On the Bulk Collection of Tangible Things

David S. Kris*

Beginning in June 2013, in response to a series of unauthorized disclosures of classified information, the government confirmed and revealed information about its use of FISA's tangible-things provision, 50 U.S.C. § 1861, to acquire telephony metadata in bulk. This paper discusses that use.[1] Disclosure of the bulk metadata collection also contributed to a broader policy debate concerning the transparency and scope of intelligence activities, particularly signals intelligence, and the role of the FISA Court, among other issues. This paper also discusses those issues.[2]

Unauthorized Disclosures and Historical Context

On June 5, 2013, the Guardian newspaper posted on its website a four-page order signed by Judge Roger Vinson of the FISC,[3] the authenticity of which the government later acknowledged.[4] The order, directed at a subsidiary of a

* Former Assistant Attorney General for National Security, U.S. Department of Justice.

1. This paper was first submitted for prepublication review in mid-July 2013 based on information available as of that time, cleared in September 2013, and then submitted and cleared repeatedly through an iterative process as new information became available, including being submitted on January 28 and cleared in its present form on February 25, 2014. As such, it reflects developments only as of January 28, 2014. An earlier version of this paper was published on Lawfare. David Kris, On the Bulk Collection of Tangible Things (2013), *available at* http://www.lawfareblog.com/wp-content/uploads/2013/09/Lawfare-Research-Paper-Series-No.-4-2.pdf. This paper is reprinted from David S. Kris & J. Douglas Wilson, National Security Investigations and Prosecutions (2d ed. 2012, Thomson Reuters/West) [hereinafter NSIP]. Any further publication of this paper without express permission by the publisher is strictly prohibited.

2. These broader issues pertain not only to the tangible things provision of FISA, 50 U.S.C. § 1861, which is discussed in Chapter 19 of NSIP, *supra* note 1, but also to oversight and regulation of the U.S. Intelligence Community (discussed in Chapter 2), the FISA Court (discussed in Chapter 5), and Congressional and public reporting of information about FISA (discussed in Chapter 13).

3. Glenn Greenwald, *Verizon Forced to Hand over Telephone Data – Full Court Ruling*, The Guardian (June 5, 2013), http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order [hereinafter 215 Bulk Secondary Order].

4. *See, e.g.*, Testimony of James Cole, Deputy Attorney General, before the House Permanent Select Committee on Intelligence (June 18, 2013) [hereinafter June 2013 Open HPSCI Hearing] ("First of all, what we have seen published in the newspaper concerning 215 – this is the business records provisions of the Patriot Act that also modified FISA – you've seen one order in the newspaper that's a couple of pages long that just says that order we're allowed to acquire metadata, telephone records. That's one of two orders. It's the smallest of the two orders. And the other order, which has not been published, goes into great detail about what we can do with that metadata."); James Clapper, DNI Statement on Recent Unauthorized Disclosures of Classified Information (June 6, 2013) [hereinafter June 6, 2013 DNI Statement on Recent Unauthorized Disclosures] ("The judicial order that was disclosed in the press is used to support a sensitive intelligence collection operation"), *available at* http://www.odni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information?tmpl=component&format=pdf. On September 17, 2013, the FISA Court publicly released a redacted opinion and order, filed on August 29, 2013, granting a renewal of the bulk telephony metadata collection program. *See* In re Application of the Federal Bureau of

U.S. telecommunications provider and issued under FISA's tangible-things provision, required production to NSA, "on an ongoing daily basis" for approximately 90 days, of "all call detail records or 'telephony metadata'" for calls with one or both ends in the United States, "including local telephone calls."[5] The order excluded production of metadata concerning "communications wholly originating and terminating in foreign countries."[6]

The FISA Court's order described the metadata to be produced as including "comprehensive routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile state Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call."[7] The order provided that the metadata to be produced "does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer."[8] The order also contained a non-disclosure provision commanding that, with certain exceptions as set forth in the statute, "no person shall disclose to any other person that the FBI or NSA has sought or obtained tangible things under this Order."[9]

Although the June 2013 disclosure understandably caused a sensation, it was not the first time that bulk collection of telephony metadata had been publicly discussed. In the years prior to the unauthorized disclosure, such collection had been reported by the news media, and was the subject of litigation, although it

---

Investigation for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-109 (FISA Ct. 2013) [hereinafter August 2013 FISC Opinion and August 2013 FISC Order], *available at* http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf.

5. 215 Bulk Secondary Order, *supra* note 3, at 2.

6. *Id.*; *see* BUS. RECORDS FISA TEAM, BUSINESS RECORDS FISA NSA REVIEW 15 (2009) [hereinafter NSA End-to-End Review], *available at* http://www.dni.gov/files/documents/section/pub_NSA%20Business%20Records%20FISA%20Review%2020130909.pdf; August 2013 FISC Order, *supra* note 4, at 10 n.10; *cf.* 18 U.S.C. § 2511(2)(f) (2006) ("Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978.").

7. 215 Bulk Secondary Order, *supra* note 3, at 2; *see* August 2013 FISC Opinion, *supra* note 4, at 2 n.2. An IMSI number is typically a 15-digit number that identifies the telephone used in a mobile telephone network, usually associated with the telephone's subscriber identity module (SIM) card that authenticates the telephone to the network. *See International Mobile Subscriber Identity*, WIKIPEDIA, http://en.wikipedia.org/wiki/International_mobile_subscriber_identity. An IMEI number is a similar kind of number identified with the telephone itself. *See* International Mobile Station Equipment Identity, WIKIPEDIA, http://en.wikipedia.org/wiki/Imei.

8. 215 Bulk Secondary Order, *supra* note 3, at 2; *see* August 2013 FISC Opinion, *supra* note 4, at 2 n.2. Under 18 U.S.C. § 2510(8), "contents" is defined to include "any information concerning the substance, purport, or meaning of that communication." For a discussion of this definition and its relevance to FISA, *see* NSIP, *supra* note 1, at §§ 7:11, 18:2, 18:4.

9. 215 Bulk Secondary Order, *supra* note 3, at 2. For a discussion of non-disclosure requirements under the tangible-things provision, *see* NSIP, *supra* note 1, at § 19:5.

had not been confirmed by the government.[10] In 2006, for example, USA Today published an article with the headline, "NSA Has Massive Database of Americans' Phone Calls."[11] The 2006 article explained that shortly after September 11, 2001, NSA approached certain telephone companies and "told the companies that it wanted them to turn over their 'call-detail records,' a complete listing of the calling histories of their millions of customers. In addition, the NSA wanted the carriers to provide updates, which would enable the agency to keep tabs on the nation's calling habits."[12] The article described how certain companies cooperated with NSA, but noted that one company, Qwest, refused: "Unable to get comfortable with what NSA was proposing, Qwest's lawyers asked NSA to take its proposal to the FISA court. According to the sources, the agency refused."[13] A 2006 article in the New Yorker magazine alleged more details on the collection,[14] as did a 2008 article in Newsweek.[15]

A second document published by the Guardian purported to be a March 2009 "working draft" of the NSA Inspector General's report on the President's Surveillance Program (PSP).[16] According to the purported draft report, and as

10. *See, e.g.*, Hepting v. AT & T, 439 F. Supp. 974, 978 (N.D. Cal. 2006) ("Plaintiffs allege that AT & T Corporation (AT & T) and its holding company, AT & T Inc., are collaborating with the National Security Agency (NSA) in a massive warrantless surveillance program that illegally tracks the domestic and foreign communications and communication records of millions of Americans.").

11. Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, at A1. Descriptions of this and other news articles or documents not officially acknowledged by the government should not be understood as an endorsement or verification of any statement made in those articles; the point here is only that the general subject of bulk telephony metadata collection was under discussion, accurately or inaccurately, prior to the June 2013 disclosures.

12. *Id.*

13. *Id.* For an interesting discussion of the legality of the collection in 2007, see PBS Newshour, *From The Archives: NSA Surveillance Seven Years Earlier*, PBS (June 6, 2013), http://www.pbs.org/newshour/rundown/2013/06/from-the-archives-nsa-surveillance-seven-years-earlier.html.

14. Seymour Hersh, *Listening In*, THE NEW YORKER (May 29, 2006), http://www.newyorker.com/archive/2006/05/29/060529ta_talk_hersh.

15. Daniel Klaidman, *Now We Know What the Battle Was About*, NEWSWEEK (Dec. 12, 2008), http://www.thedailybeast.com/newsweek/2008/12/13/now-we-know-what-the-battle-was-about.html. The article referred to "vast and indiscriminate collection of communications data," and "a system in which the National Security Agency, with cooperation from some of the country's largest telecommunications companies, was able to vacuum up the records of calls and e-mails of tens of millions of average Americans between September 2001 and March 2004." As part of that program, the article continued, "NSA's powerful computers became vast storehouses of 'metadata.' They collected the telephone numbers of callers and recipients in the United States, and the time and duration of the calls."

16. NAT'L SEC. AGENCY, OFF. OF THE INSPECTOR GEN., WORKING DRAFT ST-09-0002 (2009) [hereinafter NSA IG Working Draft Report], *available at* http://www.guardian.co.uk/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection; *see* Charlie Savage, *New Leak Suggests Ashcroft Confrontation Was Over N.S.A. Program*, N.Y. TIMES, June 27, 2013, at A6. An unclassified summary of a report by several Inspectors General on the PSP had been released in 2009, but it referred only to the Terrorist Surveillance Program (TSP), which collected the content of communications and is discussed in Chapters 15 and 16 of NSIP, *supra* note 1, and "Other Intelligence Activities," without specifying what those other activities involved. *See* OFFS. OF INSPECTORS GEN., UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM 6 (2009), *available at* http://www.justice.gov/oig/special/s0907.pdf. The government has not acknowledged or declassified the NSA Draft IG Report, as it has for certain other unlawfully disclosed documents, and thus it is referred to here only as a document that is,

later confirmed by an official disclosure in December 2013,[17] both content and Internet and telephony metadata were collected outside the ambit of FISA beginning in October 2001, shortly after the September 11 attacks.[18] In March 2004, a disagreement between the White House and the Department of Justice, which has been recounted in vivid detail elsewhere,[19] apparently caused the President "to discontinue bulk collection of Internet metadata" under the PSP and seek authorization from the FISA Court,[20] but allowed the remaining elements of the program, including collection of content and telephony metadata, to continue without FISA Court authorization.[21] The court issued its first order authorizing bulk collection of internet metadata under FISA's pen-trap provisions in July 2004,[22] which "essentially gave NSA the same authority to collect bulk Internet metadata that it had under the PSP," with a few additional limits.[23] However, collection of bulk telephony metadata is described as having

---

in fact, available the Internet, but without any suggestion that it is or is not what it purports to be, or that any statements within it are accurate. The point of referring to them here is to describe the context in which the ongoing public debate is occurring, not to verify the accuracy of any alleged facts that have not been officially acknowledged, because the public understanding is significant in and of itself, whether or not it is factually accurate in all respects.

17. *See* Unclassified Declaration of Frances J. Fleisch, National Security Agency, at 18-19, Jewel v. NSA, No. 08-cv-4373-JSW (D. Ca. Dec. 20, 2013) [hereinafter December 2013 Fleisch Declaration] ("Starting on October 4, 2001, President Bush authorized" the collection), *available at* http://www.dni.gov/files/documents/1220/NSA%20Fleisch%202013%20Jewel%20Shubert%20Declaration%20Unclassified.pdf.

18. NSA IG Working Draft Report, *supra* note 16, at 1. According to the purported report, the Presiding Judge of the FISA Court was first informed of the collection on January 31, 2002, and the remaining Members of the Court were briefed in January 2006. *Id.* at 24, 37. At least one company, referred to in the purported draft report as COMPANY F, "did not participate in the PSP because of corporate liability concerns," *Id.* at 30, but others did.

19. *See, e.g.*, Dan Eggen & Paul Kane, *Gonzales Hospital Episode Detailed*, WASH. POST, May 16, 2007, at A1 (reporting on "vivid" Congressional testimony by James Comey); Memorandum for the Attorney General (May 6, 2004) [hereinafter May 2004 OLC PSP Opinion], *available at* http://www.justice.gov/olc/docs/memo-president-surveillance-program.pdf.

20. NSA IG Working Draft, *supra* note 16, at 32. The purported NSA Inspector General's draft report explains that the Department of Justice's Office of Legal Counsel (OLC) "found three of the four types of collection authorized under the PSP to be legally supportable. However, it determined that, given the method of collection, bulk Internet metadata [collection] was prohibited by the terms of FISA and Title III," the criminal wiretapping statute. *Id.* at 37. The government has since acknowledged and released FISA Court orders authorizing bulk collection of Internet metadata. *See, e.g.*, FISC Redacted Opinion and Order, *available at* http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf.

21. NSA IG Working Draft, *supra* note 16, at 37. *See also id.* at 39 ("According to NSA personnel, the decision to transition Internet metadata collection to a FISC order was driven by DoJ."). According to the purported draft report, until this confrontation with DOJ, NSA took the position that it could "obtain bulk internet metadata . . . because the NSA did not actually 'acquire' communications until specific communications were selected," e.g., by querying the database containing all of the communications. *Id.* at 38. For a discussion of a similar theory in a different context, see NSIP, *supra* note 1, at § 7:9.

22. *See* December 2013 Fleisch Declaration, *supra* note 17, at 19.

23. NSA IG Working Draft, *supra* note 16, at 39. Those limits are said to have included "specif[ying] the datalinks from which NSA could collect, and [limiting] the number of people that could access the data." *Id.* at 39. The NSA IG Working Draft states that the "FISC continues to renew the [pen-trap authorization] every 90 days," but the report is dated March 2009, and therefore does not reveal

continued for approximately two more years under Presidential authority, and having transitioned to the FISC based on resistance from a provider, rather than any intra-governmental disagreement.[24] The FISC issued its first order authorizing bulk collection of telephony metadata under FISA's tangible-things provision in May 2006,[25] and continued to do so at 90-day intervals thereafter.[26]

ADDITIONAL DISCLOSURES BY THE GOVERNMENT

Shortly after the June 2013 unauthorized disclosure of the FISA Court's order by the Guardian, the government confirmed and declassified the order, and provided additional information about the bulk telephony metadata collection program, both in writing and orally, through official channels.[27] In

---

whether the collection was interrupted or modified in any way thereafter. ODNI has confirmed, however, that the bulk pen-trap collection of internet metadata ended in 2011. *See* Savage, *supra* note 16 (quoting ODNI spokesperson: "The Internet metadata collection program authorized by the FISA court was discontinued in 2011 for operational and resource reasons and has not been restarted"). At a July 17, 2013 hearing of the House Judiciary Committee, government witnesses confirmed the pen-trap bulk collection. *See Oversight of the Administration's use of FISA Authorities, Hearing Before the H. Jud. Comm.*, 113 Cong. (2013) [hereinafter July 2013 HJC Hearing], *available at* http://judiciary.house.gov/_cache/files/b98fdf66-9420-4111-aeda-f64f7fe819c7/113-45-81982.pdf.

24. *See* NSA IG Working Draft, *supra* note 16, at 39 ("According to NSA General Counsel Vito Potenza, the decision to transition telephony metadata to the [FISA] Business Records Order was driven by a private sector company."). In an opinion issued in August 2013, the FISC stated that no provider had challenged any of the FISC's orders directing production of telephony metadata. *See* August 2013 FISC Opinion, *supra* note 4, at 8 n.13, 15-16 ("To date, no holder of records who has receive an Order to produce bulk telephony metadata has challenged the legality of such an Order").

25. In re Application of the Federal Bureau of Investigation for an order Requiring the Production of Tangible Things from [Redacted], No. BR 06-05 (FISA Ct. 2006) [hereinafter May 2006 Order], *available at* http://www.dni.gov/files/documents/section/pub_May%2024%202006%20Order%20from%20FISC.pdf. *See* December 2013 Fleisch Declaration, *supra* note 17, at 19.

26. NSA IG Working Draft, *supra* note 16, at 40; *see* August 2013 FISC Opinion and Order, *supra* note 4. As described in NSIP, *supra* note 1, at §§ 15:1 *et seq.* and 16:1 *et seq.*, collection of content (rather than metadata) was disclosed by the New York Times in 2005, initially authorized by the FISC in January 2007, see NSA IG Working Draft, *supra* note 16, at 38-39, and ultimately authorized by the Protect America Act of 2007 and the FISA Amendments Act of 2008.

