronic surveillance [or physical search] of that aggrieved person."[393] Where these conditions hold, the government is required, *prior* to the trial, hearing, or other proceeding, to notify the aggrieved person and the Court (or other authority), that such information is to be disclosed or used.[394] The defendant may then challenge the use of the information on two grounds: either it was unlawfully obtained, or it was not acquired consistent with an order of authorization or approval.[395]

Two points deserve notice. First, one could reject the *de facto* targeting argument discussed above, hewing more closely to the proposition that the information being collected, despite the volume, is merely incidental to the program. It is, after all, inevitable that in the course of electronic intercepts, at least some sort of other information may be obtained. But, even assuming notice, the absence of procedural protections in §702, in contrast to those in place under traditional FISA raises concerns about the extent to which the use of incidentally-collected §702 information at trial—including trials unrelated to the foreign intelligence purposes for which the FAA was introduced—raises Fourth Amendment issues.

---

[392] 50 U.S.C. §1881e(a) ("Information acquired from an acquisition conducted under section 1881a of this title shall be deemed to be information acquired from an electronic surveillance pursuant to subchapter 1 for purposes of section 1806 of this title.")
[393] 50 U.S.C. §1806(c).
[394] 50 U.S.C. §1806(c).
[395] 50 U.S.C. §§1806(e) and (f), 1881e(a).

Second, it is not at all clear that the government is actually abiding by the requirement that it reveal to defendants that information obtained from or related to information acquired under the FAA is being used in prosecution. Not only has the government made misrepresentations to the Supreme Court in this regard, but the practice of parallel construction (made public by leaked documents in 2013), suggests that further steps are being taken to avoid disclosure.

a. Procedural Protections and Incidental Collection

As a matter of criminal law, Title III does not forbid the interception of incidental or "nonpertinent" communications. Instead, the statute, as one court explained, "requires that measures be adopted to reduce the extent of such interception to a practical minimum while allowing the legitimate aims of the Government to be pursued."[396] The government must minimize its interception of conversations that do not implicate predicate offenses.[397] And the initial order may not authorize interception "for any period longer than is necessary to achieve the objective of the authorization," with an outside window of 30 days.[398] Courts keep a close eye on law enforcement to ensure that these steps are being followed.[399]

Even with these precautions, at times incidental 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.[400] The contents of incidental communications, and any evidence that is derived from such communications, must 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 statutory provisions.[401]

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.[402] Courts thus look to the legislative 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."[403]

The purpose behind requiring law enforcement to return to a court of law is to ensure that the executive branch does not simply evade the restrictions placed upon applications for original wiretap orders, such as the belief that the target is involved in

---

[396] United States v. Turner, 528 F.2d 143 (9th Cir. 1975). *See also* United States v. Ozar, 50 F.3d 1440 (8th Cir.1995) (considering minimization requirements met in bank fraud case); and Wayne R. LaFave, Jerold H. Israel, Nancy J. King, Orin S. Kerr, Minimization, 2 Crim. Proc. §4.6(h)(3d ed.).

[397] 18 USC §2518(5).

[398] 18 USC 2518. Extensions are similarly limited. *Id.*

[399] *See, e.g.,* Dennis K. Berman, *The Galleon Legacy: White-Collar Wiretaps*, WALL ST. J., May 11, 2011, *available at* http://online.wsj.com/news/articles/SB10001424052748704681904576317641529229136 (quoting a federal judge who discovered that the FBI had listened in to personal details in phone calls between defendants in one case "nothing short of disgraceful.")

[400] Robert A. Morse, *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 (1991), §2[a].

[401] 18 USCA §2517(5).

[402] *See generally* 18 USCA §2517(5) (absence therein of specific guidance of subsequent application or procedure to be followed).

[403] S Rep 1097, 90th Cong., 2nd Sess.

the commission of a serious offense.[404] 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.[405] 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.[406] It was precisely to prevent such searches that Congress inserted the requirement that law enforcement return to a third party magistrate to evaluate the incidental information thereby obtained.[407] This was the compromise struck between protecting the right to privacy enshrined in the Fourth Amendment and the inadvertent discovery of criminal activity.[408]

Congress and the courts frown on the deliberate interception of incidental information. In other words, 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 enforcement must demonstrate that the information is relevant to the target and/or specific investigation underway.

Information incidentally obtained under traditional FISA may also be used in criminal prosecution. But acquisition of communications under §702 includes none of the procedural protections that mark either Title III or traditional FISA.[409] At no point in the process is anything even approximating a warrant obtained. (For notice considerations, *see* discussion below). In light of the role of Congress in setting the outer limits of Executive power in the realm of foreign intelligence collection (see discussion, *infra*),, the collection of significant amounts of incidental information absent judicial warrant raises Fourth Amendment concerns. Under §§703 and 704, Congress has explicitly directed that where U.S. persons are being targeted, either domestically or overseas, they be given stronger protections, ensuring that their rights are protected. In contrast, the use of information collected under §702 in criminal prosecution means that individuals suspected of wrongdoing are brought to trial without ever satisfying the particularization and warrant requirements embraced by criminal law and national security law. It bypasses the constitutional requirements as understood by Congress in enacting the 2008 FAA. And it allows the information to then be used to prosecute any number of crimes, unrelated to the offense for which information was being sought in the first place. Unlike criminal law, at no point must

---

[404] *See* United States v. Marion (1976, CA2 NY) 535 F2d 697; United States v. Arnold (1985, CA7 Ill) 773 F2d 823, 18 Fed Rules Evid Serv 1000; 103 A.L.R. Fed. 422, at 9.

[405] United States v. Arnold (1985, CA7 Ill) 773 F2d 823, 18 Fed Rules Evid Serv 1000.

[406] 103 A.L.R. Fed. 422, at 9. *See also* United States v. Marion (1976, CA2 NY) 535 F2d 697; United States v. Smith (1984, CA1 Mass) 726 F2d 852, on remand (DC Mass) 587 F Supp 653, aff'd (CA1 Mass) 752 F2d 640 and app dismd (CA1 Mass) 754 F2d 31 and cert den 469 US 841; United States v. Campagnuolo (1977, CA5 Fla) 556 F2d 1209, later app (CA5 Fla) 592 F2d 852.

[407] *See, e.g.,* United States v. Smith, 726 F2d 852 (1984); United States v. Campagnuolo, 556 F2d 1209 (1977).