27. There were several disclosures made by the government through official channels. Most are catalogued at *Foreign Intelligence Surveillance Act: 2013 Leaks and Declassifications*, LAWFARE (Oct. 1, 2013), http://www.lawfareblog.com/wiki/nsa-papers/. Among the most significant were the following:

> 1. On June 6, 2013, the day after the FISA Court order appeared, the DNI released a "Statement on Recent Unauthorized Disclosures of Classified Information." June 6, 2013 DNI Statement on Recent Unauthorized Disclosures, *supra* note 4.
>
> 2. On June 15, the government released to the news media a short background briefing paper on the recent disclosures. Press Release, Int. Comm., IC Backgrounder on Two NSA Programs (June 15, 2013) [hereinafter June 2013 IC Backgrounder], *available at* http://www.fas.org/sgp/news/2013/06/ic-back.pdf.
>
> 3. On June 18, the NSA posted on its website a two-page paper entitled "Section 215." Press Release, Nat'l Sec. Agency, Section 215 (June 18, 2013) [hereinafter June 2013 NSA Section 215 Backgrounder], *available at* http://www.wyden.senate.gov/news/blog/post/wyden-and-udall-to-general-alexander-nsa-must-correct-inaccurate-statement-in-fact-sheet, which it later removed after complaints about a companion factsheet (concerning the FISA Amendments Act) from Senators Wyden and Udall. *See* Letter from Keith Alexander, Nat'l Sec.

September 2013, the FISA Court released an opinion and order (issued in August 2013) that re-authorized the bulk collection of telephony metadata and

Agency Dir., to Senators Wyden and Udall (June 25, 2013), *available at* http://images.politico.com/global/2013/06/25/nsawydenudallltr.html.

4. Also on June 18, various government officials from NSA, DOJ, and ODNI testified at an open hearing of the House Permanent Select Committee on Intelligence. *How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries, H. Perm. Select Comm. on Int.*, 113 Cong. (2013) [hereinafter June 2013 HPSCI Open Hearing], *available at* http://intelligence.house.gov/hearing/how-disclosed-nsa-programs-protect-americans-and-why-disclosure-aids-our-adversaries.

5. On June 25, 2013, the General Counsel of ODNI participated in a Newseum Special Program. Transcript, NSA Surveillance Leaks: Facts and Fiction, Remarks at the Newseum (June 25, 2013), *available at* http://www.odni.gov/index.php/news10room/speeches-and-interviews/195-speeches-interviews-2013/887-transcript-newseum-special-program-nsa-surveillance-leaks-facts-and-fiction?tmpl=component&format=pdf.

6. On July 16, 2013, the Department of Justice sent a letter to Representative Sensenbrenner responding to an earlier letter from Representative Sensenbrenner to the Attorney General on June 6, 2013. Letter from Dep't of Just. to Rep. Sensenbrenner (July 16, 2013) [hereinafter July 16, 2013 Letter to Sensenbrenner], *available at* http://sensenbrenner.house.gov/uploadedfiles/ag_holder_response_to_congressman_sensenbrenner_on_fisa.pdf; *see also* Letter from Dep't of Just. to Judge William H. Pauley, SDNY (July 18, 2013), *available at* http://www.aclu.org/files/assets/2013.07.18_govt_pre-motion_ltr_to_court.pdf.

7. On July 17, 2013, various government officials from NSA, DOJ, and ODNI testified at an open hearing of the House Judiciary Committee. July 2013 HJC Hearing, *supra* note 23.

8. On July 19, 2013, Bob Litt, General Counsel of ODNI, gave a speech at the Brookings Institution. Bob Litt, Address at the Brookings Institute, Privacy, Technology and National Security: An Overview of Intelligence Collection (July 19, 2013) [hereinafter July 2013 Litt Speech], *available at* http://www.lawfareblog.com/2013/07/odni-gc-bob-litt-speaking-at-brookings/.

9. In an undated letter responding to a letter dated June 27, 2013 from Senator Wyden and others, the DNI sent a letter to Senator Wyden that was received on or about July 26, 2013. Letter from James Clapper, Dir. Nat'l Int., to Sen. Wyden (July 26, 2013) [hereinafter July 2013 DNI Response to 26 Senators], *available at* http://www.wyden.senate.gov/download/?id=285dc9e7-195a-4467-b0fe-caa857fc4e0d.

10. On July 31, 2013, various government officials from NSA, DOJ, and ODNI testified at an open hearing of the Senate Judiciary Committee. *Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs, S. Jud. Comm.*, 113 Cong. (2013) [hereinafter July 2013 SJC Hearing], *available at* http://www.judiciary.senate.gov/hearings/testimony.cfm?id=0d93f03188977d0d41065d3fa041decd&wit_id=0d93f03188977d0d41065d3fa041decd-0-6.

11. Also on July 31, 2013, ODNI declassified various documents relating to the bulk metadata collection. *See* Press Release, Off. of the Dir. Of Nat'l Int., DNI Clapper Declassifies and Releases Telephone Metadata Collection Documents (July 31, 2013, *available at* http://www.odni.gov/index.php/newsroom/press-releases/191-press-releases-2013/908-dni-clapper-declassifies-and-releases-telephone-metadata-collection-documents; DEP'T OF JUST., REPORT ON THE NATIONAL SECURITY AGENCY'S BULK COLLECTION PROGRAMS FOR USA PATRIOT ACT REAUTHORIZATION (2011) [hereinafter 2011 Briefing Documents]; Primary Order, In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-80 (FISA Ct. 2013) [hereinafter 215 Bulk Primary Order].

12. On August 9, 2013, the government released an Administration White Paper. OBAMA ADMIN., ADMINISTRATION WHITE PAPER: BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT (2013) [hereinafter White Paper].

explained the court's reasoning,[28] and subsequent court authorizations were also released to the public.[29] Together, these official disclosures revealed the following:

1. The FISA Court order disclosed in June 2013 is denominated a "Secondary Order" and is directed at a telecommunications provider;[30] the court also issued a "Primary Order" to the government,[31] setting out various requirements and limits on the collection and use of the telephony metadata.[32] The primary and secondary orders are issued by the FISC every 90 days,[33] and have been renewed consistently since May 2006 – including after the unauthorized disclosures.[34] Altogether, as of July 2013, "the court [had] authorized the program on 34 separate occasions by 14 different judges."[35] Although only one secondary order, directed at one company, was disclosed, the government has confirmed that the "FISA Court has repeatedly approved orders directing several telecommunications companies" to produce the telephony metadata,[36] and in public remarks in July 2013, the General Counsel of the NSA referred to "three

13. On September 10, 2013, the government declassified and released a series of FISA Court and other documents primarily concerning compliance issues in the bulk telephony metadata collection program. *See DNI Clapper Declassifies Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (FISA)*, IC ON THE RECORD (Sept. 10, 2013), http://icontherecord.tumblr.com/post/60867560465/dni-clapper-declassifies-intelligence-community.

14. On September 17, 2013, the FISA Court released an opinion and order, dated August 29, 2013 reauthorizing the bulk metadata collection. August 2013 FISC Opinion and August 2013 FISC Order, *supra* note 4.

28. August 2013 FISC Opinion and August 2013 FISC Order, *supra* note 4.

29. *See, e.g.*, In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-158 (FISA Ct. Oct. 11, 2013) [hereinafter October 11, 2013 FISC Opinion], *available at* http://www.uscourts.gov/uscourts/courts/fisc/br13-158-memo-131018.pdf.

30. 215 Bulk Secondary Order, *supra* note 3, at 1.

31. *See* June 2013 HPSCI Open Hearing, *supra* note 27 (statement of James Cole) ("The court sets out the standard that we must meet . . . in its order, and that's in the primary order."). As noted above, a primary order was declassified and released by ODNI on July 31, 2013, *see* 215 Bulk Primary Order, *supra* note 27, and the FISC released an opinion and order (issued in August 2013) in September 2013, *see* August 2013 FISC Opinion and August 2013 FISC Order, *supra* note 4.

32. *See* June 2013 HPSCI Open Hearing, *supra* note 27 (statement of James Cole) ("You've seen one order in the newspaper that's a couple of pages long . . . . That's one of two orders . . . . And the other order, which has not been published, goes into great detail [about] what we can do with that metadata. How we can access it, hoe we can look through it, what we can do with it once we have looked through it . . . .").

33. June 2013 NSA Section 215 Backgrounder, *supra* note 27, at 1; July 16, 2013 Letter to Sensenbrenner, *supra* note 27, at 1.

34. Off. of the Dir. Of Nat'l Int., Press Release, Foreign Intelligence Surveillance Court Renews Authority to Collect Telephony Metadata (July 19, 2013), *available at* http://www.odni.gov/index.php/newsroom/press-releases/191-press-releases-2013/898-foreign-intelligence-surveillance-court-renews-authority-to-collect-telephony-metadata; White Paper, *supra* note 27; August 2013 FISC Opinion and Order, *supra* note 4.

35. July 2013 SJC Hearing, *supra* note 27 (statement of Jim Cole); White Paper, *supra* note 27, at 1.

36. July 2013 Litt Speech, *supra* note 27, at 11; see White Paper, *supra* note 27, at 3 ("certain providers"); *Id.* at 13.

providers" possessing relevant metadata.[37]

2. The metadata collected does not, of course, include the contents[38] of any communication; nor does it include any subscriber's identity,[39] or data about a subscriber's physical location (other than the area code of a telephone number).[40] The information collected is essentially limited to "the telephone numbers in contact, the time and date of the call, and the duration of that call."[41]

3. Once collected, the metadata is stored by NSA in restricted databases with limited access.[42]

---

37. Raj De, Remarks at the Aspen Institute, Counterterrorism, National Security and the Rule of Law (July 18, 2013), *available at* http://aspensecurityforum.org/2013-video (remark is at approximately 18:06 in video). As of December 2013, the government continues to resist formally identifying providers who assisted with bulk metadata collection. See December 2013 Fleisch Declaration, *supra* note 17, at 27-28 (although the participation of a Verizon subsidiary for one 90-day period has been acknowledged, "the continued protection of whether or not, or to what extent, a particular telecommunications provider assisted the NSA under FISC order or otherwise [as to bulk collection of telephony metadata] remains an extraordinarily sensitive and significant matter that the Government continues to protect to avoid even greater harm to national security than has already occurred since June 2013 . . . . I am also supporting the DNI's state secrets privilege assertion, and asserting NSA's statutory privilege, over information relating to which carriers have assisted the NSA under presidential authorization and other authorities.").

38. August 2013 FISC Opinion, *supra* note 4, at 2 n.2. For a discussion of the term "contents" as used in FISA and Title III, the federal wiretap statute, see NSIP, *supra* note 1, at §§ 7:11, 18:2. The bulk collection order is explicit in using the definition from Title III, 18 U.S.C. § 2510(8). 215 Bulk Secondary Order, *supra* note 3, at 2.

39. June 2013 HPSCI Open Hearing, *supra* note 27 (statement of Chris Inglis) (Question: "So there are no names and no addresses affiliated with these phone numbers?" Answer: "No, there are not, sir."); August 2013 FISC Opinion, *supra* note 4, at 2 n.2.

40. August 2013 FISC Opinion, *supra* note 4, at 2 n.2, 4 n.5; June 6, 2013 DNI Statement on Recent Unauthorized Disclosures, *supra* note 4, at 1; June 2013 NSA Section 215 Backgrounder, *supra* note 27, at 1 ("This program concerns the collection only of telephone metadata. Under this program, the government does not acquire the content of any communication, the identity of any party to the communication, or any cell-site locational information"); June 2013 HPSCI Open Hearing, *supra* note 27 (statement of Keith Alexander) (Question: "does the American government have a database that has the GPS location/whereabouts of Americans, whether it's by our cellphones or by other tracking device? Is there – is there a known database?" Answer: "NSA does not hold such a database." Question: "can you figure out the location of the person who made a particular phone call?" Answer: "Not beyond the area code." Question: "Do you have any information about signal strength or tower direction?" Answer: "No we don't . . . . We don't have that in the database."). In its August 2013 opinion, the FISA Court stated: "In the event that the government seeks the production of CSLI [cell site location information] as part of the bulk production of call detail records in the future, the government would be required to provide notice and briefing to this Court pursuant to FISC Rule 11." August 2013 FISC Opinion, *supra* note 4, at 4 n.5.

41. June 2013 HPSCI Open Hearing, *supra* note 27 (statement of Chris Inglis); *see id.* (statement of James Cole) ("It is the number that was dialed from, the number that was dialed to, the date and length of time. That's all we get under 215. We do not get the identity of any of the parties to this phone call. We don't get any cell site or location information as to where any of these phones were located and . . . we don't get any content under this").

42. June 2013 IC Backgrounder, *supra* note 27, at 2; June 2013 NSA Section 215 Backgrounder, *supra* note 27, at 1 ("This metadata is stored in repositories within secure networks, must be uniquely marked, and can only be accessed by a limited number of authorized personnel who have received appropriate and adequate training"); June 2013 HPSCI Open Hearing, *supra* note 27 (statement of Keith Alexander) ("So each set of data that we have – and in this case, let's say the business records FISA – you have to have specific certificates . . . . He would have to get one of those certificates to

4. The stored metadata "may be queried only when there is a reasonable suspicion, based on specific and articulated facts, that an identifier [e.g., a telephone number that is used as the query] is associated with specific foreign terrorist organizations."[43] The queries may not relate to any other foreign intelligence purpose, such as counter-espionage.[44] The government submits and the FISA Court approves a specific list of terrorist groups or targets to which a query must relate.[45]

5. A finding of reasonable, articulable suspicion (RAS) supporting a query must be made initially by one of 22 persons at NSA (20 line personnel and two supervisors); certain selectors as to which the FISC has already found probable cause pursuant to a traditional FISA order (not a FISA Amendments Act directive) for full content surveillance may be deemed to be RAS-approved.[46] The RAS determinations generally must be made in writing, in advance of the query being submitted, and are subject to after-the-fact auditing and review by

---

actually enter that area [of NSA's network or databases]. Does that make sense? In other words, it's a key."); July 16, 2013 Letter to Sensenbrenner, *supra* note 27, at 2 ("only specially cleared counterterrorism personnel specifically trained in the court-approved procedures can access the records to conduct queries"); August 2013 FISC Order, *supra* note 4, at 4-5 & nn.2-3.

43. June 2013 IC Backgrounder, *supra* note 27, at 1; *see* June 2013 HPSCI Open Hearing, *supra* note 27 (statement of Chris Inglis); July 2013 HJC Hearing, *supra* note (statement of James Cole); July 16, 2013 Letter to Sensenbrenner, *supra* note 27, at 2; August 2013 FISC Order, *supra* note 4, at 6-11.

44. June 2013 HPSCI Open Hearing, *supra* note 27 (statement of Chris Inglis) ("It cannot be used to do anything other than terrorism"); July 16, 2013 Letter to Sensenbrenner, *supra* note 27, at 2; July 2013 Litt Speech, *supra* note 27, at 13 ("we only look at a tiny fraction of it, and only for a carefully circumscribed purposes – to help us find links between foreign terrorists and people in the United States"); *cf.* 215 Bulk Primary Order, *supra* note 27, at 7-9.

45. June 2013 NSA Section 215 Backgrounder, *supra* note 27, at 1 ("This metadata may be queried only when there is a reasonable suspicion . . . that the identifier . . . is associated with specific foreign terrorist organizations"); June 2013 HPSCI Open Hearing, *supra* note 27 (statement of James Cole) ("there needs to be a finding that there is reasonable suspicion . . . that the person whose phone records you want to query is involved with some sort of terrorist organization. And they are defined – it's not everyone; they are limited in the [order]"); July 16, 2013 Letter to Sensenbrenner, *supra* note 27, at 2 ("[T]he FISC allows the data to be queried for intelligence purposes only when there is reasonable suspicion, based on specific facts, that a particular query term, such as a telephone number, is associated with a specific foreign terrorist organization that was previously identified and approved by the court."); *Id.* (RAS standard requires link to "a specific foreign terrorist organization that was previously identified to and approved by the court"); July 2013 Litt Speech, *supra* note 27, at 14 ("the Government's applications to collect the telephony metadata have identified the particular terrorist entities that are the subject of the investigations").

46. June 2013 NSA Section 215 Backgrounder, *supra* note 27, at 1; June 2013 HPSCI Open Hearing, *supra* note 27 (statement of Chris Inglis) ("It must be approved by one of those 20 plus two individuals, 20 analysts, specially trained analysts, or their two managers, such that it might then be applied as a query against the data set . . . Any analyst that wants to form a query, regardless of whether it's this authority or any other, essentially has a two-person control rule. They would determine whether this query should be applied, and there is someone who provides oversight on that."); 215 Bulk Primary Order, *supra* note 27, at 7-10; White Paper, *supra* note 27, at 5 ("No more than twenty-two designated NSA officials can make a finding that there is [RAS] that a seed identifier proposed for query is associated with a specific foreign terrorist organization, and NSA's Office of General Counsel must review and approve any such findings for numbers believed to be used by U.S. persons."); August 2013 FISC Order, *supra* note 4, at 7.

other elements of the Executive Branch.[47] A RAS determination endures for 180 days for selectors associated with U.S. persons, and for one year for selectors associated with non-U.S. persons.[48] The FISA Court itself does not routinely approve or review individual queries, and it does not receive regular reports on individual queries, although its sets the criteria for queries and receives regular reports (every 30 days) on the number of identifiers used to query the collected metadata as well as the number of instances in which query results that contain U.S. person information are disseminated by NSA.[49] The Congressional Intelligence Committees also receive regular reporting.[50]

6. In 2012, "less than 300 unique identifiers met this [RAS] standard and were queried,"[51] although it is clear that at least some of the RAS-approved identifiers were used in multiple queries.[52] Initial queries may also produce two

47. June 2013 NSA Section 215 Backgrounder, *supra* note 27, at 1 (describing 30-day reports to the FISC, 90-day meetings of NSA, DOJ, and ODNI, and 90-day meetings between NSA and its Inspector General); June 2013 HPSCI Open Hearing, *supra* note 27 (statement of James Cole) (RAS "is documented in writing ahead of time so that somebody can take a look at it. Any of the accessing that is done is done in an auditable fashion. There is a trail of it. So both the decision and the facts that support the accessing in the query is documented."); July 16, 2013 Letter to Sensenbrenner, *supra* note 27, at 3 ("The basis for a query must be documented in writing in advance and must be approved by a limited number of highly trained analysts"); August 2013 FISC Order, *supra* note 4, at 7, 7 n.6. The FISC's original bulk telephony metadata order, issued in May 2006, identified only seven NSA officials who could approve queries. May 2006 Order, *supra* note 25, at 7.

48. 215 Bulk Primary Order, *supra* note 27, at 10; August 2013 FISC Order, *supra* note 4, at 10. For selectors believed to be used by U.S. persons, NSA's OGC must determine that the RAS determination is not based solely on First Amendment activities. August 2013 FISC Order, *supra* note 4, at 8-9. Selection terms that are approved for surveillance or search under traditional FISA (which requires a showing of probable cause) may be deemed RAS-approved; the same rule does not apply to selectors under surveillance pursuant to the FISA Amendments Act, including not only 50 U.S.C. § 1881a, which does not require any showing of probable cause, but also 50 U.S.C. §§ 1881b and 1881c, which do require a showing of probable cause, albeit in areas not limited to international terrorism and concerning U.S. persons. *See* August 2013 FISC Order, *supra* note 4, at 9-10.

49. June 2013 NSA Section 215 Backgrounder, *supra* note 27, at 1; June 2013 HPSCI Open Hearing, *supra* note 27 (statement of James Cole) ("We do not have to get separate court approval for each query. The court sets out the standard that we must meet in order to make the query in its order, and that's in the primary order . . . . We don't go back to the court each time"); 215 Bulk Primary Order, *supra* note 27, at 16. As discussed below, in a speech delivered on January 17, 2014, the President directed the Attorney General to work with the FISC to require FISC approval of RAS findings absent an emergency. Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014) [hereinafter POTUS Sigint Speech], *available at* http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

50. *See* June 2013 NSA Section 215 Backgrounder, *supra* note 27, at 2. For a discussion of Congressional oversight of FISA, see discussion in text, *infra*, and NSIP, *supra* note 1, at § 13:1 *et seq.*

51. June 2013 IC Backgrounder, *supra* note 27, at 1; July 16, 2013 Letter to Sensenbrenner, *supra* note 27, at 2 ("NSA has reported that fewer than 300 unique identifiers were used to query the data after meeting this standard"). It appears that the actual number of identifiers used may have been 288, although the matter is not entirely clear. *See* July 2013 SJC Hearing, *supra* note 27 (statement of Senator Feinstein) ("Mr. Inglis's statement makes public for the first time a fact, and it's an important fact . . . But – and quote, in 2012 based on those fewer than 300 selectors, that's queries, which actually were 288 for Americans . . . .").

52. June 2013 HPSCI Open Hearing, *supra* note 27 (statement of Chris Inglis) ("So only less than 300 numbers were actually approved for query against that database. Those might have been queried

additional "hops" – i.e., numbers that are connected to numbers that are responsive to queries.[53] As the government explained, "[u]nder the FISC's order, the NSA may also obtain information concerning second and third-tier contacts of the identifier (also referred to as 'hops'). The first 'hop' refers to the set of numbers directly in contact with the seed identifier. The second 'hop' refers to the set of numbers found to be in direct contact with the first 'hop' numbers, and the third 'hop' refers to the set of numbers found to be in direct contact with the second 'hop' numbers."[54] Some of the querying is automated and some is manual.[55] Extending three hops from 300 seed identifiers clearly could in theory embrace a large quantity of telephone numbers, but altogether, in 2012, the NSA reviewed approximately 6,000 telephone numbers as a result of all queries conducted through all hops,[56] and "provided a total of 12 reports to FBI, which altogether 'tipped' less than 500 numbers" generated by the initial queries and hops.[57]

---

multiple times, and therefore, there might be some number greater than that of actual queries against the database.").

53. July 2013 HJC Hearing, *supra* note 23 (statement of Chris Inglis) ("the court has also given permission to do, not just first-hop analysis, meaning what numbers are in contact with that selector [that is used for the initial query] but to then from those numbers, go out two or three hops"). *See* July 2013 SJC Hearing, *supra* note 27 (statement of Chris Inglis) ("they try to be judicious about choosing when to do a second hop or, under the court's authorization, a third hop. Those aren't always exercised."). *See* NSA IG Working Draft, *supra* note 16, at 13 n.6 ("Additional chaining can be performed on the associates' contacts to determine patterns in the way a network of targets may communicate. Additional degrees of separation from the initial target [query] are referred to as 'hops.' For example, a direct contact is one hop away from the target.")

54. White Paper, *supra* note 27, at 4. In his January 17, 2014 speech, the President directed that effective immediately, only two hops, not three, would be permitted. POTUS Sigint Speech, *supra* note 49.

55. 215 Bulk Primary Order, *supra* note 27, at 11. The President's Civil Liberties Oversight Board (PCLOB) reported that the "ultimate result of the automated query process is a repository, the corporate store, containing the records of all telephone calls that are within three 'hops' of every currently approved selection term. Authorized analysts looking to conduct intelligence analysis may then use the records in the corporate store, instead of searching the full repository of records. According to the FISA court's orders, records that have been moved into the corporate store may be searched by authorized personnel 'for valid foreign intelligence purposes, without the requirement that those searches use only RAS-approved selection terms.' Analysts therefore can query the records in the corporate store with terms that are not reasonably suspected of association with terrorism. They also are permitted to analyze records in the corporate store through means other than individual contact-chaining queries that begin with a single selection term: because the records in the corporate store all stem from RAS-approved queries, the agency is allowed to apply other analytic methods and techniques to the query results." PRIVACY & CIV. LIBERTIES OVERSIGHT B., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 30 (2014) [hereinafter PCLOB Report], *available at* http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf. It is not clear that this authority was ever implemented.

56. John Chris Inglis, Outgoing Nat'l Sec. Agency Deputy Dir., Interview on National Public Radio (Jan. 10, 2014) [hereinafter Chris Inglis NPR Interview] ("6,000 numbers is what we actually then touched, all based upon the seeds that started with less than 300"), *available at* http://icontherecord.tumblr.com/post/72883714923/outgoing-nsa-deputy-director-john-inglis.

57. July 2013 SJC Hearing, *supra* note 27 (statement of Chris Inglis). In prior years, the number of tips apparently has been somewhat higher. *See, e.g.,* In re Application of the Federal Bureau of

7. NSA is "not authorized to go into the data nor [is it] data-mining or doing anything with the data other than those queries . . . There are no automated processes running in the background pulling together data, trying to figure out networks."[58] The government did not, of course, foreclose data mining, contact chaining,[59] or other analysis with respect to metadata responsive to queries,[60] or of metadata collected using methods or programs other than the FISC's bulk collection order under the FISA tangible things provision.[61] Moreover, NSA

Investigation for an Order Requiring the Production of Tangible Things from [Redacted], No. 07-04 at 4 n.2 (FISA Ct. May 4, 2007) ("The Court understands that NSA expects that it will continue to provide on average approximately three telephone numbers per day to the FBI"), *available at* http://www.dni.gov/files/documents/11714/FISC%20Order,%20BR%2007-04.pdf.

58. June 2013 HPSCI Open Hearing, *supra* note 27 (statement of Keith Alexander); *see* August 2013 FISC Order, *supra* note 4, at 5 n.7 ("A selection term that meets specific legal standards has always been required. The Court has not authorized government personnel to access the data for the purpose of wholesale 'data mining' or browsing."). Prior to initiation of the FISC-approved bulk collection of telephony metadata in 2006, NSA had developed an "alert list" process to assist it in prioritizing its review of the telephony metadata it received. The alert list contained telephone identifiers that NSA was targeting for collection, including some that had not met the RAS standard, and NSA used an automated system to compare incoming telephony metadata against the alert list identifiers, which was a violation of the FISC's orders. *See* Memorandum of the United States in Response to the Court's Order Dated January 28, 2009, No. BR-08-13 (FISA Ct. Feb. 17, 2009), *available at* www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf.

59. Contact-chaining involves the use of "computer algorithms . . . [to create] a chain of contacts linking communications and identifying additional telephone numbers, IP addresses, and e-mail addresses of intelligence interest." Memorandum for the Attorney General, from Kenneth L. Wainstein, Assistant Attorney General, at 2 (November 20, 2007), *available at* http://www.guardian.co.uk/world/interactive/2013/jun/27/nsa-data-collection-justice-department [hereinafter Wainstein Contact Chaining Memo]. As with the NSA Draft IG Report, the government has not acknowledged or declassified this memorandum, as it has for certain other unlawfully disclosed documents, and thus it is referred to here only as a document that is, in fact, available the Internet, but without any suggestion that it is or is not what it purports to be, or that any statements within it are accurate. The 215 Bulk Primary Order discusses contact chaining through queries. 215 Bulk Primary Order, *supra* note 27, at 6.

60. *See* August 2013 FISC Order, *supra* note 4, at 11-13.

61. Alternative methods of collection would include non-bulk FISA orders, or what prior NSA Directors in the past have referred to as "vacuum cleaner" surveillance outside the ambit of FISA, under Executive Order 12,333 and its subordinate procedures, such as DOD 5240-1.R, and perhaps voluntary production if not otherwise prohibited by law. *See* NSA End-to-End Review, *supra* note 6, at 15; August 2013 FISC Order, *supra* note 4, at 10 n.10 ("The Court understands that NSA receives certain call detail records pursuant to other authority, in addition to the call detail records produced in response to this Court's Orders."); *cf.* 18 U.S.C. § 2511(2)(f) ("Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978"). A purported September 2006 letter from the Acting General Counsel of NSA to the Counsel for Intelligence Policy at DOJ, Attachment B to the Wainstein Contact Chaining Memo, notes that "NSA acquires this communications metdata . . . under Executive Order 12,333. All of the communications metadata that NSA acquires under this authority should have at least one communicant outside the United States." For a discussion of "vacuum cleaner" surveillance, see NSIP, *supra* note 1, at § 16:5 & nn.14, 31, § 16:12 & nn.16, 18, § 16:17. For a discussion of DOD 5240-1.R, see NSIP, *supra* note 1, at §§ 2:7-2:9, Appendix J. The purported Wainstein Contact Chaining Memo discusses such contact chaining with respect to the "large amount of communications metadata," including

technicians may access the metadata to make the data more useable – e.g., to create a "defeat list" to block contact chaining through "high volume identifiers" presumably associated with telemarketing or similar activity.[62]

8. When a query produces information of interest, and the information pertains to a U.S. person, one of 11 persons (holding any of seven senior positions at NSA) must approve before the information may be disseminated outside of NSA (e.g., to the FBI), and it may be disseminated only if it pertains to counterterrorism and is necessary to understand counterterrorism information, or assess its importance.[63]

9. Metadata that has not been reviewed and minimized is retained for five years, consistent with the general five-year retention period for NSA data set out in USSID-18,[64] and is purged automatically from NSA's systems on a rolling

---

metadata associated with persons in the United States, contained in NSA's databases. Wainstein Contact Chaining Memo, *supra* note 59 at 3. The 215 Bulk Primary Order states that the FISA "Court understands that NSA may apply the full range of SIGINT analytic tradecraft to the results of intelligence analysis queries of the collected BR metadata." 215 Bulk Primary Order, *supra* note 27, at 13 n.15.

As the purported Wainstein memorandum explains, the general rule is that "analysis of information legally within the possession of the Government is likely neither a 'search' nor a 'seizure' within the meaning of the Fourth Amendment," Wainstein Contact Chaining Memo, *supra* note 59, at 4 n.4, and therefore may be conducted at will, subject only to specific statutory or other limits, such as FISA minimization procedures governing data collected under FISA. *Id.* at 6 n.8 ("As noted above, some of the metadata the NSA would analyze has been acquired pursuant to FISA and thus is subject to the minimization procedures applicable to that collection. The standard NSA FISA minimization procedures contain no restrictions that would prohibit the metadata analysis described herein."). For a more complete discussion of FISA minimization, see NSIP, *supra* note 1, at §§ 9:1 *et seq.* However, citing to a purported 1984 OLC opinion addressing NSA surveillance outside the scope of FISA, the purported memorandum goes on to analyze the constitutionality of such analysis with respect to data that was lawfully collected. *See* Wainstein Contact Chaining Memo, *supra* note 59, at 4, 4 n.4. If it were occurring, such Fourth Amendment analysis would presumably be most important with respect to non-minimized U.S. person data incidentally collected through vacuum-cleaner surveillance – e.g., surveillance that is not predicated on any showing or finding of probable cause or suspicion.

62. *See* 215 Bulk Primary Order, *supra* note 27, at 5-6; August 2013 FISC Order, *supra* note 4, at 5-6.

63. June 2013 NSA Section 215 Backgrounder, *supra* note 27, at 1; June 2013 HPSCI Open Hearing, *supra* note 27 (statement of Chris Inglis) ("Only seven senior officials at NSA may authorize the dissemination of any information we believe that might be attributable to a U.S. person . . . . And that dissemination in this program would only be made to the Federal Bureau of Investigation, after determining that the information is related to and necessary to understand a counterterrorism initiative."); July 2013 SJC Hearing, *supra* note 27 (statement of Chris Inglis); 215 Bulk Primary Order, *supra* note 27, at 13. This standard is similar in certain ways to the minimization standards governing dissemination of other FISA information. For a discussion of FISA minimization, see NSIP, *supra* note 1, at §§ 9:1 *et seq.* In June 2009, the government informed the FISC that "unminimized results of some queries of metadata [redacted] had been 'uploaded [by NSA] into a database to which other intelligence agencies . . . had access.'" In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted], No. BR-09-06 (FISA Ct. June 22, 2009) (square bracketed material referring to NSA and ellipsis in original), *available at* http://www.dni.gov/files/documents/section/pub_Jun%2022%202009%20Order.pdf.

64. For a discussion of USSID-18, and the five-year retention period, see NSIP, *supra* note 1, at §§ 2:7, 2:18.

basis.[65] Data that is determined to have been improperly collected, e.g., due to a compliance problem, is also purged, as the Deputy Director of NSA explained:

> It gets fairly complicated very quickly, but we have what are called source systems of record within our architecture, and those are the places that we say, if the data element has a right to exist [e.g., was properly collected and has not expired] it's attributable to one of those. If it doesn't have the right to exist, you can't find it in there. And we have very specific lists of information that determine what the provenance of data is, how long that data can be retained. We have on the other side of the coin purge lists that . . . if we were required to purge something [e.g., due to an improper collection], that item would show up explicitly on that list. And we regularly run that against our data sets to make sure that we've checked and double-checked that those things that should be purged have been purged.[66]

10. The bulk telephony metadata collection program has suffered a number of compliance issues,[67] and the FISA Court has been very concerned about the

---

65. June 2013 NSA Section 215 Backgrounder, *supra* note 27, at 2; June 2013 HPSCI Open Hearing, *supra* note 27 (statement of Chris Inglis) (Metadata collected under this program "simply ages off . . . at the expiration of those five years [and] it is automatically taken out of the system, literally just deleted from the system . . . . It's destroyed when it reaches five years of age."); 215 Bulk Primary Order, *supra* note 27, at 14; August 2013 FISC Order, *supra* note 4, at 14.