[408] 103 A.L.R. Ref. 422, 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.,* at 10. N

[409] *But see* In re Directives, at 1013 [addressing prior judicial review, probable cause, and particularity required under the warrant clause and finding that the safeguards in the PAA (i.e., targeting procedures, minimization procedures, procedure to ensure that a significant purpose of surveillance is to obtain foreign intelligence, procedures incorporated via Exec order 2.5, and procedures outlined in affidavit supporting certifications) meet the standard].

an application seeking judicial approval for the testimonial use of intercepted communications relating to "other offenses" be made.[410]

b. Notice

As aforementioned, under FISA and the FAA, the government is required to provide notice to "aggrieved persons" that information obtained from §702 is to be used prior to trial. This requirement is folded into the procedures highlighted in traditional FISA, in relation to which Courts routinely review information material to prosecution (and central to the defense) to ascertain whether defendants must have access to the information and whether, and to what extent, such information should be suppressed.[411]

Consistent with the statutory provisions, and the government's practice with regard to traditional FISA, in 2012 the Administration informed the Supreme Court that the Department of Justice was required to notify criminal defendants if evidence obtained from §702 would be used during trial.[412] In *Clapper v. Amnesty International*, Justice Samuel A. Alito, Jr. relied in part on this claim to support the Court's holding.[413] The question was whether plaintiffs had standing to challenge the constitutionality of §702. The Court underscored that other protections were in place to ensure that collection under §702 could be challenged: "if the Government intends to use or disclose information obtained or derived from a [§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."[414]

While this position was consistent with the statutory requirement, it did not reflect DOJ's actual practice at the time. In December 2012, during FAA renewal debates, Senator Diane Feinstein had credited the statute with providing information central to the successful prosecution of domestic terrorism cases.[415] She cited one hundred

---

[410] Compare to 18 USC §2517(5).

[411] 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), *aff'g* 531 F.Supp. 2d 832 (N.D. Ohio 2008); 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), *aff'g* United States v. Megahey, 553 F.Supp. 1180 (E.D.N.Y. 1982); 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, 1017-1019 (5th Cir. 2014); United States v. Campa, 529 F.3d 980, 988-89, 993-94 (11th Cir. 2009); United States v. Hammoud, 381 F.3d 316, 331-34 (4th Cir. 2004) (en banc), *reinstated in relevant part,* 405 F.3d 1034 (4th Cir. 2005). See generally Robert Timothy Reagan, Foreign Intelligence Surveillance Act Litigation, Federal Judicial Center, April 30, 2014, p. 25, fns 218 & 219. 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.,* Memorandum Order, United States v. Adel Daoud, No. 1:12-cr-00723 (N.D. Ill., Jan. 29, 2014), at 5 ("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.")

[412] Government Reply Brief, p. 15, Clapper v. Amnesty Int'l USA, No. 11-1025 (U.S. Oct. 17, 2012), available at http://www.americanbar.org/content/dam/aba/publications/supreme_court_preview/briefs/11-1025_pet-reply.authcheckdam.pdf. ("[T]he government must provide advance notice of its intent to use information obtained or derived from [§702]-authorized surveillance against a person in judicial or administrative proceedings and that person may challenge the underlying surveillance.") See also Transcript, at 4, id., (Oct. 29, 2012), available at http://www.supremecourt.gov/oral_arguments/argument_transcripts/11-1025.pdf (recognizing "notice that the government intends to introduce information in a proceeding against" a defendant).

[413] Clapper v. Amnesty Int'l USA, 568 U.S. ____ (2013) (Alito, J.)

[414] *Id.*

[415] Feinstein on FISA Amendments Act and Domestic Terror Cases: Senator Dianne Feinstein Discusses the FISA Amendments Act and Domestic Terrorism Cases on Dec. 27, 2012, C-SPAN, Oct. 8, 2013,

arrests between 2009 and 2012.[416] Feinstein went on to address specific cases related to charges of material support, use of weapons of mass destruction, and bombing and assassination plots.[417] Lawyers in two of the cases mentioned (one in Chicago, and one in Fort Lauderdale) responded to Feinstein's speech by asking prosecutors to confirm whether information obtained under the FAA had been used in their clients' cases.[418] 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 702.[419] According to the government, such notification would be "unwarranted and unprecedented."[420]

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.[421] He was reportedly informed that it had been a misunderstanding, stemming from a rather narrow definition of what "derived from" meant.[422] A two-month debate within DOJ ensued as to whether prosecutors were required to provide information to defendants in regard to information derived from §702.[423] And the government changed its position: 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 didn't need to disclose when such evidence had been used, "that is not the government's position."[424]

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

---

transcript and video of statement available at http://www.c-span.org/video/?c4467868/feinstein-fisa-amendments-act-domestic-terror-cases.

[416] Feinstein on FISA Amendments Act and Domestic Terror Cases: Senator Dianne Feinstein Discusses the FISA Amendments Act and Domestic Terrorism Cases on Dec. 27, 2012, C-SPAN, Oct. 8, 2013, transcript and video of statement available at http://www.c-span.org/video/?c4467868/feinstein-fisa-amendments-act-domestic-terror-cases.

[417] *Id.*

[418] Eric Schmitt, David E. Sanger, Charlie Savage, *Administration Says Mining of Data is Crucial to Fight Terror*, N.Y. TIMES, June 7, 2013, available at 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.

[419] Barrett Devlin, *U.S. Spy Program Lifts Veil in Court; Justice Department Ways Prosecution in Terrorist Cases Must Tell Defendants When Surveillance Program Was Used*, WALL ST. J., July 31, 2013.

[420] *Id. See also* Eric Schmitt, David E. Sanger, Charlie Savage, *Administration Says Mining of Data is Crucial to Fight Terror*, N.Y. TIMES, June 7, 2013, available at 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.; Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. TIMES, Oct. 16, 2013, available at http://www.nytimes.com/2013/10/17/us/politics/us-legal-shift-may-open-door-for-challenge-to-secret-wiretaps.html?_r=0.

[421] Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. TIMES, Oct. 16, 2013, available at http://www.nytimes.com/2013/10/17/us/politics/us-legal-shift-may-open-door-for-challenge-to-secret-wiretaps.html?_r=0.

[422] Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. TIMES, Oct. 16, 2013, available at http://www.nytimes.com/2013/10/17/us/politics/us-legal-shift-may-open-door-for-challenge-to-secret-wiretaps.html?_r=0.

[423] Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. TIMES, Oct. 16, 2013, available at http://www.nytimes.com/2013/10/17/us/politics/us-legal-shift-may-open-door-for-challenge-to-secret-wiretaps.html?_r=0.

[424] Barrett Devlin, *U.S. Spy Program Lifts Veil in Court; Justice Department Ways Prosecution in Terrorist Cases Must Tell Defendants When Surveillance Program Was Used*, WALL ST. J., July 31, 2013.

surveillance authorized by" the FAA.[425] In light of settlement negotiations, Judge Robert W. Sweet held the case in abeyance.[426] And in 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*.[427] The government has not yet responded.

As a practical matter, in the six months following DOJ's shift in policy, the government only submitted §702 notices in three cases.[428] Two of these cases were already post-conviction. The failure to provide prior notice meant that defendants were deprived of an opportunity to challenge the FAA as constitutional (either on its face or as applied). They were unable to challenge whether the government complied with the statutory requirements of the FAA. And they could not address whether the withheld surveillance evidence tainted pretrial motions or defenses at trial, or whether the government had engaged in over-reaching, misrepresentation, or misconduct during either pre-trial or trial proceedings.

In the first case, Loretta Lynch, the U.S. attorney for the Eastern District of New York, informed the defendant that the government had used information obtained from §702 to obtain an order under traditional FISA.[429] In the government's view, however, because he had pled guilty in 2012, he had given up his right to appeal: "this supplemental notification does not afford you a basis to withdraw your plea or to otherwise attack your conviction or sentence because you expressly waived those rights, as well as the right to any additional disclosures from the government, in your plea agreement."[430] (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).[431]

The second case involved a 19-year old Somali-born student at Oregon State, Mohamed Osman Mohamud, who was convicted in January 2013 of attempting to use a weapon of mass destruction.[432] In 2009 the FBI intercepted Mohamud's emails with an individual suspected of recruiting for terrorist organizations.[433] The FBI later made contact with Mohamud through an undercover agent who posed as an acquaintance of the recruiter, and who helped Mohamud to make plans to detonate a bomb in 2010 at a

---

[425] Complaint, ACLU v. United States Dep't of Justice, No. 1:13-cv-7347 (S.D.N.Y. Oct. 17, 2013), D.E. 1.
[426] Order, ACLU v. United States Dep't of Justice, No. 1:13-cv-7347 (S.D.N.Y. Jan. 16, 2014), D.E. 9.
[427] Charlie Savage, *Justice Department Criticized on Spying Statements*, N. Y. TIMES, May 13, 2014.
[428] Charlie Savage, *Justice Department Informs Inmate of Pre-Arrest Surveillance*, N.Y. TIMES, Feb. 25, 2014, available at http://www.nytimes.com/2014/02/26/us/justice-dept-informs-inmate-of-pre-arrest-surveillance.html.
[429] Letter to Agron Hasbajrami, from Loretta Luynch, Feb. 24, 2014, available at https://www.documentcloud.org/documents/1028728-hasbajrami-supplemental-notice-2-24-2014.html.
[430] Letter to Agron Hasbajrami, from Loretta Luynch, Feb. 24, 2014, available at https://www.documentcloud.org/documents/1028728-hasbajrami-supplemental-notice-2-24-2014.html.
[431] Charlie Savage, *Justice Department Informs Inmate of Pre-Arrest Surveillance*, N.Y. TIMES, Feb. 25, 2014, available at http://www.nytimes.com/2014/02/26/us/justice-dept-informs-inmate-of-pre-arrest-surveillance.html.
[432] Indictment, United States v. Mohamud, No. 3:10-cr-475 (D.Or. Jan. 31, 2013), D.E. 2; Verdict, United States v. Mohamud, No. 3:10-cr-475 (D.Or. Jan. 31, 2013), D.E. 428; United States v. Mohamud, 941 F. Supp. 2d 1303, (D. Or. 2013).
[433] Colin Miner, Liz Robbins, and Erik Eckholm, *FBI Says Oregon Suspect Planned "Grand" Attack*, N.Y. TIMES, Nov. 27, 2010, available at http://www.nytimes.com/2010/11/28/us/28portland.html?pagewanted=all&_r=0.

Portland, Oregon Christmas Tree lighting ceremony.[434] In November 2013, eleven months after his conviction, the government informed Mohamud that information obtained or derived from traditional FISA may also have been related to prior §702 collection.[435] During briefing, the government acknowledged that the notice had been untimely.[436]

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 §702-derived information, as statutorily required. (Muhtorov, was arrested at O'Hare airport on his way to Turkey on January 21, 2012.)[437] In October 2013, the government filed a §702 notice.[438] The matter has not yet been fully addressed by the court: the defendant's motion to suppress was filed in January 2014.[439] On May 9, 2014 the government filed both a classified and an unclassified memorandum in opposition to the defendant's motion.[440] This document recognized the statutory basis for the FAA notice requirement, but asserted that the §702 collection had been both lawful and constitutional.[441]

As aforementioned, these three cases are the only ones, as of the time of writing, to involve §702 notice. Even the two cases discussed by Feinstein, which spurred the debate, did not later result in notice being served. Prosecutors in both cases submitted documents to the court saying, to the contrary, that they did not plan to use FAA-derived materials. A letter from a Senate lawyer, in turn, later stated that Senator Feinstein "did not state, and did not mean to state" that the cases were linked to the warrantless surveillance program.[442] The defense lawyers protested to the court that reference to their clients had not been random; it had been part of the debate over whether to renew authorities under the 2008 FAA.[443] Senator Feinstein declined comment.[444]

At a minimum, government practice appears to be rather conservative in informing defendants of the use of §702 information. During her remarks, for instance, Senator Feinstein noted that in 2012 alone there had been 16 domestic terrorism arrests.[445] Yet only one person who had not yet gone to trial had, between July 2013 and June 2014, received a §702 notice.

---

[434] Colin Miner, Liz Robbins, and Erik Eckholm, *FBI Says Oregon Suspect Planned "Grand" Attack*, N.Y. TIMES, Nov. 27, 2010, available at http://www.nytimes.com/2010/11/28/us/28portland.html?pagewanted=all&_r=0.

[435] Supplemental FISA Notification, United States v. Mohamud, No. 3:10-cr-475 (D.Or. Jan. 31, 2013), D.E. 486 *(cited also in Minutes of Proceedings, Nov. 26, 2013, D.E. 439). See also* Charlie Savage, *Warrantless Surveillance Challenged by Defendant.* N.Y. TIMES, Jan. 30, 2014, at A15.

[436] Government Discovery Opposition Brief at 9, n. 5, 12, Mohamud, No. 3:10-cr-475 (D.Or.Feb. 13, 2014), D.E. 491.

[437] Complaint, United States v. Muhtorov, No. 1:12-cr-33 (D. Colo. Jan 19, 2012), ED.E. 1; Indictment, Muhtorov. No. 1:12-cr-33 (D. Colo. Jan. 23, 2012) D.E. 5. Note that a Section 702 notice was not served on the other defendant, Jumaev.

[438] FISA Notice, Muhtorov, No. 1:12-cr-33 (D.Colo. Jan. 23, 2012) D.E. 457.

[439] Motion, Muhtorov, No. 1:12-cr-33 (D.Colo. Jan. 23, 2012) D.E. 520.