66. June 2013 HPSCI Open Hearing, *supra* note 27 (statement of Chris Inglis).

67. *See id*. (statement of Bob Litt) ("When compliance problems are identified . . . the vast majority of them are self-identified by NSA"); *Id.* (statement of Keith Alexander) ("Every time we make a mistake . . . they [the FISC judges] work with us to make sure it is done correctly . . . In every case that we've seen so far, we have not seen one of our analysts willfully do something wrong . . . That's where disciplinary action would come in. What I have to overwrite – underwrite – is when somebody makes an honest mistake. These are good people; if they transpose two letters in typing something in, that's an honest mistake. We go back and say, now, how can we fix it? The technical controls that you can see that we're adding in to help fix that. But it is our intent to do this exactly right."); *Id.* (statement of James Cole) ("Every now and then, there may be a mistake . . . . And let me tell you, the FISA court pushes back on this . . . . if there's any compliance issue, it is immediately reported to the FISC. The FISC again pushes back: how did this happen, what are the procedures, what are the mechanisms you're using to fix this; what have you done to remedy it; if you acquired information you should [not] have, have you gotten rid of it as you're required? . . . . We also report quarterly to the FISC concerning the compliance issues that have arisen during that quarter, on top of the immediate reports and what we've done to fix it and remedy the ones that we reported . . . . there has never been found an intentional violation of any of the provisions of a court order or any of the collection in that regard"); White Paper, *supra* note 27, at 5.

In September 2013, the government released a series of FISA Court orders describing in strong terms the Court's concerns about a variety of compliance issues, including (1) improper automated querying of the incoming metadata with non-RAS approved selectors, NSA End-to-End Review, *supra* note 6, at 3-6; (2) inadvertent manual queries of the metadata using 14 non-RAS approved selectors by 3 analysts over a period of approximately 11 weeks, *id.* at 6; (3) omitting the required review by NSA's Office of General Counsel of approximately 3,000 RAS determinations between 2006 and 2009, *id.* at 7; (4) failure to audit a database of query results, *id.* at 8; (5) using telephony metadata selectors identified by data integrity analysts as not appropriate for follow-up investigation to populate similar kinds of defeat lists in other NSA databases, *id.* at 9-10; (6) treating as RAS-approved all selectors associated with a particular person when any selector associated with that person is RAS-approved, *id.* at 11-12; (7) sharing query results with the 98% of NSA analysts not authorized to access the metadata

issues, issuing strong rebukes and adding new restrictions to the program. According to the government, none of the compliance incidents reported to the FISC has been intentional and, since 2009, none has involved application of the RAS standard:[68] in a July 2013 letter, the DNI stated that since "the telephony metadata program under section 215 was initiated [in May 2006], there have been a number of compliance problems that have been previously identified and detailed in reports to the Court and briefings to Congress as a result of Department of Justice reviews and internal NSA oversight. However, there have been no findings of any intentional or bad-faith violations."[69]

---

database, *id.* at 12-13; (8) acquisition of metadata for foreign-to-foreign telephone calls from a provider that believed such metadata to be within the scope of the FISC's orders, when it was not, *id.* at 15; *cf.* August 2013 FISC Order, *supra* note 4, at 10 n.10 ("The Court understands that NSA receives certain call detail records pursuant to other authority, in addition to the call detail records produced in response to this Court's Orders."); *see generally* 18 U.S.C. § 2511(2)(f) ("Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978"); (9) failure to conduct the required OGC review for certain RAS findings, NSA End-to-End Review, *supra* note 6, at 15-16; (10) mistaken inclusion of unminimized query results in a database available to analysis from other U.S. intelligence agencies, *id.* at 16; (11) sharing of query results without the required approvals, *id.* at 16-17; and (12) dissemination of query results to NSA analysts who had not received the proper training. In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, No. BR 09-15 at 3 (FISA Ct. Nov. 5, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Nov%205%202009%20Supplemental%20Opinion%20and%20Order.pdf.

In August 2013, the FISA Court issued an opinion stating the following: "The Court is aware that in prior years there have been incidents of non-compliance with respect to NSA's handling of produced information. Through oversight by the Court over a period of months, those issues were resolved." August 2013 FISC Order, *supra* note 4, at 5 n.8.

68. June 2013 HPSCI Open Hearing, *supra* note 27 (statement of Keith Alexander) ("I don't know of any inaccurate RAS numbers that have occurred since 2009").

69. July 2013 DNI Response to 26 Senators, *supra* note 27, at 3. The DNI's letter went on to explain that the compliance problems "generally involved human error or highly sophisticated technology issues related to NSA's compliance with particular aspects of the Court's orders." *Id*. On September 11, 2013, the Inspector General of NSA sent an unclassified letter to Senator Grassley discussing "12 substantiated instances of intentional misuse of signals intelligence (SIGINT) authorities of the Director of the National Security Agency" since January 1, 2003. George Ellard, Nat'l Sec. Agency Inspector Gen., Letter to Sen. Grassley (Sept. 11, 2013), *available at* http://www.scribd.com/doc/171512150/NSA-letter-on-LOVEINT-and-intentional-misuse-of-NSA-authority. None of those instances involved the bulk telephony metadata collection program. As Chris Inglis, the Deputy Director of NSA explained, "[t]here have been 12 cases over the last 10 or so years where individuals [at NSA] made misuse of the sigint system. They essentially tried to collect a communication that they were not authorized to collect 12 times. The vast majority of these were, in fact, overseas . . . . They were NSAers operating in foreign locations trying to collect the communication of an acquaintance so that they could better understand what the acquaintance was doing, but those acquaintances were foreigners." Chris Inglis NPR Interview, *supra* note 56.

ANALYSIS

The bulk telephony metadata order from the FISC raises at least five statutory issues. First, the collection seems to depend on a theory as to the "relevance" to an FBI terrorism "investigation" of the bulk data being collected. Second, although the FBI applied for the order, as the statute requires, the FISA Court directed the Custodian of Records to produce metadata to NSA, not to the FBI itself. Third, the timing of the production required from the provider – ongoing on a daily basis for many days – also raises questions, both as to the rolling mode of production, and as to the date of the order and the subsequent creation date of some of the records to be produced under it. Fourth, the various restrictions on the use and dissemination of the data as described above, including the RAS query standard, seem to originate from minimization as defined in FISA, and may reflect an emerging approach in an era of what is commonly referred to as "big data." Fifth, it is worth exploring briefly whether and to what extent the legal arguments in support of bulk telephony metadata collection could apply to other kinds of business records. A sixth issue concerns the constitutionality of the collection under the Fourth Amendment.

1. As explained in §§ 19:2-19:3 of NSIP, the tangible-things provision allows certain FBI officials to "make an application for an order requiring the production of any tangible things . . . for an investigation . . . to protect against international terrorism," as long as the investigation is "conducted under guidelines approved by the Attorney General under Executive Order 12333," and is not "conducted of a United States person solely upon the basis of activities protected by the first amendment."[70] The application must include "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment)" that satisfies the requirements described in the previous sentence.[71] To issue a production order, the FISA Court must find that the application "meets the requirements" of the statute, and "may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation," or with a similar production order issued by a court.[72]

The initial question, therefore, is whether there are "reasonable grounds to believe" that telephony metadata, collected in bulk, is "relevant" to an authorized preliminary or full FBI terrorist "investigation" conducted under the appropriate guidelines, or perhaps relevant to multiple investigations.[73] As

70. 50 U.S.C. § 1861(a)(1).

71. 50 U.S.C. § 1861(a)(2).

72. 50 U.S.C. § 1861(c)(1), (c)(2)(D). As discussed in NSIP, *supra* note 1, at § 19:2, some of the requirements in the tangible-things provision apply specially to request for production of certain types of tangible things, such as "library circulation records, library patron lists," and the like. 50 U.S.C. § 1861(a)(3). Those special requirements are not involved in the bulk collection of telephony metadata.

73. As discussed in NSIP, *supra* note 1, at § 19:1, between enactment of the Patriot Act in 2001 and its reauthorization in 2005 and 2006, the government could obtain a tangible-things order "for an

discussed in § 2:18 of NSIP, the FBI's Consolidated Domestic Operations Guidelines (DOG), approved by the Attorney General under Executive Order 12333, divide investigative activity into three or four main categories: assessments (formerly known as "threat assessments," the term used in the tangible things statute); preliminary investigations; full investigations; and enterprise investigations (which are a species of full investigation). Under the DOG, an assessment must have an authorized purpose but does not require any factual predicate – e.g., it does not require any suspicion that someone is committing a crime. A preliminary investigation requires information that a crime or national security threat "may occur" or may have occurred, or that affirmative foreign intelligence "may" be obtained. A full or enterprise investigation requires "an articulable factual basis" to believe that the "may occur" standard has been met.

As described in the DOG, an enterprise investigation is broad in scope:

> The distinctive characteristic of enterprise investigations is that they concern groups or organizations that may be involved in the most serious criminal or national security threats to the public – generally, patterns of racketeering activity, terrorism or other threats to the national security, or the commission of offenses characteristically involved in terrorism as described in 18 U.S.C. 2332b(g)(5)(B). A broad examination of the characteristics of groups satisfying these criteria is authorized in enterprise investigations, including any relationship of the group to a foreign power, its size and composition, its geographic dimensions and finances, its past acts and goals, and its capacity for harm.[74]

---

investigation . . . to protect against international terrorism," with no requirement to show that the tangible things were "relevant" to that investigation. The legislative history of the "relevant" language shows that it was a compromise:

> Section 106 of the conference report is a compromise between section 107 of the House bill and section 7 of the Senate amendment. This section of the conference report amends section 215 of the USA PATRIOT Act to clarify that the tangible things sought by a section 215 FISA order ("215 order") must be "relevant" to an authorized preliminary or full investigation to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities. The provision also requires a statement of facts to be included in the application that shows there are reasonable grounds to believe the tangible things sought are relevant, and, if such facts show reasonable grounds to believe that certain specified connections to a foreign power or an agent of a foreign power are present, the tangible things sought are presumptively relevant. Congress does not intend to prevent the FBI from obtaining tangible items that it currently can obtain under section 215.

H.R. Rep. 109-333, at 90-91 (2005) (Conf. Rep.). As discussed in the text, the FISC issued its first bulk telephony metadata collection order in May 2006, after this language was in effect.

74. DEP'T OF JUST., THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS 18 (2008). *See also id.* at 23-24 (describing the scope and other aspects of enterprise investigations in greater detail). The FBI's Domestic Operations and Investigations Guide (DIOG) provides additional detail on the requirements of an enterprise investigation. *See* FED. B. OF INVEST., DOMESTIC OPERATIONS AND INVESTIGATIONS GUIDE § 8 (2011), *available at* http://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/fbi-domestic-investigations-and-operations-guide-diog-2011-version/fbi-domestic-investigations-and-operations-guide-diog-october-15-2011-part-01-of-03.

It is quite easy to believe – in fact, it would be difficult not to believe – that the FBI has opened full or enterprise investigations into al Qaeda and other international terrorist groups under this authority. As noted above, the government confirmed that the bulk telephony metadata order involves several listed terrorist organizations that are specified in the application and the FISA Court's primary order, and that "we can investigate the organization, not merely an individual or a particular act, if there is a factual basis to believe the organization is involved in terrorism."[75] These investigations have an extremely wide aperture when it comes to the terrorist groups in question, meaning that the FBI seeks to know essentially everything about the groups and how they operate. The FBI could have thousands of open full or enterprise investigations on terrorist groups or targets, and/or their sponsors, some or all of which could underlie the bulk telephony metadata collection applications and orders.[76]

If the authorized "investigations" concern the specified terrorist groups, the question remains whether "there are reasonable grounds to believe" that bulk telephony metadata is "relevant" to those investigations. In its August 2013 opinion, the FISC concluded that there are, explaining: "Because known and unknown international terrorist operatives are using telephone communications, and because it is necessary to obtain the bulk collection of a telephone company's metadata to determine those connections between known and unknown international terrorist operatives as part of authorized investigations, the production of the information sought meets the standard for relevance under Section 215."[77] The FISA Court concluded, by analogy to Fed. R. Evid. 401, that information was "relevant" if it "has some bearing on [the government's] investigations of the identified international terrorist organizations,"[78] and that bulk collection is necessary to find the relevant connections between terrorists.[79] "Because the subset of terrorist communications is ultimately contained within the whole of the metadata produced, but can only be found after the production is aggregated and then queried using identifiers determined to be associated with identified international terrorist organizations, the whole production is relevant to the ongoing investigation out of necessity."[80]

---

75. July 2013 Litt Speech, *supra* note 27, at 14; *see* June 2013 NSA Section 215 Backgrounder, *supra* note 3, at 1 ("This metadata may be queried only when there is a reasonable suspicion . . . that the identifier . . . is associated with specific foreign terrorist organizations"); June 2013 HPSCI Open Hearing, *supra* note 27 (statement of James Cole) ("there needs to be a finding that there is reasonable suspicion . . . that the person whose phone records you want to query is involved with some sort of terrorist organization. And they are defined – it's not everyone; they are limited in the [order]"); July 2013 Litt Speech, *supra* note 27, at 14 ("the Government's applications to collect the telephony metadata have identified the particular terrorist entities that are the subject of the investigations.").

76. *See* White Paper, *supra* note 27, at 6-7 (noting that "there have been numerous FBI investigations in the last several years to which the telephony metadata records are relevant").

77. August 2013 FISC Opinion, *supra* note 4, at 18.

78. *Id.* at 19.

79. *Id.* at 19-22.

80. *Id.* at 22.

This reasoning, echoed by the government in its White Paper[81] and a letter to Congress,[82] is quite similar to arguments made in favor of relevance by outside observers. One of the clearest such arguments is that "large databases are effective in establishing patterns only to the extent they are actually comprehensive"; that when they are comprehensive they can "reveal the organizational details of social structures" like terrorist groups and activities; and that accordingly there are "reasonable grounds to believe that the telephone call metadata data base is relevant to the discovery of that structure and therefore relevant to an investigation of those terrorists."[83] As a former government official put it in

---

81. *See* White Paper, *supra* note 27, at 4 ("It would be impossible to conduct [the] queries effectively without a large pool of telephony metadata to search, as there is no way to know in advance which numbers will be responsive to the authorized queries"). In its August 2013 opinion, the FISA Court stated that it "has not reviewed the government's 'White Paper' and the 'White Paper' has played no part in the Court's consideration of the Government's Application or this Memorandum Opinion." August 2013 FISC Opinion, *supra* note 4, at 3 n.4.

82. The letter explained that the "large volume of telephony metadata is relevant to FBI investigations into specific foreign terrorist organizations because the intelligence tools that NSA uses to identify the existence of potential terrorist communications within the data require collecting and storing large volumes of the metadata to enable later analysis." July 16, 2013 Letter to Sensenbrenner, *supra* note 27, at 2. If the metadata is not collected by NSA, the government explained, it "may not continue to be available . . . because it need not be retained by telecommunications service providers." *Id.* Perhaps more importantly, "unless the data is aggregated by NSA, it may not be possible to identify telephony metadata records that cross different telecommunications networks." *Id.*; *see* July 2013 Litt Speech, *supra* note 27, at 12 ("telephone companies have no legal obligation to keep this kind of information, and they generally destroy it after a period of time determined solely by their own business purposes. And the different telephone companies have separate datasets in different formats, which makes analysis of possible terrorist calls involving several providers considerably slower and more cumbersome").

The need for aggregation across providers is particularly strong, of course, if two or three additional "hops" are conducted following each query: the multiplier effect across two or three generations of additional queries, emanating from a single seed query, each producing some number of responsive numbers of interest that generate further queries, all being done across multiple providers, quickly requires a very large quantity of court orders (or other compulsory process) and would be extremely difficult to manage logistically. Thus, the government argued, "Because the telephony metadata must be available in bulk to allow NSA to identify the records of terrorist communications, there are 'reasonable grounds to believe' that the data is relevant to an authorized investigation to protect against international terrorism, as [the tangible things provision] requires, even though most of the records in the dataset are not associated with terrorist activity." July 16, 2013 Letter to Sensenbrenner, *supra* note 27, at 2.