[440] Muhtorov, No. 1:12-cr-33 (D.Colo. Jan. 23, 2012) D.E. 559. Unclassified version available at https://www.aclu.org/sites/default/files/assets/muhtorov_-_govt_response_to_motion_to_suppress.pdf.

[441] *Id.*

[442] Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. TIMES, Oct. 16, 2013, available at http://www.nytimes.com/2013/10/17/us/politics/us-legal-shift-may-open-door-for-challenge-to-secret-wiretaps.html?_r=0.

[443] *Id.*

[444] *Id.*

[445] Feinstein on FISA Amendments Act and Domestic Terror Cases: Senator Dianne Feinstein Discusses the FISA Amendments Act and Domestic Terrorism Cases on Dec. 27, 2012, C-SPAN, Oct. 8, 2013,

To the extent that, as a result of *Clapper*, only those so notified may have standing to challenge the constitutionality of §702, the pool of potential challengers is extremely limited. And there is evidence that a conscious effort is being made to avoid reference to foreign intelligence gathering in non-terrorism cases—even where the FAA may have played a key role.

In August 2013 Reuters reported that federal agents were being directed to cover up the source of intelligence leading to criminal prosecution by following a process referred to as "parallel construction."[446] Under this approach, law enforcement re-constructs an evidentiary trail to hide the origins of information obtained through national security surveillance.[447] Reuters published slides generated by the Special Operations Division (SOD) of the U.S. Drug Enforcement Administration (DEA), an entity made up of two dozen agencies, including, *inter alia*, the FBI, CIA, NSA, Internal Revenue Service, and Department of Homeland Security. [448] SOD, which employs several hundred people, was created in 1994 to combat Latin American drug cartels.[449] It has since expanded to include a range of terrorism, narcotics, and criminal concerns.

SOD distributes information from NSA intercepts and domestic wiretaps, as well as other information, to other agencies.[450] The slides published by Reuters (and confirmed by interviews with prior and current DEA employees) direct agents to employ parallel construction when constructing criminal cases against U.S. citizens that actually derive from warrantless surveillance.[451] The purpose is to keep methods and sources secret.[452]

The incentive structure to use parallel construction works against providing notice to defendants. The number of terrorism prosecutions in the United States represents only a small percentage of all criminal cases. In March 2014, for instance, there were 12,174 new criminal prosecutions.[453] Of these, only about 16 appear to be linked to terrorism.[454] This means that in March 2014, 0.1% of all criminal prosecutions in the U.S. were terrorism-related. This is a very small percentage of cases in which §702 information might be introduced. The number of terrorism prosecutions, moreover, is steadily decreasing: between 2008 and 2013, for instance, prosecutions were down

---

transcript and video of statement available at http://www.c-span.org/video/?c4467868/feinstein-fisa-amendments-act-domestic-terror-cases.

[446] John Shiffman and Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover up Program Used to Investigate Americans*, Reuters, Aug. 5, 2013, available at http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805.

[447] John Shiffman and Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover up Program Used to Investigate Americans*, Reuters, Aug. 5, 2013, available at http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805.

[448] *Id.*

[449] *Id.*

[450] *Id.*

[451] *Id.*

[452] *Id.*

[453] Prosecutions for March 2014, TRAC Reports, available ta http://trac.syr.edu/tracreports/bulletins/overall/monthlymar14/fil/.

[454] This total includes 2 domestic terrorism prosecutions (Terrorism-Domestic Prosecutions for March 2014, available at http://trac.syr.edu/tracreports/bulletins/domterror/monthlymar14/fil/); 1 international terrorism prosecution (Terrorism-International Prosecutions for March 2014, available at http://trac.syr.edu/tracreports/bulletins/intterror/monthlymar14/fil/); 2 terrorism-related financing prosecutions (Terrorism-related Financing Prosecutions for March 2014, available at http://trac.syr.edu/tracreports/bulletins/finterror/monthlymar14/fil/); and 11 national internal security/terrorism prosecutions (National Internal Security/Terrorism Prosecutions for March 2014, available at http://trac.syr.edu/tracreports/bulletins/terrorism/monthlymar14/fil/).

38.9%.[455] In contrast, in March 2014, there were 1,487 new prosecutions for narcotics or drug-related crimes.[456] If DEA agents use §702-derived information and fail to engage in parallel construction, there would be a significantly higher pool of potential challengers to §702.

Concern about the use of parallel construction has begun to make its way into court opinions.[457] Because of the highly classified nature of the material, however, it is not clear how much of a role this plays in the prosecution of criminal offences. As of August 2013, DOJ informed the media that it was looking into the allegations.[458] No further information has been forthcoming.

3. Further Query of §702 Data

Just because information is already in government hands, it does not necessarily follow that the government has the authority to conduct further searches in order to uncover criminal activity either related or unrelated to the purpose of initially obtaining the data in question. Perhaps the most intriguing case on this point is *United States v. Cotterman*, a border search case in which a laptop was seized at the border and then transported nearly 170 miles for further inspection.[459]

The Supreme Court has long recognized that weaker Fourth Amendment protections apply at U.S. borders. In *United States v. Ramsey*, the Court stated that "searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border."[460] Routine searches at the border therefore do not require a search warrant, probable cause, or individualized suspicion.[461] This is true of both physical inspection and examination of mail.[462] The court looks to the balancing test under *Camara*, noting that there is a "vital national interest in preventing illegal entry and smuggling", and that such searches represent a "limited invasion"—i.e., they are directed at individuals who may themselves choose when and where they will undergo the search.[463] As the intrusion becomes more invasive, the outcome of applying the balancing test shifts.[464]

In *Cotterman*, the Ninth Circuit considered the intrusive nature of digital searches in a world where individuals "carry with them laptop computers, iPhones, iPads, iPods, Kindles, Nooks, Surfaces, tablets, Blackberries, cell phones, digital cameras, and more."[465] The Court noted, "These devices often contain private and sensitive

---

[455] Terrorism/National Internal Security Prosecutions for February 2013, Trac Reports, available at http://trac.syr.edu/tracreports/terrorism/316/.
[456] Federal Drug Prosecutions Fall to Lowest Level in Over 13 Years, TRAC Reports, http://trac.syr.edu/tracreports/crim/347/.
[457] *See, e.g.,* Second Memorandum Opinion and Order, In the Matter of the Search of Information Associated with [REDACTED] @Mac.com That is Stored at Premises Controlled by Apple, Inc., Magistrate Case No. 12-228 (JMF), U.S. Disctrict Court for the District of Columbia, p. 16, fn. 15 ("Even if outright abuse does not occur, there is always the risk of troubling uses such as 'parallel construction,' where illegal or secret criminal investigations are recreated in a manner that is seemingly consistent with the Constitution without informing the accused or the court.")
[458] Karen McVeigh, *US Drug Agency Surveillance Unit to be Investigated by Department of Justice*, THE GUARDIAN, Aug. 6, 2013, available at http://www.theguardian.com/world/2013/aug/06/justice-department-surveillance-dea.
[459] United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013).
[460] United States v. Ramsey, 431 U.S. 606 (1977).
[461] United States v. Lincoln, 494 F.2d 833 (9th Cir. 1974).
[462] United States v. Ramsey, 431 U.S. 606 (1977).
[463] Wayne R. LaFave, Jerold H. Israel, Nancy J. King, Orin S. Kerr, 2 Crim. Proc. §3.9(f)(3d ed).
[464] *Id.*
[465] 709 F.3d at 957.