83. Paul Rosenzwieg, *Answering the 215 Relevance Question . . . And Tracking Paul Revere*, LAWFARE (June 12, 2013), http://www.lawfareblog.com/2013/06/answering-the-section-215-relevance-question-and-tracking-paul-revere/. The blog post explains in more detail the reasoning underlying this conclusion (the post is careful to note that the author is being descriptive, not normative – i.e., not necessarily arguing that the law should permit this, only that it does):

> If your argument is that we need to do a social network analysis to find terrorist connections, then you need the entire network to provide the grist for the mill, so to speak. That, almost surely, is what DNI Clapper meant when he said: "The collection is broad in scope because more narrow collection would limit our ability to screen for and identify terrorism-related communications. Acquiring this information allows us to make connections related to terrorist activities over time."
>
> And, so, that brings us to Paul Revere. Readers who want to see how social network analysis can be done from data sets will find most interesting (and amusing) this post by

testimony before the House Judiciary Committee in July 2013, "the telephone metadata is 'relevant' to counterterrorism investigations because the use of the database is essential to conduct the link analysis of terrorist phone numbers . . . and this type of analysis is a critical building block in these investigations. In order to 'connect the dots,' we need the broadest set of telephone metadata we can assemble, and that's what this program enables."[84]

> Kieran Healey (a sociology professor at Duke) – "Using Metadata to find Paul Revere." Healy did a very simple form of matrix analysis using only two factors – the name of a person and the name of the political clubs he belonged to – and applied it to the colonist revolutionaries. The names were familiar – Sam and John Adams – as were the clubs (the North Party and the Long Room Club, for example). He used data collected from historical records by David Hackett Fisher that might well have been available to the British at the time of the revolution.
>
> The results demonstrate the power of matrix analysis. And, notably, this is only analysis of metadata (who belonged to which clubs) and not at all related to any of the content of what happened inside those clubs.
>
> What he found is quite stunning for those who don't know big data. Perhaps it's a bit of a spoiler to say so (and I urge you, if you are interested, to read the whole paper, which is quite entertaining) but it turns out that the data pop out one man as the lynchpin for a large fraction of the organization of the clubs and the men in Boston – Paul Revere. And while, in historical retrospect he may not have been THE leader of the revolution, it is pretty clear that he was a significant operative in the revolutionary operations. And with just two fields of data British counter-intelligence of the era might have learned about his significance. [Note, of course, that more fields of data gives even greater granularity and fidelity to the conclusions.]
>
> And that, I think, is the answer to the relevance question. It is quite easy, in fact, to say that the large data set can, with appropriate manipulation, reveal the organizational details of social structures. Terrorist activities are social structures of that sort. To my mind it is pretty clear that there are reasonable grounds to believe that the telephone call metadata data base is relevant to the discovery of that structure and therefore relevant to an investigation of those terrorists. I'm not at all surprised that the FISA Court agreed.

84. July 2013 HJC Hearing, *supra* note 23 (statement of Stephen Bradbury). One of the clearest counter-arguments is simply that, in the words of a capable observer, "if that constitutes relevance for purposes of [the tangible things provision] then isn't all data relevant to all investigations?" Benjamin Wittes, *a Correction and a Reiteration*, LAWFARE (June 6, 2013), http://www.lawfareblog.com/2013/06/a-correction-and-a-reiteration/. The blog post explains in more detail the reasoning underlying this concern:

> So presumably, the theory would have to be that the "tangible things" here are the giant ongoing flood of data from the telecommunications companies and that they are "relevant to an authorized investigation," perhaps of Al Qaeda, "to protect against international terrorism." That reading seems oddly consistent with the statutory text, which may be why the intelligence committee leadership seems so comfortable with the program.
>
> But that still leaves the question of how it's possible to regard metadata about all calls to and from a Dominos Pizza in Peoria, Illinois or all calls over a three month period between two small businesses in Juneau, Alaska as "relevant" to an investigation to protect against terrorism. I think the only possible answer to this question is that a dataset of this size could be "relevant" because there are ways of analyzing big datasets algorithmically to yield all kinds of interesting things – but only if the dataset is known to include all of the possibly-relevant material. The individual data may not be relevant, but the dataset or data stream is relevant because it is complete – and therefore is sure to include any communications by whomever we turn out to be concerned about.
>
> But here's the problem: if that constitutes relevance for purposes of Section 215 then isn't all data relevant to all investigations? Grand jury subpoenas, after all, issue on the basis of relevance too – albeit relevance to a criminal investigation. Why couldn't the FBI obtain all

As discussed in §§ 19:1 and 19:5 of NSIP, the tangible things provision states that an order "may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things."[85] In the grand jury context, where the test governing a challenged

---

domestic metadata on the theory that some sort of data-mining would be useful in a mob investigation – and that a complete dataset is therefore "relevant" to it?

85. 50 U.S.C. § 1861(c)(2)(D). There is no question that telephony metadata records generally can be produced via grand jury subpoena, see 18 U.S.C. § 2703(c)(2), and to the extent that this provision limits the general *types* of information that may be obtained, it is clearly satisfied here. For a discussion of the issues pertaining to the *amount* of information that can be obtained, or whether data *sets* rather than individual pieces of data can be collected by grand jury subpoena, see discussion in the text.

In 2008, the FISC issued an opinion addressing whether the tangible-things provision could be used to collect telephone business records in light of 18 U.S.C. § 2702-2703. Supplemental Opinion, In re Production of Tangible Things from [Redacted], No. BR 08-13 (FISA Ct. Dec. 12, 2008), *available at* http://www.dni.gov/files/documents/section/pub_Dec%2012%202008%20Supplemental%20Opinions%20from%20the%20FISC.pdf. The court concluded, after a brief analysis, that it could. The issue has nothing to do with bulk collection per se, but instead concerns whether the tangible-things provision may be used to collect telephone records at all, even on an individual basis.

As one capable commentator has explained, *see* Marty Lederman, *The Kris Paper, and the Problematic FISC Opinion on the Section 215 'Metadata' Collection Program*, JUSTSECURITY (Oct. 1, 2013), http://justsecurity.org/2013/10/01/kris-paper-legality-section-215-metadata-collection/, 18 U.S.C. § 2702(a)(3) generally prohibits a telephone company from providing call detail records to the government, and then (via 18 U.S.C. § 2702(c)(1)) provides several exceptions under which a provider "shall disclose to a governmental entity" such records (as specified in the statute), including "when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena," 18 U.S.C. § 2703(c)(2), or a court order "if the governmental entity [seeking the court order] offers specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation," subject to the proviso that a "court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider." 18 U.S.C. § 2703(d) (incorporated via 18 U.S.C. § 2703(c)(1)(B)). The tangible-things provision is not really an administrative subpoena; nor is it a grand jury subpoena, although it is expressly linked to grand jury subpoenas and administrative subpoenas as discussed in the text above. It is a court order that requires "a statement of facts" (as opposed to "specific and articulable facts") showing "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation" conducted under the DOG, which (as discussed in NSIP, *supra* note 1, at § 2:17) expressly combine intelligence and law enforcement investigations; but there is no requirement for a showing of "materiality."

Nonetheless, as discussed in NSIP, *supra* note 1, at § 19:1, beginning no later than 2005 (shortly after it first started using the tangible things provision), the government sought and the FISC issued more than 140 tangible-things orders for telephone records, as discussed in contemporaneous testimony from Attorney General Gonzales and other communications from the Executive Branch to Congress, and detailed in two reports from the Department of Justice's Inspector General. These tangible-things orders were issued primarily, but not exclusively, in combination with orders for pen/trap surveillance – because, at the time, FISA's pen/trap provisions were interpreted not to allow collection of subscriber information. This led to a legislative fix in the 2006 Patriot Act reauthorization, under which FISA's pen/trap provisions were changed expressly to require production of call detail records, 50 U.S.C. § 1842(d)(2)(C), ending the need for, and use of, "combo" orders. Nothing in the 2006 legislation, however, suggests that Congress intended to change or prohibit the ongoing practice of using the tangible-things provision for collection of telephone records not connected to pen/trap surveillance; on

subpoena is whether there is any "reasonable possibility" that the materials sought "will produce information relevant to the general subject matter of the grand jury's investigation,"[86] the results often depend on the facts, as illustrated by three cases discussed below.

In *In re Grand Jury Proceedings*,[87] the Tenth Circuit held that it was "legal error" for a district court to "redefine[e] the categories of material sought by the Government in order to assess relevancy and further engaging in a document-by-document and line-by-line assessment of relevancy"; that the court was "bound to assess relevancy based on the category of materials sought by the government"; and that the court could not "create new categories for purposes of assessing relevancy."[88] Although it could "sympathize with the district court's desire to prevent the grand jury from subpoenaing wholly irrelevant information," the court of appeals observed that "incidental production of irrelevant documents . . . is simply a necessary consequence of the grand jury's broad investigative powers and the categorical approach to relevancy adopted" by the Supreme Court.[89] Although it appears to require an all-or-nothing approach with respect

---

the contrary, it appears to have been assumed that the FISC would continue to enjoy authority to issue such "pure" tangible-things orders as needed. *See, e.g.*, 151 Cong. Rec. S14006-01 (Dec. 19, 2005), Statement of Senator Sessions, ("With regard to the business records . . . these are records . . . in the control of a bank or telephone company. They are not the words one says in a telephone message, but the telephone toll records"); 151 Cong. Rec. S8220-01 (July 13, 2005), Statement of Senator Specter (referring to Attorney General Gonzales' testimony about the use of the tangible-things provision to obtain telephone records). The 2006 legislation amended the tangible-things provision itself, as discussed in NSIP, *supra* note 1, at §§ 19:1 and 19:2, but the Conference Report explained that "Congress does not intend to prevent the FBI from obtaining tangible items that it currently can obtain under section 215." H.R. REP. NO. 109-133, at 91 (2005) (Conf. Rep). Whatever the technical merits as a textual matter prior to 2006, it seems that all three branches of government publicly understood Section 215 to permit orders for call detail records, and that Congress reenacted the Patriot Act with that interpretation in mind. As such, there is an argument for ratification of the interpretation through enactment of the 2006 legislation, under the standards discussed in the text, *infra*.

Ironically, if the tangible things provision had been interpreted to exclude telephone records, the government apparently could have obtained the information in bulk by using the pen/trap provisions of FISA, which as noted above were amended expressly to authorize collection of the information in 2006, and which underlay the bulk collection of Internet metadata beginning as early as 2004 as mentioned in the text, *supra*. In December 2013, a district court in the Southern District of New York rejected a claim based on Section 2702, concluding that when "[r]ead in harmony, the Stored Communications Act does not limit the Government's ability to obtain information from communications providers under section 215 because section 215 orders are functionally equivalent to grand jury subpoenas. Section 215 authorizes the Government to seek records that may be obtained with a grand jury subpoena, such as telephony metadata under the Stored Communications Act." ACLU v. Clapper, No. 13 Civ. 3994(WHP) (S.D.N.Y., Dec. 27, 2013), 2013 WL 6819708 at *13.

86. U.S. v. R. Enterprises, 498 U.S. 292, 301 (1991). For a discussion of *R. Enterprises* and the use of the grand jury in national security investigations, see NSIP, *supra* note 1, at § 22:1.

87. In re Grand Jury Proceedings, 616 F.3d 1186 (10th Cir. 2010).

88. *Id.* at 1202.

89. *Id.* at 1203. The facts in this case are quite different than in the context of bulk collection of telephony metadata. The subpoenas in question sought documents "regarding [an employee's] involvement in completing" certain forms for the company that employed him, and following an *in camera* review, the district court required production of some, but not all of the documents within the scope of the subpoena, and allowed redactions of other documents. *Id.* at 1191-1192.

to the categories (or sub-categories) of information sought and specified in the subpoena, and despite some expansive language, the decision is not properly read to hold that the presence of even one relevant document in a larger category of documents would support production of the entire category, no matter how broadly it is defined.

A second case, interesting not only because of its holding but also because of its author, is Judge Mukasey's decision *In re Grand Jury Subpoena Duces Tecum Dated November 15, 1993*.[90] There, the court held that two grand jury subpoenas were overbroad in seeking entire hard drives and related floppy disks from the computers of certain employees of a company, as part of an investigation of securities fraud and possible obstruction of justice.[91] There was no question, and the government conceded, that the hard drives and disks contained some material that was wholly irrelevant to the grand jury's investigation, such as a draft will for one employee.[92] The question, then, was whether the appropriate "category of materials" to be assessed was "the information-storage devices demanded, or . . . the documents contained within them."[93] The court held that it was the documents, in part because "the government has acknowledged that a 'key word' search of the information stored on the devices would reveal 'which of the documents are likely to be relevant to the grand jury's investigation,'" but still tried to insist on receiving all of the storage devices in full.[94] Judge Mukasey's decision seems to depend in substantial part on the idea that the government had at its disposal a feasible method of pre-filtering the information to be collected – a concession that the government has not made with respect to its bulk collection of telephony metadata.

Perhaps the closest analogue in the grand jury context, albeit on a much smaller scale than the FISC's order, is *In re Grand Jury Proceedings: Subpoena Duces Tecum*.[95] In that case, "the United States Attorney caused two grand jury subpoenas duces tecum to be served on employees of appellant Western Union Telegraph Company" for records of its customers' wire transfers:[96]

---

90. In re Grand Jury Subpoena Duces Tecum, 846 F. Supp. 11 (S.D.N.Y. 1994) (Mukasey, J.). Judge Mukasey was Attorney General from November 2007 through the end of President George W. Bush's second term. As explained above, the bulk telephony metadata collection was underway in the FISC during this period. Of course, by the time Judge Mukasey was sworn in, the FISA Court had already approved the bulk collection numerous times, and it is quite different to allow continuation of judicially-approved investigative activity than to attempt to initiate it.

91. As described by the court, the "subpoena demands that X Corporation provide the grand jury with the central processing unit (including the hard disk drive) of any computer supplied by X Corporation for the use of specified officers and employees of X Corporation, or their assistants. It demands also all computer-accessible data (including floppy diskettes) created by any of the specified officers and employees or their assistants." *Id.* at 12.

92. *Id.*

93. *Id.*

94. *Id.* at 13.

95. In re Grand Jury Proceedings: Subpoena Duces Tecum, 827 F.2d 301 (8th Cir. 1987).

96. *Id.* at 302.

> The first subpoena requested production of Western Union's Agency Monthly Summary of Activity Report of wire transactions at the Royalle Inn, Kansas City, Missouri for the period January, 1985 through February, 1986. The second subpoena requested production of Western Union's Telegraphic Money Order Applications for amounts of $1,000.00 or more from the Royalle Inn for the period January, 1984 through February, 1986. The Royalle Inn is Western Union's primary wire service agent in the Kansas City area.[97]

In response to Western Union's motion to quash the subpoena, the government maintained that along with law-abiding persons, "drug dealers in Kansas City frequently use Western Union to transmit money in drug deals" under both true and fictitious names.[98] This was enough for the court of appeals to reject Western Union's constitutional and statutory arguments, despite the company's claim that "the subpoena may make available to the grand jury records involving hundreds of innocent people."[99]

The court left open the possibility of narrowing the subpoena on remand, allowing the district court to consider "the extent to which the government would be able to identify in advance those patterns or characteristics [of wire transfers] that would raise suspicion."[100] While it endorsed the idea that a "common law right does not in any way restrict the grand jury's access to records for which the government can make a minimal showing of general relevance," it also allowed the district court to consider "evidence of potentially adverse effects on Western Union's business should it be compelled to produce an overabundance of irrelevant data concerning its customers' transactions" – a factor that seems more significant after the June 2013 disclosures than it did previously.[101]

In the context of administrative or civil subpoenas, which are expressly cross-referenced along with grand jury subpoenas in FISA's tangible things provision,[102] and which also turn on a relevance determination, the courts have upheld relatively broad subpoenas, but as in the grand jury context, no single subpoena discussed in a reported decision is as broad as the FISC's telephony

---

97. *Id.*

98. *Id*.

99. *Id.* at 305.

100. *Id.*

101. *Id.* at 306. *See also* State ex rel. Goddard v. Western Union Financial Services, Inc., 166 P.3d 916 (Ariz. App. 2007) (quashing administrative subpoena under state statute for "data reflecting any wire-transfers made in an amount of $300 or more to any location in Sonora, Mexico from any Western Union location worldwide for a three-year period."); *see generally* Joshua Gruenspecht, Note, *"Reasonable" Grand Jury Subpoenas: Asking for Information in the Age of Big Data*, 24 HARV. J.L. & TECH. 543 (2011).