information ranging from personal, financial, and medical data to corporate trade secrets."[466] The Ninth Circuit referred to the case as a "watershed," implicating both the narrow border search exception to the Fourth Amendment's warrant requirement, as well as the privacy rights entailed in common electronic devices.[467] In this case, although the warrant requirement was found not to apply, the Court nevertheless subjected officials' actions to a reasonableness test to determine whether child pornography obtained in the distance search should be admitted as evidence.[468]

Central to the case was the use of a primary and secondary search, in that the first search did not turn up any evidence that implicated Cotterman in the suspected crime. Nevertheless, ICE sent the computer for further forensic examination, in the course of which the government uncovered evidence. The government, accordingly, initially characterized the question before the court as "Whether the authority to search a laptop computer without reasonable suspicion at a border point of entry permits law enforcement to take it to another location to be forensically examined, when it has remained in the continuous custody of the government."[469]

A divided panel of the Ninth Circuit initially concluded that reasonable suspicion was not required for the search.[470] Judge Betty B. Fletcher dissented, stating that "officers must have some level of particularized suspicion in order to conduct a seizure and search like the one at issue here."[471] Following oral argument en banc, the Ninth Circuit requested supplemental briefing on the question of whether reasonable suspicion existed at the time of the search, later determining that it did.[472]

This case is important for §702 analysis not because PRISM and Upstream collection necessarily take place at the border, but because the Ninth Circuit underscored the possibility that, while the government may have the authority to obtain and to search a computer at the border, further search of that information may not meet the reasonableness standard under the Fourth Amendment.[473] For the Ninth Circuit, the forensic examination was not merely an extended border search.[474] The Court explained, "A border search of a computer is not transformed into an extended border search simply because the device is transported and examined beyond the border."[475] Instead, the Court treated the second search as the functional equivalent of a border search. The Court determined that the second search must also comport with the reasonableness requirement of the Fourth Amendment.

The case is important in highlighting that further search of information already in government hands, must nevertheless comport with Fourth Amendment requirements. That is, in light of the privacy interests implicated, the requirement of further judicial approval prior to conducting a further search may be one way to ensure that privacy

---

[466] 709 F.3d at 957.
[467] 709 F.3d at 957.
[468] 709 F.3d at 957.
[469] United States v. Cotterman, 637 F.3d 1068 (9th Cir. 2011).
[470] *Id*.
[471] 637 F.3d at 1084 (B. Fletcher, J., dissenting).
[472] 709 F.3d at 959.
[473] Further Fourth Amendment analysis might consider whether the cables carrying electronic communications across the border constitute a functional equivalent to the border search exception. See, e.g., Almeida-Sanchez v. United States, 413 U.S. 266, 272 (1973). The Court's purpose in adopting broader standards at the border was to protect the United States' sovereign interest in monitoring items or individuals entering or leaving U.S. territory. U.S. v. Flores-Montano, 541 U.S. 149, 152-153 (2004). Having rejected an approach that links physical presence to electronic, however, I similarly reject an analysis that applies the same to international communications for purposes of a functional border.
[474] 709 F.3d at 961.
[475] 709 F.3d at 961.

interests continue to be protected under the Fourth Amendment. The case also leads us to a more detailed discussion of reasonableness in the context of §702.

E. Reasonableness Standard

Courts have routinely recognized, prior to FISA and in the intervening years, that regardless of whether the warrant clause applies, government actions (in criminal law and foreign intelligence), with regard the domestic collection of information, or the international collection of information on individuals with a substantial connection to the United States, must still comport with the Fourth Amendment's reasonableness requirement.[476]

As a domestic, criminal law matter, in determining whether a search is reasonable under the Fourth Amendment, the Court looks to the totality of the circumstances.[477] This test amounts to a balancing test of the interests at stake.[478] It considers the nature of the government intrusion into privacy.[479] 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.[480]

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.[481] In 1987, then Judge (and now Justice) Kennedy explained that the exclusionary rule only applies where U.S. officials fail to act in good faith reliance on foreign law.[482] This approach has been adopted with regard to both physical searches and wiretaps conducted overseas.[483]

Under this approach, U.S. constitutional rights depend in some form on foreign legal systems and the relevant laws. Although this seems odd at the outside, it does reflect 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 it to the FAA realm is that in its global intercepts, the U.S. intelligence community is not operating solely according to one set of laws. Upstream collection, for instance, may include the interception of packets that pass through dozens of different countries. It would be almost impossible to apply each law's contours as even one packet moves over the network—much less as all the packets that constitute just communication—much less tens of thousands of communications. Even taking into account the Five Eyes, moreover, such operations

---

[476] *See, e.g.,* United States v. Place, 462 U.S. 696 (1983).

[477] Samson v. California, 547 U.S. 843, 848 (2006); Tennessee v. Garner, 471 U.S. 1 (1985). See also Scott v. United States, 436 128 (1978) (finding the acquisition of virtually all conversations reasonable and underscoring that reasonableness depends on the facts and circumstances of each case).

[478] Samson, 547 U.S. at 848; US v. Knights, 534 U.S. 112 (2001).

[479] Garner, 471 U.S. at 8; Place, 462 U.S. at 703.

[480] Michigan v. Summers, 452 U.S. 692 (1981); In re Directives, at 1012.

[481] United States v. Peterson, 812 F.2d 486 (9th Cir. 1987).

[482] *Id.*

[483] *See, e.g.,* Barona, 56 F.3d at 1092; 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.Puerto Rico 1991); United States v. Scarfo CRIM.A. No. 88-00003-1-19, 1988 WL 115805, at *4 (E.D. Penn. Oct. 26, 1988).

could not properly be understood as joint operations, of the sort considered by the Ninth Circuit in *Barona*.

Perhaps because of these difficulties, FISC 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 Second Circuit employed a reasonableness analysis that weighed governmental interests against the privacy intrusion involved.[484] In 2013 the Seventh Circuit largely followed course.[485]

This is the test to which FISC has appealed in considering the reasonableness of intercepts overseas. (See discussion, below) An important point to note at the outset, though, is the trouble with simply 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"[486] create a heavy burden to be overcome. National security, in other words, is a powerful trump card. As soon as a foreign intelligence purpose is introduced, the standards for reasonableness shift.

Even so, looked at in relation to §702, while the targeting procedures and the interception of information to or from non-U.S. persons located outside the United States may meet the Fourth Amendment's standard of reasonableness, the inclusion of communications "about" targets or selectors falls outside constitutional bounds. The inclusion of "about", and the subsequent use of information obtained in criminal prosecution, also moves incidentally-collected information beyond Fourth Amendment standards.

1. Translation of Criminal Law to National Security Law

In *In Re Sealed case*, in which FISCR 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.[487]

Six years later, FISCR, 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, otherwise, it would contradict the "totality of the circumstances test".[488]

The totality test derives from criminal law, in the context of which the Court, like FISCR, has enumerated factors that must be taken into account to determine whether

---

[484] In re Terrorist Bombings of US Embassies in East Africa, 552 F.3d 157, 167 (2nd Cir. 2008)

[485] U.S. 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. For Kerr's discussion of reconciling the two views see Kerr, supra note at 16 ("If a foreign search warrant is not a search warrant for Fourth Amendment purposes, then a foreign search in reliance on foreign law (the Ninth Circuit approach) does not require a warrant (the Second and Seventh Circuit approach). And if the compliance with foreign law is a factor in the reasonableness, as Stokes suggests, then the two standards will often produce the same results in practice.")

[486] In re Directives at 1012. *See also* Haig v. Agee, 453 U.S. 280 (1981); In re Sealed Case, 310 F.3d at 746.

[487] In re Sealed Case, 310 F.3d at 737-41.

[488] In re Directives at 1013.

the procedures followed in minimization are reasonable. Thus, in *Scott v. United States*, the Supreme 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.[489] 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 percentages 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.[490]

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.[491]

The Court noted that various other factors may play a significant role, such as the precise 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 thus contemplated a learning curve for law enforcement, where the standards applied may shift based on the evolution and maturity of the electronic surveillance.[492]

In *Scott*, most of the nonpertinent calls were either "very short", "ambiguous in nature", or one-time conversations.[493] They thus did not amount to a violation of the

---

[489] Scott v. United States, 436 U.S. 128, 98 S. Ct. 1717, 56 L. Ed. 2d 168 (1978).
[490] 436 U.S. at 140.
[491] 436 U.S. at 140.
[492] *See* 436 U.S. at 141.
[493] 436 U.S. at 141-142.

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.[494]

In translating the totality of the circumstances test to national security law, the unique nature of foreign intelligence gathering matters. As FISCR explained in *In Re Sealed Case*, "Given 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."[495] Resultantly, it is common practice in FISA surveillance to leave surveillance devices on continuously, with the emphasis on minimization occurring at the back end, in the process of indexing and logging the relevant communications.[496] For FISCR, the possibility that the government might, in this process, make a mistake, was not sufficient to invalidate the surveillance in question.[497]

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, to support its claim as to the reasonableness of the surveillance in questions (i.e., targeting procedures, minimization procedures, a procedure to ensure that a significant purpose of a surveillance is to obtain foreign intelligence information, procedures incorporated through Executive Order 12333, §2.5 and procedures outlined in an affidavit supporting the certifications.)[498]

FISCR accepted the government's position.[499] The arguments regarding particularity and prior judicial review fell short in light of how the PAA had been applied. While the PAA itself did not require a particularized showing, the "pre-surveillance procedure" [which remains classified] established a procedure "analogous to and in conformity with the particularity showing" considered by FISCR in *In re Sealed Case*.[500]

The particularity requirement contemplated by FISCR in *In re Sealed Case* related to the probable cause standards applied in traditional FISA.[501] Applied to the PAA, FISCR found in *In re Directives* that the procedures incorporated via Executive Order 12333, §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 US or against a US 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

---

[494] United States v. Quintana, 508 F.2d 867 (7th Cir.1975). See also United States v. Uribe, 890 F.2d 554 (1st Cir. 1989); United States v. Adams, 759 F.2d 1099 (3d Cir. 1985); United States v. Dumes, 313 F.3d 372 (7th Cir. 2002); United States v. McGuire, 307 F.3d 1192 (9th Cir. 2002); United States v. Mansoori, 304 F.3d 635 (7th Cir. 2002); United States v. Brown, 303 F.3d 582 (5th Cir. 2002); United States v. Bennett, 219 F.3d 1117 (9th Cir. 2000).

[495] In re Sealed Case, at 741.

[496] In re Sealed Case, at 740.

[497] In re Directives, at 1015.

[498] In re Directives, at 1013.

[499] In re Directives at 1013. ("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.")

[500] In re Directives at 1013-1014.

[501] In re Sealed Case, 310 F.3d at 740.

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."[502]

What this requirement means is that for the intelligence community to act upon a certification, the Attorney General first has to determine probable cause that the individual being targeted is a foreign power or an agent thereof.[503] Combined with the other protections, such as minimization procedures, such measures offered sufficient compensation for any encroachments into individual privacy, bringing the PAA within the bounds of the Fourth Amendment reasonableness requirement.[504]

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 FISC (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 similarly 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.[505] The only U.S. person information that would have fallen within collection under §702 was either a result of a mistake (i.e., where a U.S. person had be targeted in error), or a result of U.S. persons communicating directly with tasked selectors (i.e., non-U.S. person targets located outside of the country).

In October 2011 Bates concluded that, to the extent that the targeting procedures, as applied to the acquisition of information *other than* Internet transactions (i.e., telephone and Internet communications), still reflected the Court's previous assumptions, they were consistent with the Fourth Amendment reasonableness requirement. The problem, for Bates, was the interception of Internet transactions involving either single discreet communication (Single Communication Transactions, or SCTs) or multiple discrete communications (Multi-[C]ommunication Transactions, or MCTs).[506] Here, Fourth Amendment reasonableness questions loomed large.

The reason these communications changed the picture appears to be that 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. It is therefore the inclusion of "about" that changes the constitutionality of the procedures adopted by the NSA.