102. 50 U.S.C. § 1861(c)(2) ("An order under this subsection . . . (D) may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things").

metadata orders.[103] For example, in *Gonzales v. Google*,[104] in connection with a facial challenge to the Child Online Protection Act,[105] the Department of Justice issued a subpoena to Google "to compile and produce a massive amount of information,"[106] and the court found "that 50,000 URLs randomly selected from Google's data base for use in a scientific study of the effectiveness of filters is relevant."[107] In *High Point SARL v. Sprint Nextel Corp.*,[108] although Sprint had produced a spreadsheet containing "over 1.1 million entries" concerning certain hardware components on a network, the court ordered production of the entire database from which the spreadsheet was derived, despite claims that "the . . . database in its entirety includes tremendous quantities of irrelevant information."[109] The court also granted a motion to compel in connection with a demand to "[i]dentify all revenue received by Sprint directly or indirectly from operation of the Sprint CDMA Network (including service revenue and product sales revenue) on a monthly basis since December 1, 2002, with such revenue broken down by each category of revenue separately tracked by Sprint, including by type of traffic (e.g., voice versus data), by geographic location, and by supplier or manufacturer of the Infrastructure Products."[110]

As a matter of the tangible things provision's statutory text, there are at least four ways to approach the issue. First, there is the question of what might be called the relevance ratio – i.e., the ratio of the number of terrorist-related calls to the total number of calls on which metadata is collected. As discussed above, there is language in some cases suggesting that even a single needle will justify collection of a large haystack, but there obviously must be some limiting principle, beyond the government's ability to describe it in the subpoena or court order, on the maximum size of the haystack and the minimum ratio required. Second, there is the related question whether the data set as a whole is somehow more "relevant" than the sum of its parts – e.g., whether the haystack is relevant because it contains all of the needles and allows searches for them in a comprehensive and/or efficient manner that would be impossible if the data were disaggregated. Third, expressing the same idea in the language of a different statutory term, what is the tangible "thing" that must be relevant and that the government may seek – i.e., what is the unit of analysis for evaluating

103. *See* July 2013 Litt Speech, *supra* note 27, at 15 ("[T]he scope of the collection here is broader than typically might be acquired through a grand jury subpoena or civil discovery request," but "the basic principle is similar: the information is relevant because you need to have the broader set of records in order to identify within them the information that is actually important to a terrorism investigation.").

104. Gonzales v. Google, 234 F.R.D. 674 (N.D. Ca. 2006).

105. 47 U.S.C. § 231.

106. 234 F.R.D. at 678.

107. *Id.* at 682.

108. Civil Action No. 09-2269-CM-DJW, 2011 WL 4526770 (D. Kan. Sept. 28, 2011).

109. *Id.* at *12.

110. *Id.* at *10.

relevance?[111] Is it the record of a single telephone call, the record of all calls by a single telephone number, the record of all calls by a single user who may subscribe to multiple numbers, or some larger category up to and including all call detail records for all domestic and one-end-U.S. calls? Does it depend on how the providers maintain the records, and if so, what does this mean in an era of computerized data and records that may be subject to querying by the providers themselves? (For each of these possibilities, there is also a temporal aspect as to the period of time for which the records are sought.) Fourth, if the arguments on the question of relevance are hard to resolve, does the "reasonable grounds" modifier tip the balance?

Regardless of how the question is approached, the answer may ultimately turn on the Supreme Court's observation that the analysis "cannot be reduced to formula; for relevancy and adequacy or excess in the breadth of [a] subpoena are matters variable in relation to the nature, purposes and scope of the inquiry."[112] It is clear that the government's inquiry is both broad and important, and – if statements of officials are to be believed – that the collection is valuable.[113] On the other hand, as the government itself has ar-

111. A related question is whether electronic records are "tangible things" within the meaning of the FISA provision. It is reasonably clear that they are, because the statute refers to "any tangible things (including books, records, papers, documents, and other items)." 50 U.S.C. § 1861(a)(1). As used in the provision, therefore, "records" embraces something different from mere paper "documents." *See* H.R. REP. NO. 109-174(I) at 17-18 (2005).

112. Oklahoma Pub. Press. Co. v. Walling, 327 U.S. 186, 209 (1946).

113. *See, e.g.,* June 2013 IC Backgrounder, *supra* note 27, at 1. On August 17, 2009, the Directors of FBI and NSA submitted affidavits to the FISC describing the value of the bulk telephony metadata collection program. *See* Affidavit of Robert S. Mueller III & Declaration of Lt. Gen. Keith B. Alexander, U.S. Army, Dir. of the Nat'l Sec. Agency, In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted], No. BR 09-09, at 5 (FISA Ct. 2009), *available at* http://www.dni.gov/files/documents/section/pub_August%2019%202009%20Report%20of%20the%20US%20with%20Attachments%2020130910.pdf. In its August 2013 opinion authorizing the collection, the FISC stated that "although not required by statute, the government has demonstrated through its written submissions and oral testimony that this production has been and remains valuable for obtaining foreign intelligence information regarding international terrorist organizations." August 2013 FISC Order, *supra* note 4, at 5-6. One district judge concluded that the bulk collection program was not very valuable: "Given the limited record before me at this point in the litigation – most notably, the utter lack of evidence that a terrorist attack has ever been prevented because searching the NSA database was faster than other investigative tactics – I have serious doubts about the efficacy of the metadata collection program as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism." Klayman v. Obama, No. 13-0851 (RJL) 2013 WL 6571596, at *24 (D.D.C. Dec. 16, 2013) [hereinafter December 2013 Klayman Opinion]. Another district judge referred to the collection as a "vital tool" and concluded: "Any individual call record alone is unlikely to lead to matter that may pertain to a terrorism investigation . . . . But aggregated telephony metadata is relevant because it allows the querying technique to be comprehensive. And NSA's warehousing of that data allows a query to be instantaneous. This new ability to query aggregated telephony metadata significantly increases the NSA's capability to detect the faintest patterns left behind by individuals affiliated with foreign terrorist organizations." ACLU v. Clapper, No. 13 Civ. 3994 (WHP), 2013 WL 6819708, at *18, *27 (SDNY Dec. 27, 2013) [hereinafter ACLU Opinion]. The President's Review Group stated that "there has been no instance in which NSA could say with confidence that the outcome would have been different without the section 215 telephony meta-data program. Moreover, now that the existence of the program has been

gued,[114] it is also clear that only the tiniest fraction of the data collected reflects communications between suspected terrorists and persons in any way associated with terrorism – as noted above, fewer than 300 different seed selectors were run against the metadata in 2012, causing NSA to review approximately 6,000 numbers in total.[115] But having the larger data set on hand for five years may allow for real-time (and after-the fact) mapping of terrorist networks in a way that individualized collection obviously could not achieve, especially given the providers' inconsistent retention of records over time, and the fact that each provider retains only its own records, even though calls are obviously made from one provider's network to another's.[116] As noted above, that is the government's basic argument and the FISA Court's basic conclusion: the telephony metadata must be available in bulk to allow NSA to identify the records of terrorist communications because without access to the larger haystack of data, it cannot find the needles using the much narrower querying process.[117]

Perhaps the best assessment of the program's value was provided by Chris Inglis, the departing Deputy Director of NSA, in January 2014. Inglis explained the limited purpose of the bulk metadata program, which was "precisely defined to cover a seam exposed in the 9/11 terrorist attacks," where "we could see . . .

---

disclosed publicly, we suspect that it is likely to be less useful still." REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 120 n.119 (2013) [hereinafter Review Group Report], *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf. One member of the Review Group, Michael Morrell, wrote in an editorial that while "many commentators said [the Review Group] found no value in the program," this was a "misperception," and that, "Had the program been in place more than a decade ago, it would likely have prevented 9/11." Michael Morrell, Op-Ed, *Correcting the Record on the NSA Review*, WASH. POST DIGITAL (Dec. 27, 2013), http://www.washingtonpost.com/opinions/michael-morell-correcting-the-record-on-the-nsa-recommendations/2013/12/27/54846538-6e45-11e3-aecc-85cb037b7236_story.html. He added: "Personally, I would expand the Section 215 program to include all telephone metadata (the program covers only a subset of the total calls made) as well as e-mail metadata (which is not in the program) to better protect the United States." *Id*. These differing assessments are not necessarily inconsistent factually – instead, they may reflect different standards of efficacy against which the program should be measured, as well as a recognition of the loss of efficacy resulting from public disclosure of the program. However, it does seem reasonably clear that individual members of the President's Review Group have some differences of opinion. *Compare id. with, e.g.*, Geoffrey R. Stone, *The NSA's Telephon Meta-Data Program: Part III*, HUFF. POST (Dec. 31, 2013) http://www.huffingtonpost.com/geoffrey-r-stone/the-nsas-telephone-meta-d_b_4524272.html.

114. July 16, 2013 Letter to Sensenbrenner, *supra* note 27, at 2.

115. *See* June 2013 IC Backgrounder, *supra* note 27, at 1; Chris Inglis NPR Interview, *supra* note 56.

116. June 2013 HPSCI Open Hearing, *supra* note 27 (statement of Chris Inglis) (Question: "And how long do the phone companies on their own maintain data?" Answer: "That varies. They don't hold that data for the benefit of the government; they hold that for their own business internal processes. I don't know the specifics. I know that it is variable. I think that it ranges from six to 18 months and that the data they hold is, again, useful for their purposes, not necessarily the government's"); *see* July 16, 2013 Letter to Sensenbrenner, *supra* note 27, at 2.

117. July 16, 2013 Letter to Sensenbrenner, *supra* note 27, at 2; August 2013 FISC Opinion, *supra* note 4, at 18-23; *see also* July 2013 HJC Hearing, *supra* note 23 (statement of Stephen Brabury) ("The legal standard of relevance in [the tangible things provision] is the same standard used in other contexts. It does not require a separate showing that every individual record in the database is 'relevant' to the investigation; the standard is satisfied if the use of the database as a whole is relevant.").

[a] communication at a [terrorist] safe house overseas but did not know . . . that the [other] end of that [communication] was actually in the United States of America."[118] After describing the role of certain other collection programs in thwarting specific terrorist plots,[119] Inglis acknowledged that the value of the bulk metadata collection is "a harder thing to pin down." As to cases in which "but-for the existence of the metadata you would not have uncovered a plot," the best candidate was probably a "plot that was exposed in San Diego," where "we were able to essentially tell the FBI that an individual was materially involved in terrorism that they had, three years prior, investigated based on a tip and kind of laid that case to rest. And but for the 215 Program, which we essentially tied that individual to some foreign terrorist activity overseas, the FBI would have let that case lain fallow for quite sometime."[120] In other cases, the absence of responses to a metadata query was "useful information to the FBI" because it "gave them confidence that there wasn't a domestic plot," allowing them to "focus their time and attention elsewhere." As Inglis described it, in short, "in a mosaic [of intelligence from many sources, the metadata is] useful to essentially inform other tools. But it's not a silver bullet in and of itself."

Ultimately, Inglis explained, determining how to assess the value of the bulk telephony metadata program itself depended on an assessment of the relative values of liberty and security:

---

118. Chris Inglis NPR Interview, *supra* note 56. A week later, the President made similar points in a speech at the Department of Justice. The President stated:

> The program grew out of a desire to address a gap identified after 9/11. One of the 9/11 hijackers – Khalid al-Midhar – made a phone call from San Diego to a known al Qaeda safe-house in Yemen. NSA saw that call, but it could not see that the call was coming from an individual already in the United States. The telephone metadata program under Section 215 was designed to map the communications of terrorists so we can see who they may be in contact with as quickly as possible. And this capability could also provide valuable in a crisis. For example, if a bomb goes off in one of our cities and law enforcement is racing to determine whether a network is poised to conduct additional attacks, time is of the essence. Being able to quickly review phone connections to assess whether a network exists is critical to that effort.

POTUS Sigint Speech, *supra* note 49.

119. Inglis began by explaining that he and NSA Director Keith Alexander had previously referred publicly to 54 terrorist plots that were thwarted by some form of intelligence collection, including 13 that had a nexus to the U.S. (e.g., an operative being present in the U.S.), and that the metadata program "returned information in 8 of those that we turned over to the FBI." (As to the 54, Inglis explained, "[t]hat's, of course, not the totality of terrorist activity that we might have uncovered and exposed. But we were able to disclose in an unclassified domain, there are about 54 plots.") Inglis explained that "[t]he vast majority of those were uncovered using what's called the 702 Authority [50 U.S.C. § 1881a, discussed in Chapter 17 of NSIP, *supra* note 1], what has been sometimes referred to as Prism. We might for purposes in kind of a plain English way say that that's simply a lawful incept capability." Chris Inglis NPR Interview, *supra* note 56.

120. *Id*. Inglis warned that "I cannot tell you that that wouldn't have turned up some other way. There wouldn't have been some other tool in the tool kit."

> I think we as a nation have to ask ourselves the policy question of what risks do we want to cover? Do we want to cover 100 percent of the risk? Or do we want to perhaps take a risk that from time to time something will get through? 9/11 was the single execution, it was the execution of a single plot with multiple threats. And about 3,000 people lost their lives that day. That's one terrorist plot coming to fruition.
>
> If that is an acceptable cost, if we can say, we can take the risk that we'll miss something, then we don't need to have all of the tools that cover these various seams. We don't need to have the belts and suspenders and Velcro that essentially will overlap in an interlocking way. The 215 is designed to essentially cover a seam that we don't know any other way to cover.[121]

In keeping with this assessment, although the tangible things provision refers to "an investigation" in the singular, it appears (as discussed above) that the bulk collection was conducted in respect of many investigations of multiple, named terrorist targets and/or groups.[122] This raises a separate interpretive question about whether the singular can include the plural,[123] but with respect to the scope of the collection, it suggests that the relevant comparison may not be to any grand jury or other subpoena issued in a single investigation, but instead to the aggregate of subpoenas that could be or were issued in all of what may be thousands of specified terrorism investigations that underlie the bulk metadata collection.[124] In a way, the bulk collection orders represent a kind of aggregation of terrorism-related collection – one-stop shopping across a potentially very large number of ongoing full or enterprise investigations. It reflects the fact that the bulk collection occurs in a unique context.

2. FISA's tangible things provision is unusual in that it discriminates among federal agencies, referring specifically to the FBI rather than any other agency.[125] It authorizes certain FBI officials to make the necessary application,[126] and requires approval from a high-ranking FBI official if the tangible things sought

---

121. *Id.*

122. *See, e.g.*, August 2013 FISC Opinion, *supra* note 4, at 5 (referring to "one of the identified international terrorist organizations").

123. The general rule is that it can, and there does not appear to be anything in the context of FISA or the tangible things provision to counsel against the application of this general rule. *See* 1 U.S.C. § 1 ("In determining the meaning of any Act of Congress, unless the context indicates otherwise . . . words importing the singular include and apply to several persons, parties, or things").

124. June 2013 NSA Section 215 Backgrounder, *supra* note 3, at 1 ("This metadata may be queried only when there is a reasonable suspicion . . . that the identifier . . . is associated with specific foreign terrorist organizations"); June 2013 HPSCI Open Hearing, *supra* note 27 (statement of James Cole) ("There needs to be a finding that there is reasonable suspicion . . . that the person whose phone records you want to query is involved with some sort of terrorist organization. And they are defined – it's not everyone; they are limited in the [order]").

125. This is not unprecedented – for example, national security letter statutes apply in various ways to various agencies, as discussed in Chapter 20 of NSIP, *supra* note 1 – but most other provisions of FISA do not distinguish between agencies.

126. 50 U.S.C. § 1861(a)(1).

are particularly sensitive (e.g., library patron lists).[127] Its language also strongly suggests that the FBI will receive the tangible things pursuant to the FISA Court's order. Thus, for example, it requires the Attorney General to "adopt specific minimization procedures governing the retention and dissemination by the Federal Bureau of Investigation of any tangible things, or information therein, received by the Federal Bureau of Investigation in response to an order under this title,"[128] and requires the application to include "an enumeration of [those] minimization procedures . . . applicable to the retention and dissemination by the Federal Bureau of Investigation of any tangible things to be made available to the Federal Bureau of Investigation based on the order requested in such application."[129] The statute restricts the use of information "acquired from tangible things received by the Federal Bureau of Investigation in response to an order . . . concerning any United States person."[130] The nondisclosure provision of the statute warns that in general, "No person shall disclose to any other person that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to an order under this section."[131]

The FISA Court's bulk collection order disclosed in June 2013 (and other publicly available documents) makes clear that the application underlying the collection was made by the FBI, as required by the statute.[132] But the order directs "the Custodian of Records [to] produce to the National Security Agency (NSA) . . . an electronic copy of the [specified] tangible things,"[133] and the nondisclosure directive refers to the fact "that the FBI or NSA has sought or obtained tangible things under this Order."[134] As such, the order seems to rest on a principle of minimization that national security agencies may share data freely with one another, without alteration, processing, or minimization, in some circumstances. Such an approach would have many practical advantages, particularly in terms of optimizing resources among the agencies. It has roots in FISA's 1978 minimization provisions, as discussed in § 9:3, in situations where one agency is providing technical assistance to another (e.g., decryption), and it may be within the discretion of the FISC to approve, especially if, as may be the case here, the sheer volume of information is challenging for FBI to ingest and retain, and NSA's bandwidth and other technical assistance is therefore required.