2. Incidental Interception

In its October 2011 opinion, FISC confronted the fact that the number of wholly domestic communications being intercepted was significantly higher than the Court had previously understood. The problem lay with both MCTs and SCTs.[507] Upstream collection added another layer of complexity: "NSA's upstream collection devices

---

[502] Exec. Order 12333, §2.5, 46 Fed. Reg. at 59,951 (emphasis added).
[503] In re Directives at 1014.
[504] In re Directives at 1013.
[505] October 2011 Memorandum Opinion, p. 71.
[506] Foreign Intelligence Surveillance Court Memorandum Opinion, Oct. 3, 2011, pp. 27-28.
[507] October 2011 Memorandum Opinion, p. 33 (Bates, J.) ("The Court now understands. . . that NSA has acquired, is acquiring, and, if the certifications and procedures now before the Court are approved, will continue to acquire, tens of thousands of wholly domestic communications.")

will acquire a wholly domestic 'about' SCT if it is routed internationally."[508] The further interception of incidental information created significant constitutional concerns.[509]

Judge Bates underscored the importance of evaluating the government's targeting and minimization procedures in light of the communications actually acquired.[510] The problem was that the sheer volume of information obtained by the NSA via upstream collection made it difficult, as Bates explained, to conduct "any meaningful review of the entire body of the transactions."[511] Only a statistical sampling was possible. In the future, moreover, 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."[512]

Actual practice similarly figured largely 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. *See, e.g.,* United States v. Kahn, 415 U.S. 143, 157-158 (1974); United States v. Schwartz, 535 F.2d 160, 164 (2d Cir. 1976). **The government assures us that it does not maintain a database of incidentally collected information from non-targeted United States persons,** and there is no evidence to the contrary. On these facts, incidentally collected communications of non-targeted United States persons do not violate the Fourth Amendment.[513]

The problem with FISCR'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 could simply feed information incidentally collected under §702 into other databases. Section 702 data, for instance, appears to be contained in multiple databases, including, *inter alia*, MARINA, MAINWAY, NUCLEON, and PINWALE. [514]

---

[508] Foreign Intelligence Surveillance Court Memorandum Opinion, Oct. 3, 2011, p. 34 (Bates, J.).
[509] Foreign Intelligence Surveillance Court Memorandum Opinion, Oct. 3, 2011, pp. 35-36 (Bates, J.).
[510] Foreign Intelligence Surveillance Court Memorandum Opinion, Oct. 3, 2011, p, 28 (Bates, J.)
[511] Foreign Intelligence Surveillance Court Memorandum Opinion, Oct. 3, 2011, p. 31 (Bates, J.).
[512] Foreign Intelligence Surveillance Court Memorandum Opinion, Oct. 3, 2011, p. 32 (Bates, J.).
[513] In re Directives, at 1015.
[514] James Ball and Spencer Ackerman, *NSA Loophole Allows Warrantless Search for U.S. citizens' emails and phone calls*, THE GUARDIAN, Aug. 9, 2013, available at http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls (containing screen shot of classified document). "The documents show that significant amounts of information from the United States go into Mainway. An internal N.S.A. bulletin, for example, noted that in 2011 Mainway was taking in 700 million phone records per day. In August 2011, it began receiving an additional 1.1 billion cellphone records daily from an unnamed American service provider under §702 of the 2008 FISA Amendments Act, which allows for the collection of the data of Americans if at least one end of the communication is believed to be foreign. The overall volume of metadata collected by the N.S.A. is reflected in the agency's secret 2013 budget request to Congress. The budget document, disclosed by Mr. Snowden, shows that the agency is pouring money and manpower into creating a metadata repository capable of taking in 20 billion "record events" daily and making them available to N.S.A. analysts within 60 minutes. The spending includes support for the "Enterprise Knowledge System," which has a $394 million multiyear budget and is designed to "rapidly discover and correlate complex relationships and patterns across diverse data sources on a massive scale," according to a 2008 document. The data is automatically computed to speed queries and discover new targets for surveillance. A top-secret document titled "Better Person Centric Analysis" describes how the agency looks for 94 "entity types," including phone numbers, e-mail addresses and IP addresses. In addition, the N.S.A.

Information is also forwarded to other agencies, such as the National Counterterrorism Center (NCTC), at which point it is no longer associated with the specific authority under which it was collected.[515] For datasets acquired pursuant to Track 3 (i.e., 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."[516] It is thus plausible that incidental information can be fed into broader datasets that can be searched based on pattern analysis. Beyond further database analysis, the use of incidentally collected information in future criminal prosecution raises even more significant concerns.

Although Bates concluded in October 2011 that the 2009 Minimization procedures did not pass constitutional muster, the following month he approved new minimization procedures as consistent with the Fourth Amendment.

In August 2013 the Director of National Intelligence declassified the 2011 minimization procedures. They apply to the acquisition, retention, use, and dissemination of non-publicly available information concerning U.S. persons acquired by targeting non-U.S. persons reasonably believed to be located outside the United States—i.e., incidental collection.

Any inadvertently acquired communications are to be destroyed "at the earliest practicable point in the processing cycle at which such communication can be identified" as either not containing foreign intelligence information, or as not containing evidence of a crime.[517] Entirely domestic communications, however, if to/from, or about a target, may be processed.[518] Unlike the 2009 procedures, the 2011 document draws attention to the inclusion of upstream collection, in the course of which both SCTs and MCTs may be obtained.[519] They require analysts to segregate and to destroy information in either SCTs or MCTs identified as containing domestic

---

correlates 164 "relationship types" to build social networks and what the agency calls "community of interest" profiles, using queries like "travelsWith, hasFather, sentForumMessage, employs."" N.Y. TIMES, Sept. 28, 2013.

[515] 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 §702 programs. *See, e.g.,* National Counterterrorism Center, 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, for the period Mar. 23, 2012 through Mar. 31, 2013; Overview of the Baseline Safeguard Protections Under NCTC's 2012 Attorney General Guidelines, available at NCTC.

[516] National Counterterrorism Center, 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, for the period Mar. 23, 2012 through Mar. 31, 2013, p. 7.

[517] 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, Nov. 2011, §3(b)(1), *available at* http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf.

[518] 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, Nov. 2011, §3(b)(4), available at http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf.

[519] 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, Nov. 2011, §3(b)(5), *available at* http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf.

communications (i.e., communications as to which the sender and all intended recipients are reasonably believed to be located in the United States).[520] Analysts seeking to use MCTs are required to assess whether the communication is entirely domestic, as well as whether it is to/from, or about a tasked selector, or otherwise contains foreign intelligence information.[521] The use of incidentally-collected information in criminal prosecution raises a number of serious concerns.

Returning to the six categories for reasonableness laid out by FISCR in *In re Sealed Case*, in incidental collection obtained under §702, there is no prior judicial review.[522] There is neither the presence (nor absence) of probable cause—indeed, there is no standard applied at all (collection under §702 being outside the confines of either Exec. Order 12333, §2.5 or FAA §§703-704). There is no particularity involved (the target being another individual/entity/selector and the collection broad). 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 FISCR in *In re Directives*, and looks at these not as strict categories to be satisfied, but, rather, as a general balancing test, the fact that none of them is actually satisfied is certainly probative of the constitutionality of using incidentally collected information in subsequent prosecution.

In *In Re Directives*, the government pointed, as aforementioned, to the targeting and minimization procedures, a procedure to ensure that a significant purpose of the surveillance is to obtain foreign intelligence information, procedures incorporated via Executive Order 12333, and procedures outlined in an affidavit supporting the certifications.[523] 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 §702 (as derived from the to/from or about interpretation) and its subsequent use in criminal prosecution.

VI. CONCLUDING REMARKS

One aspect of both PRISM and upstream collection that has received very little attention is the role of the CIA with regard to the collection of domestic intelligence. Following the Church Committee, an effort was made via FISA and, from 1981, through Executive Order 12333, to circumscribe the CIA's domestic role, limiting it to overseas operations.[524] The latter explicitly forbids the CIA from engaging "in electronic surveillance within the United States except for the purpose of training,

---

[520] 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, Nov. 2011, §3(b)(5)(a)(1)(a), available at http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf. Note, however, that redacted text in the section may refer to an exception to this practice, as it is interspersed with the requirement. *See id.*

[521] 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, Nov. 2011, §3(b)(5)(b), available at http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf.

[522] In re Sealed Case, 310 F.3d at 737-41.

[523] In re Directives at 1013.

[524] *See* LAURA K. DONOHUE, THE COST OF COUNTERTERRORISM (2009); and *Bulk Metadata* (2014).

testing, or conducting countermeasures to hostile electronic surveillance."[525] Instead, bureaucratic division—namely, giving the responsibility of domestic foreign intelligence collection to the FBI—creates protections for U.S. persons.

From what has been released since June 2013, it appears that the CIA is actively engaged in collection under §702. In light of the NSA's to/from or about interpretation, and lowered levels of due diligence regarding U.S. persons as targets and the location of a target—which has resulted in the collection of, by FISC's account, tens of thousands of communications of a wholly domestic nature, there is question now about the extent to which the restrictions previously applied to the CIA still hold. There has been almost no discussion publicly of the CIA's targeting procedures, which have yet to be declassified.

Like the CIA's targeting procedures, there has been no public discussion of the CIA's minimization procedures, even though declassified materials note their existence, as well as FISC's approval of the same.[526] Nor has there been any discussion of the CIA's query of information collected under §702 using U.S. person information. FISC, however, has explicitly recognized (and approved of) CIA use of U.S. person identifiers in the analysis of information collected under §702.[527]

Information also has not been made publicly available about the relationship between information obtained by the NSA and then provided to the CIA. The NSA's minimization procedures note that, "technical data regarding domestic communications may be retained and provided to the FBI and CIA for collection avoidance purposes."[528] This data may include a significant amount of information about U.S. persons, since the NSA is not required to minimize the information prior to transfer. NSA documents explain, "NSA may provide to the Central Intelligence Agency (CIA) unminimized communications acquired pursuant to §702 of the Act." It is then up to the CIA to process the information under separate "minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act."[529]

The lack of information available gives rise to questions about the CIA's role. At a minimum, it appears that the CIA is an active participant in the §702 collection programs. The FISC opinion of Oct. 3, 2011, for instance, released by Obama Administration Aug. 21, 2013, redacts one of the affidavits {DIR/Acting Dir of NSA, Dire of FBI, and [redacted]} submitted for FISC's consideration, but the opinion then notes the submission of three sets of minimization procedures, for use by NSA, FBI, and the CIA.[530]

Outside of considerations about the CIA, what we do know, thus far, is that the NSA appears to be making extensive use of §702. It is doing so through an interpretation of the statutory language that adds "about" to the traditional understanding of the targeting of communications in which the individual or entity under surveillance act actually take part. In-built assumptions, such as the status of

---

[525] Exec. Order 12333, §2.4(a).

[526] FISC Order, John D. Bates, Docket No. 702(i)-08-01, In Re DNI/AG Certification 2008-A, market SECRET "For the reasons stated in the Memorandum Opinion issued contemporaneously herewith, and in reliance on the entire record in this matter, the Court finds, in the language of 50 USC §1881a(i)(3)(A), that the certification submitted. . . as amended, "contains all the required elements" and that the revised NSA, FBI and CIA minimization procedures submitted with the amendment "are consistent with the requirements of [50 USC §1881a(e)] and with the fourth amendment to the Constitution of the United States." 19 Aug. 2010.

[527] October 2011 FISC Memorandum Opinion, pp. 25-26.

[528] July 2009 Minimization procedures, §5, p. 6.

[529] July 2009 Minimization procedures, §6(c)(2), p. 8.

[530] U.S. Foreign Intelligence Surveillance Court, Memorandum Opinion, Oct. 3, 2011, p. 3.

the target (non-U.S. person) and the location (international), allow the agency to gather more information and to sidestep §§703-704 of the FAA.

With regard to post-targeting analysis, minimization procedures draw attention to the breadth of information obtained at the front end even as the statute fails to provide sufficient redress for collection outside of FISC direction. The use of U.S. person information to query data raises the potential for reverse targeting, as recombinant information alters the type of data obtained under §702.

As for the retention and dissemination of information, increasing consumer and industrial reliance on protected communications raises concern about the NSA's policy of automatically retaining all encrypted data, even as "foreign intelligence" remains understood broadly. The use of §702 data, moreover, absent any of the protections otherwise present in Title III, traditional FISA, or §§703-704, raises significant constitutional concerns.

Although the government contends that an exception to the Warrant Clause exists in the realm of foreign intelligence, its claims fall short for the collection of both domestic information and the interception of U.S. persons' information overseas. In nearly four decades, in the post-FISA world, not a single court has held the former, even as the latter has been overtaken by the FAA and Congress' explicit introduction of §§703-704.

Turning to a reasonableness analysis, the collection of information on non-U.S. persons outside the United States takes place entirely outside the Fourth Amendment. But by including information to/from or about a target, the incidental collection of both domestic conversations and the communications of U.S. persons, particularly in light of the potential criminal prosecution of individuals using information obtained from §702 surveillance, raises the protections of the Fourth Amendment.

In 2009, just after the adoption of the FAA, Professor William Banks recognized that, historically, U.S. law has rejected "granting discretion for government to undertake intrusive surveillance of individuals without some showing of suspicious activities."[531] Perhaps the combination of new threats and digitization requires that the government be granted greater latitude to conduct electronic surveillance. But if so, then the elements of discretion that is central to that systems should be subjected to greater, not weaker controls, both at the point of collection and in the subsequent back-end analysis.[532] Without the addition of particularized suspicion, a warrant equivalent, and heightened standards, at some point in the cycle, the statute, NSA practice, and potentially the programs undertaken by the CIA and others, run the risk of violating the protections otherwise afforded under the Fourth Amendment.

[531] Banks (2009-2010), *supra* note 91, at 1636 (internal citations omitted).
[532] Banks (2009-2010), *supra* note 91, at 1636 (internal citations omitted).