3. The tangible things provision states that an order "shall include the date on which the tangible things must be provided, which shall allow a reasonable period of time within which the tangible things can be assembled and made

127. 50 U.S.C. § 1861(a)(3).
128. 50 U.S.C. § 1861(g)(1).
129. 50 U.S.C. § 1861(b)(2)(B).
130. 50 U.S.C. § 1861(h).
131. 50 U.S.C. § 1861(d)(1).
132. 215 Bulk Secondary Order, *supra* note 3, at 1; August 2013 FISC Opinion, *supra* note 4, at 1; August 2013 Order at 1.
133. 215 Bulk Secondary Order, *supra* note 3, at 1-2.
134. *Id.* at 2; *see id.* at 3.

available."[135] The FISC's order disclosed in June 2013 directs the Custodian of Records to produce records "upon service of this Order, and continue production on an ongoing daily basis thereafter for the duration of this Order."[136] The FISC's conclusion, apparently accepted by the Custodian of Records, is that a rolling production ending on the last day of the period specified in the order is within the statutory language.[137] Rolling production is a relatively common approach in grand jury and other subpoena-related cases. As one commentator has explained, "[i]n many instances, the [grand jury] subpoena will require millions of pages of documents to be located, retrieved, reviewed and produced within an unrealistically short time period. Defense counsel can typically negotiate a phased or rolling production that extends over weeks or months."[138] The federal courts have on occasion required production of documents created after the date on which a subpoena was issued, or even after the subpoena's return date.[139] The alternative would be to issue multiple, separate orders seeking the same information on a daily basis; it is easy to see how the government, the FISC, and the Custodian of Records might all prefer the integrated approach actually used by the FISC.[140]

4. The various restrictions on the use and dissemination of the data as described above, including the RAS query standard, originate from minimization as defined in FISA.[141] As explained in § 9:10 of NSIP, the tangible things provision requires the government to adopt minimization procedures governing retention and dissemination of information (there is no requirement for minimi-

---

135. 50 U.S.C. § 1861(c)(2)(B).

136. 215 Bulk Secondary Order, *supra* note 3, at 1-2; *see* August 2013 FISC Order, *supra* note 4, at 3.

137. Rolling production is occasionally used in the context of grand jury subpoenas discussed in court orders. *See, e.g.*, In re Grand Jury Subpoenas, 454 F.3d 511, 524 (6th Cir. 2006).

138. JOHN K. VILLA, 2 CORPORATE COUNSEL GUIDELINES, § 5:17 (2012).

139. *See* Chevron v. Salazar, 275 F.R.D. 437, 449 (S.D.N.Y. 2011); United States v. Int'l Bus. Machines, 83 F.R.D. 92, 96 (S.D.N.Y. 1979) ("Finally, defendant and Anderson argue that the subpoena's imposition of an 'ongoing obligation' to produce documents is an improper attempt to obtain documents not in existence as of the return date of the subpoena. However, the plain language of Rule 26(e)(3), Federal Rules of Civil Procedure, permits the court to impose a duty to supplement responses.").

140. As more and more records become electronically generated and accessible, the functional difference between collection under FISA's tangible things provision and its pen register and trap and trace provisions (50 U.S.C. §§ 1841-1846) becomes smaller. The FISA Court also approved bulk collection of communications metadata under FISA's pen-trap provisions, *see* FISC Redacted Opinion and Order, *supra* note 20, but the government later discontinued that collection, explaining on an ODNI website that "this electronic communications metadata bulk collection program has been discontinued. The Intelligence Community regularly assesses the continuing operational value of all of its collection programs. In 2011, the Director of NSA called for an examination of this program to assess its continuing value as a unique source of foreign intelligence information. This examination revealed that the program was no longer meeting the operational expectations that NSA had for it. Accordingly, after careful deliberation, the Government discontinued the program." *DNI Clapper Declassifies Additional Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act*, IC ON THE RECORD (Nov. 18, 2013), http://icontherecord.tumblr.com/post/67419963949/dni-clapper-declassifies-additional-intelligence.

141. *See* 215 Bulk Primary Order, *supra* note 27, at 4-17.

zation at the acquisition stage of a tangible things collection, because the scope of the authorized acquisition is defined by the court's order itself).[142] Minimization is the clearest statutory source of authority for the limited access and training obligations within NSA, the RAS standard for querying the data and the small number of officials who may approve RAS findings, the limited purpose of the queries (counter-terrorism only), and the procedural and substantive limits on dissemination of information to other agencies that are described above.

These limits are significant not only in and of themselves, insofar as they may affect the overall reasonableness and constitutionality of the telephony metadata collection,[143] but also because of how they reveal the FISA Court and the government working with what is sometimes referred to as "big data." As discussed in a 2009 essay,[144] "the overwhelming increase in the volume and use of digital information left by individuals in the hands of third parties" in recent years "may in the future compel more attention to standards governing retention and dissemination of information. The next generation of surveillance statutes will need to reflect the fact that countless digital footprints left by individuals in the course of modern life – particularly in combination with one another – may contain revealing information. Many of the hardest decisions will lie in balancing privacy interests against investigative needs."[145] The FISC's tangible things order, it appears, represents such an approach, with a vast collection at the front end of the program, and greater restrictions limiting access and use of the data downstream. It contrasts with a more traditional approach in which collection is relatively restricted (e.g., by a requirement to show probable cause for collection of data pertaining to a particular target), but downstream access and use of the collected data is relatively free.

A big-data compliance regime is harder to administer, and harder to follow, than a traditional regime. It is simpler to restrict collection and permit broad access and use of collected data, than it is to permit broad collection and restrict access and use. Big data is inherently hard to manage. That is not to excuse the NSA's compliance problems, or to suggest the inevitability of significant compli-

142. *See* 50 U.S.C. § 1861(g).

143. *See* discussion, *infra*.

144. *See* David 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) [hereinafter FISA Modernization Paper]. I am by no means the first or only person to express this idea. Similar points are made, for example, in the Markle Foundation Task Force's report. THE MARKLE FOUND., PROTECTING AMERICA'S FREEDOM IN THE INFORMATION AGE (2002), *available at* http://belfercenter.hks.harvard.edu/files/part_1.pdf. *See also* July 2013 Litt Speech, *supra* note 27, at 6 ("So on the one hand there are vast amounts of data that contains intelligence needed to protect us . . . . And on the other hand, giving the Intelligence Community access to this data has obvious privacy implications. We achieve both security and privacy in this context in large part by a framework that establishes appropriate controls on what the Government can *do* with the information it lawfully collects, and appropriate oversight to ensure that it respects those controls" (italics in original)).

145. FISA Modernization Paper, *supra* note 144, at 218.

ance shortfalls.[146] It is only to say that, on average, big-data collection regimes will inherently pose greater compliance challenges than traditional collection regimes.

5. It is also worth exploring briefly whether and to what extent the legal arguments in support of bulk telephony metadata collection could apply to other kinds of business records. At a June 2013 hearing of the House Intelligence Committee,[147] a July 2013 hearing of the House Judiciary Committee,[148] and a July hearing of the Senate Judiciary Committee,[149] the issue was raised but not resolved. In a July 2013 letter to Congress, the DNI confirmed the prior use of "FISA authorities" to collect "bulk Internet metadata," but said that "NSA has not used USA PATRIOT Act authorities to conduct bulk collection of any other types of records," did not refer to other agencies or other collection methods, and did refer to "[a]dditional information" provided in a classified supplement to the letter.[150] However, the express reference to grand jury subpoenas in the tangible things statute, coupled with the Western Union case described above, suggests that the legal logic behind the FISC's telephony metadata order might extend to other forms of metadata held by other providers, regardless of whether or not it has in fact been so extended.

On the other hand, the government has expressly disclaimed the universal availability of bulk collection under FISA. The August 2013 White Paper argues that the legality of bulk telephony metadata collection "does *not* mean that any and all types of business records – such as medical records or library or bookstore records – could be collected in bulk under this authority."[151] The government explained that the telephony metadata is "relevant" to FBI investigations in part because it involves communications, "in which connections

146. Some of NSA's compliance problems in this area may stem from its changing mission after September 11, 2001, and the different legal rules that govern surveillance in the U.S. or involving U.S. persons, including after the FAA, as discussed in Chapter 17 of NSIP, *supra* note 1. In this respect, NSA may resemble to some degree a corporation that expands suddenly into a new market, and faces challenges in ensuring that its compliance capabilities keep pace with its operations.

147. June 2013 HPSCI Open Hearing, *supra* note 27. At the hearing, the following colloquy occurred between a Member of the Committee and the Deputy Attorney General:

> Rep. Thompson: Have you previously collected anything else under that authority?
> Mr. Cole: Under the 215 authority?
> Rep. Thompson: Correct.
> Mr. Cole: I'm not sure, beyond the 215 and the 702, that – answering about what we have and haven't collected has been declassified to be talked about.

148. July 2013 HJC Hearing, *supra* note 23 (statement of James Cole) (Question: "Could you demonstrate – could you argue with a straight face you could demonstrate to the court to create a database of everybody's Visa and MasterCard, every transaction that happened in the country because Visa and MasterCard only keep those for a couple years?" Answer: "It is not a simple yes or no, black or white issue. It's a very complicated issue.").

149. July 2013 HJC Hearing, *supra* note 23 (statement of Senator Leahy) ("If our phone records are relevant, why wouldn't our credit card records [be relevant]?").

150. July 2013 DNI Response to 26 Senators, *supra* note 27, at 3.

151. White Paper, *supra* note 27, at 5 (italics in original).

between individual data points are important, and analysis of bulk metadata is the only practical means to find those otherwise invisible connections."[152] In a brief filed in the U.S. Supreme Court in October 2013, the government stated:

> The conclusion that the Telephony Records Program complies with Section 1861 does not suggest . . . that the "relevance" standard has no meaning. The government does not contend that Section 1861 – which applies to all "tangible things," not only telecommunications records – may be used to collect in bulk records of any type. Rather, telecommunications records have characteristics not common to other types of records – specifically, their highly standardized and inter-connected nature – that make them readily susceptible to analysis in large datasets to bring previously unknown connections between and among individuals to light. The same cannot be said of myriad other types of records that might be subject to a Section 1861 order. In the distinctive and particularly critical context of telecommunications, all of the records are relevant to an authorized investigation, because it is only with the full set that this investigative tool can be used most effectively.[153]

Additional insight into any other bulk metadata collection, perhaps not involving communications, will need to await further disclosures.

6. A final issue concerns the constitutionality of the bulk metadata collection. In Smith v. Maryland,[154] the Supreme Court held that telephone company customers have no Fourth Amendment rights in the dialing information that they convey to the telephone company. The Court in Smith relied on its prior decision in United States v. Miller,[155] which found no Fourth Amendment rights of a customer in his bank records held by the bank. As the Court explained in 1984,[156] rejecting constitutional challenges to enforcement of an administrative subpoena, "[i]t is established that, when a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities."[157] In its August 2013 opinion, the FISC relied on Smith and third-party doctrine to conclude that there was no Fourth Amendment violation in the bulk telephony metadata collection (and also noted that none of the providers had invoked a statutory procedure to challenge the orders in the FISC).[158]

---

152. *Id.*

153. Brief for the United States in Opposition at 31-32, In re EPIC, No. 13-58 (S. Ct. Oct. 2013) [hereinafter US EPIC BIO], *available at* http://epic.org/privacy/nsa/in-re-epic/13-58-SG-Brief.pdf.

154. Smith v. Maryland, 442 U.S. 735 (1979).

155. United States v. Miller, 425 U.S. 435 (1976).

156. Sec.& Exchange Comm. v. O'Brien, 467 U.S. 735, 743 (1984).

157. *See, e.g.,* Couch v. United States, 409 U.S. 322, 335 (1973). With respect to the rights of the telephone companies, *see generally* U.S. v. Powell, 379 U.S. 48 (1964) (discussing standards for enforcement of administrative subpoenas); Donovan v. Lone Steer, Inc. 464 U.S. 408 (1984) (recipient of a subpoena may complain if the subpoena is too burdensome and unreasonable).

158. August 2013 FISC Order, *supra* note 4, at 6-9, 14-16.

Judicial reaction outside the FISC has been mixed. In November 2013, a judge in the Southern District of California agreed with the FISC and denied a motion for new trial in a criminal case based on claims that the NSA's collection of bulk telephony metadata violated the Fourth Amendment.[159] Relying on Smith, the court declined the defendant's invitation to "blaze a new path and adopt the approach to the concept of privacy set forth by Justice Sotomayor in her concurrence in United States v. Jones."[160] In that opinion, Justice Sotomayor wrote that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers."[161] The district court concluded that "the Supreme Court specifically and unequivocally held in Smith that retrieval of data from a pen register by the Government without a search warrant is not a search for Fourth Amendment purposes,"[162] and therefore rejected the defendant's Fourth Amendment claim, effectively adhering to the Supreme Court's guidance that where "a precedent of this Court has direct application in a case, yet appears to rest on reasons rejected in some other line of decisions, the [lower courts] should follow the case which directly controls, leaving to this Court the prerogative of overruling its own decisions."[163]

In December 2013, a judge in the District of DC issued (but stayed pending the government's appeal) a preliminary injunction against the bulk collection program, finding a substantial likelihood that it violated the Fourth Amend-

159. United States v. Moalin, No. 10cr4246 JM, 2013 WL 607951 (S.D. Cal. Nov. 14, 2013) [hereinafter November 2013 Moalin Opinion].

160. November 2013 Moalin Opinion, *supra* note 159, at *7 (citing Jones v. United States, 132 S. Ct. 945, 954-64 (2012) (Sotomayor, J., concurring)).

161. *See, e.g.*, Laura K. Donohue, *NSA surveillance may be legal – but it's unconstitutional*, WASH. POST DIGITAL (June 21, 2013), http://articles.washingtonpost.com/2013-06-21/opinions/40110321_1_electronic-surveillance-fisa-nsa-surveillance; July 2013 SJC Hearing, *supra* note 27 (testimony of Jameel Jaffer & Laura W. Murphy, ACLU), *available at* https://www.aclu.org/files/assets/testimony.sjc_.073113.final_.pdf. For a detailed assessment of the constitutional issues here by a capable outside observer, see Orin Kerr, *Metadata, the NSA, and the Fourth Amendment: A Constitutional Analysis of Collecting and Querying Call Records Databases*, VOLOKH CONSPIRACY (July 17, 2013), http://www.volokh.com/2013/07/17/metadata-the-nsa-and-the-fourth-amendment-a-constitutional-analysis-of-collecting-and-querying-call-records-databases/.

162. November 2013 Moalin Opinion at *7.

163. Agostini v. Felton, 521 U.S. 203, 237 (1997) (internal quotation omitted). That is not to suggest that the third-party doctrine underlying Smith v. Maryland has in fact been rejected in another line of decisions, including Jones. Indeed, it seems a deeply rooted element of the Supreme Court's Fourth Amendment jurisprudence. But Judge Miller in Moalin seemed to be saying that, even if Justice Sotomayor's concurrence in Jones were taken as undermining the doctrine, Smith would still control in the lower courts.

ment.[164] The court in DC relied on the conclusion that Smith v. Maryland is outdated, and the logic of Justice Sotomayor's concurring opinion in Jones.[165] In particular, the court rejected Smith on four grounds. First, it observed, "the [collection] in *Smith* was operational for only a matter of days," while the NSA's collection "involves the creation and maintenance of a historical database containing *five years'* worth of data . . . . [and] the very real prospect that the program will go on for as long as America is combatting terrorism, which realistically could be forever!"[166] Second, the court noted, "the relationship between the police and the phone company in *Smith* is *nothing* compared to the relationship that has apparently evolved over the last seven years between the Government and telecom companies."[167] (It was not entirely clear from the opinion whether the court was making the argument that compliance with court-ordered collection on a large scale and over a period of years converts a private party into a governmental actor, or whether it was again emphasizing the relative scope and scale of the NSA's collection.[168]) Third, the court relied on the "almost-Orwellian technology" behind the NSA's collection, and concluded that when Smith was decided in 1979, governmental acquisition of information on such a large scale it "was at best . . . the stuff of science fiction."[169] Fourth, and "*most importantly*," the court concluded, "the nature and quantity of the information contained in people's telephony metadata is much greater" today than it was in 1979.[170] Although "the types of information at issue in this case are relatively limited," as they were in Smith, the dramatic increase in the number of telephones in America – from slightly less than 72 million homes with telephones in 1979 to "a whopping 326,475,248 mobile subscriber connections" today – and the change from letters and post cards to text messages, meant that "people in 2013 have an entirely different relationship with phones than they did" when Smith was decided.[171]

Later that month, another judge, in the Southern District of New York,

164. December 2013 Klayman Opinion, *supra* note 113.

165. 132 S. Ct. 945, 957 (2012).

166. December 2013 Klayman Opinion, *supra* note 113 at *47.

167. *Id.* at *48.

168. *Id.*

169. *Id.* at *49.

170. *Id.* at *50.

171. *Id.* at *50, 53. As of this writing, it is not clear whether Judge Leon's opinion will survive appellate review; and if it does survive, it is not clear whether its logic would extend to other situations involving the third-party rule, including (for example) the vast numbers of reports required by banks and other financial institutions based on the Supreme Court's decision in Miller, a case that underlies Smith. In 2011, banks and other financial institutions filed millions of reports under the Bank Secrecy Act, which the government used "to detect and deter all types of illicit activity, including money laundering, the financing of terrorist activity, and many types of fraud." DEP'T OF THE TREASURY FIN. CRIMES ENFORCEMENT NETWORK, ANNUAL REPORT 6 (2011), *available at* http://www.fincen.gov/news_room/rp/files/annual_report_fy2011.pdf. According to the government, these reports "create a financial trail that law enforcement and intelligence agencies use to track criminals and terrorist networks, their activities, and their assets." *Id.* FinCen "oversees the maintenance of a database with approximately 180 million records of financial transactions and other reports," which "represents the most broadly

disagreed with the district court in DC and upheld the bulk collection program.[172] As a statutory matter, the Southern District court found that "Congress ratified [50 U.S.C. § 1861] as interpreted by the Executive Branch and the FISC, when it reauthorized FISA."[173] Rejecting the DC district court's reasoning explicitly, the Southern District court stated:

> Some ponder the ubiquity of cellular telephones and how subscribers' relationships with their telephones have evolved since Smith. While people may "have an entirely different relationship with telephones than they did thirty-four years ago," this Court observes that their relationship with their telecommunications providers has not changed and is just as frustrating. Telephones have far more versatility now than when Smith was decided, but this case only concerns their use as telephones. The fact that there are more calls placed does not undermine the Supreme Court's finding that a person has no subjective expectation of privacy in telephony metadata. Importantly, "what metadata is has not changed over time," and "[a]s in Smith, the types of information at issue in this case are relatively limited: [tele]phone numbers dialed, date, time, and the like." Because Smith controls, the NSA's bulk telephony metadata collection program does not violate the Fourth Amendment.[174]

Although not a judicial body, the President's Civil Liberties Oversight Board (PCLOB) issued a report in January 2014 concerning the bulk telephony metadata program.[175] Three members of the board concluded that "Section 215 [of the Patriot Act] does not provide an adequate legal basis to support the

---

relied upon and largest source of financial intelligence available to law enforcement authorities at the Federal, State, and local level." *Id.* at 4.

172. ACLU Opinion, *supra* note 113.

173. *Id.* at *16. The court found that the statutory claim was precluded, but stated, "Even if the statutory claim were not precluded, it would fail," and went on to analyze it at some length. *Id.* at *13. The district court identified several occasions on which Congress reauthorized Section 215 of the Patriot Act, albeit some of them for very short periods of time and others of them before the government offered briefings to all Members of Congress:

> See An Act to Amend the USA PATRIOT Act to Extend the Sunset of Certain Provisions of that Act and the Lone Wolf Provision of the Intelligence Reform and Terrorism Provision Act of 2004 to July 1, 2006, Pub. L. No. 109-160, 119 Stat. 2957 (2005); An Act to Amend the USA PATRIOT Act to Extend the Sunset of Certain Provisions of Such Act, Pub. L. No. 109-170, 120 Stat. 3 (2006); USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006); Department of Defense Appropriations Act, 2010, Pub. L. No. 111-118, 123 Stat. 3409 (2009); An Act to Extend Expiring Provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005 and Intelligence Reform and Terrorism Prevention Act of 2004 until February 28, 2011, Pub. L. No. 111-141, 124 Stat. 37 (2010); FISA Sunsets Extension Act of 2011, Pub. L. No. 112-3, 125 Stat. 5 (2011); PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216 (2011).

ACLU opinion, *supra* note 113, at *4 n.4

174. *Id.* at *22 (quoting December 2013 Klayman Opinion).

175. PCLOB Report, *supra* note 55.

program,"[176] that Congress did not ratify the FISC's contrary interpretation when it reenacted the statute,[177] and that the program "raises concerns under both the First and Fourth Amendments to the United States Constitution."[178] Two other members of the board disagreed with these legal conclusions.[179] Interestingly, although the Board found the program to be illegal, and a violation of FISA, it "recognize[d] that the government may need a short period of time to explore and institutionalize alternative approaches, and believes it would be appropriate for the government to wind down the 215 program over a brief interim period."[180]

THE FISA COURT

The June 2013 disclosures gave rise to public discussions concerning the FISC, and in particular concerning (1) the selection method for its judges; and (2) the possibility of something approaching *inter partes* litigation on at least certain matters before the court. Although there is no real evidence of problems in the current process for selecting FISA Court judges, under which the Chief Justice makes the appointments,[181] the vast majority of the Members of the FISC were appointed by Republican Presidents,[182] and it would be relatively easy to change the selection process if desired. The possibility of a civil liberties advocate in the FISC is a more significant and difficult issue.

1. With respect to the selection of FISA Court judges, there have been claims that Chief Justice Roberts has chosen judges appointed by Republican Presidents, and that this has skewed the court in the government's favor.[183] In response, one commentator has observed, "the claim that Chief Justice Roberts's appointments have 'reshaped' the Court to favor the executive branch

176. *Id.* at 10.

177. *Id.* at 10-11.

178. *Id.* at 11.

179. *Id*. at 209-210 (Statement of Rachel Brand); *Id.* at 214 (Statement of Elisebeth Collins Cook).

180. *Id.* at 17. It is not entirely clear how the PCLOB could recommend a wind-down period, rather than an immediate stop, for a collection program it believes is unlawful. The PCLOB did recommend adoption of several privacy enhancements during the wind-down period, but none of them appear to affect the legality of the program. *See id*. The report states: "To be clear, the Board believes that this program has been operated in good faith to vigorously pursue the government's counterterrorism mission and appreciates the government's efforts to bring the program under the oversight of the FISA court. However, the Board concludes that Section 215 does not provide an adequate legal basis to support this program. Because the program is not statutorily authorized, it must be ended." *Id.* at 57.

181. For a discussion of the FISC, including the Chief Justice's authority to appoint judges to it, *see* NSIP, *supra* note 1, at § 5:1 *et seq.* and especially § 5:3.

182. For the current membership of the FISA Court, *see The Foreign Intelligence Surveillance Court*, FED. OF AM. SCIENTISTS, https://www.fas.org/irp/agency/doj/fisa/court2013.html.

183. *See, e.g.*, Sen. Richard Blumenthal, *FISA Court Secrecy Must End*, POLITICO (July 14, 2013), http://www.politico.com/story/2013/07/fisa-court-process-must-be-unveiled-94127.html ("My proposal, which I plan to introduce this month, will bring transparency to the process for selecting FISA court judges and ensure a broader diversity of views on the bench. It also will ensure that FISA court rulings are the product of a process in which both sides have the opportunity to be heard, a process designed to keep the government honest and allow for balanced consideration of difficult issues.").

in applications for warrants does not withstand a moment's scrutiny. That's because the Court's approval rate has always hovered near 100% – both before and after the Roberts era. No discernable reshaping has occurred."[184] Whatever the ideological makeup of the current FISC, as a simple matter of timing, Chief Justice Roberts was confirmed in September 2005, and as noted above the FISC first approved the bulk telephony metadata collection in May 2006, before he had any real impact on the Court's membership.

More broadly, it is important to consider the context in which the FISA Court initially approved the bulk collection. As noted above, bulk telephony metadata collection was occurring before May 2006 pursuant to Presidential authorization and voluntary cooperation from the telecommunications providers.[185] Accordingly, the practical question before the FISC in 2006 was not whether the collection should occur, but whether it should occur under judicial standards and supervision, or unilaterally under the authority of the Executive Branch.[186]

Nonetheless, if desired, it would be possible formally to disperse the authority to select FISA judges. For example, the Chief Judges of the regional courts of appeals could each name a judge, as long as there was some weighting mechanism to ensure a sufficient number of DC-area judges to handle emergencies, and with some reasonable system of rotation to account for the fact that

---

184. Steven Aftergood, *Did Justice Roberts Reshape the FISA Court?*, SECRECY NEWS (July 29, 2013), http://blogs.fas.org/secrecy/2013/07/roberts-reshape/. *See also* Editorial, *More Independence for the FISA Court*, N.Y. TIMES, July 29, 2013, at A16 ("All 11 of the current members were assigned to the court by Chief Justice John Roberts Jr. In the nearly eight years he has been making his selections, Chief Justice Roberts has leaned about as far right as it is possible to go. Ten of those 11 members were appointed to the bench by Republican presidents; the two previous chief justices put Republican-appointed judges on the court 66 percent of the time."). As the Presiding Judge of the FISA Court has pointed out, the approval rate for Title III wiretap applications, which are used in ordinary criminal cases, is similar to the approval rate for FISAs. *See* Letter from Judge Reggie Walton to Senator Patrick Leahy (July 29, 2013) at 2 n.2, 3 n.6 [hereinafter July 2013 Walton-Leahy Letter], ("the approval rate for Title III wiretap applications . . . . is higher than the approval rate for FISA applications"), *available at* http://www.leahy.senate.gov/download/honorable-patrick-j-leahy. Chief Justice Roberts was confirmed in September 2005, and the FISA Court approved the bulk telephony metadata collection in May 2006.

185. *See* December 2013 Fleisch Declaration, *supra* note 17, at 5, 13, 18-19.

186. With respect to metadata concerning foreign-to-foreign communications, which the FISC's order expressly does not address, see 18 U.S.C. § 2511(2)(f). Section 2511(2)(f) exempts from the prohibitions in Title III certain types of production of data by telecommunications providers, but it cannot be used to compel such production. The June 2013 disclosures have affected relationships between the government and the electronic communications providers. As Chris Inglis, Deputy Director of NSA explained, the unauthorized disclosures have "strained" relationships between NSA and the private sector. *See* Chris Inglis NPR Interview, *supra* note 56. As discussed in NSIP, *supra* note 1, at § 16:5, Ken Wainstein, the former Assistant Attorney General for National Security, explained the importance of those relationships: "we rely on the communications providers to do our intelligence surveillances . . . . And there's cooperation and there's cooperation . . . . Yes, we can compel the phone companies, or compel the communications providers to do a surveillance, and even if they . . . resist a directive . . . we can go the FISA Court to get our orders enforced. Problem is, throughout that time, we're dark on whatever surveillance it is that we want to go up on." American Bar Association, Breakfast Program on FISA Reform (March 3, 2008), *available at* http://apps.americanbar.org/natsecurity/multimedia/FISA_reform_panel_March_3_2008_WS_30144.mp3.

there are fewer FISC judges (11) than regional courts of appeals (13).[187] That is effectively how the selection process apparently worked, informally, at least some of the time in the past.[188]

The judicial branch itself, however, has taken the position that no change in the selection process is necessary or appropriate. In a letter to the Chair and Ranking Members of the House and Senate Judiciary and Intelligence Committees, dated January 13, 2014, Judge John Bates, the Director of the Administrative Office of the U.S. Courts and a former Presiding Judge of the FISC, wrote that the Chief Justice is "uniquely positioned . . . to review the federal judiciary and select qualified judges for additional work on the FISC or the Court of Review."[189] Acknowledging that "ten out of the eleven current FISC judges were appointed to the district court bench by Republican presidents,"[190] as discussed above, Judge Bates' letter observed that the "fact that both current Court of Review judges were appointed to the federal appellate bench by a Democratic president receives less attention."[191] Indeed, the letter expressed strong concerns about any "selection process that involves more persons – and especially one that is likely to introduce political factors."[192] The Judiciary's view, as expressed by Judge Bates, is that proposals to disperse the selection authority also "ignore the Chief Justice's unique role in the Judicial Branch" as

187. Another option would be to expand the court, although it is already a relatively large court, especially considering that its members sit part time and are geographically dispersed. *See* NSIP, *supra* note 1, at § 5:3.

188. Testimony of Judge James G. Carr before the Senate Judiciary Committee (July 31, 2013) (discussing how Chief Judge Martin forwarded his name to the Administrative Office of the U.S. Courts, which led to his appointment to the FISC by the Chief Justice), *available at* http://www.judiciary.senate.gov/hearings/testimony.cfm?id=0d93f03188977d0d41065d3fa041decd&wit_id=0d93f03188977d0d41065d3fa041decd-0-6. *See also* Review Group Report, *supra* note 113.

189. Letter from Judge John Bates to Senator Diane Feinstein (Jan. 13, 2014) [hereinafter January 2014 Bates Letter], *available at* http://www.fas.org/irp/news/2014/01/bates.pdf. The letter contains a 14-page paper, dated January 10, 2014, and describes itself as "setting forth the Judiciary's comments concerning certain potential changes to FISA and proceedings before the FISC and the Foreign Intelligence Surveillance Court of Review." It explains that "[t]raditionally, the view of the Judiciary on legislative matters are expressed through the Judicial Conference of the United States, for which I serve as secretary. However, because the matters at issue here relate to special expertise and experience of only a small number of judges on two specialized courts, the Conference has not at this time been engaged to deliberate on them." In preparing the letter, Judge Bates, himself a former Presiding Judge of the FISC, "consulted with the current Presiding Judges of the FISC and the Court of Review, as well as with other judges who serve or have served on those courts." *Id.* at 1.

190. *Id.* at 12 n.15.

191. *Id.* at 12 n.15.

192. *Id.* at 12. The letter also notes that, from time to time, a potential candidate for service on the FISC may fail a background investigation, and that "[k]knowledge of a problematic background investigation would be more widespread if more persons were involved in the selection process." *Id.* at 12. Of course, all federal judges may, in their normal duties, come into contact with FISA information, so it is potentially of concern that some of them are apparently unsuited for service on the FISC based on security concerns. *See, e.g.*, 50 U.S.C. § 1806. The letter also argues that dispersing selection authority would make it more difficult to ensure a sufficient number of DC-area judges on the courts. January 2014 Bates Letter, *supra* note 189, at 13.

the person who normally assigns other judges to serve "on special courts."[193] Such a strongly-worded letter from the Judicial Branch, on matters other than the budget of the federal courts, is quite notable, not only because it apparently reflects the views of the Chief Justice,[194] but also because of the excellent reputation that Judge Bates enjoys.

2. As to the second proposal, concerning a civil liberties advocate in the FISC, the issue is more complex. There are at least three possible versions of such an advocate, each with various costs and benefits, and other possibilities could also be considered. Most of the sensible possibilities are fundamentally designed to provide a counter-weight to the government's advocacy in a very small number of important cases, at the discretion of the FISC judges.[195]

First, the FISC could call on external lawyers, in private practice, on a case-by-case basis as desired in the court's discretion.[196] As noted above, such external advocacy would be needed very rarely, but would be potentially valuable where it is needed. Apart from the discretion of the FISC itself, which would properly control whether an advocate should be appointed, one possible guideline could be FISC Rule 11(b), which requires the government to submit a special memorandum when it presents a new issue to the court, including but not limited to "novel issues of technology or law."[197] Such an approach might assist the FISC, and increase public confidence in its rulings.

However, the use of ad hoc external advocates might also be challenging, especially in the FISC as opposed to the Court of Review.[198] At the outset, it

193. *Id.* at 13.

194. Judge Bates' letter explains that "the Chief Justice of the United States has requested that I act as liaison for the Judiciary on matters concerning the Foreign Intelligence Surveillance Act (FISA)." *Id.* at 1.

195. In testimony before the Senate Judiciary Committee, Judge James Carr, a former Member of the Court, said that there were less than five occasions during his tenure in which such advocacy would have been helpful. Testimony of Judge James G. Carr before the Senate Judiciary Committee (July 31, 2013) ("fewer than the fingers on one hand, I'm sure"), *available at* http://www.judiciary.senate.gov/hearings/testimony.cfm?id=0d93f03188977d0d41065d3fa041decd&wit_id=0d93f03188977d0d41065d3fa041decd-0-6.

196. These lawyers would not be representing a client – e.g., the FISA target – but would instead be aiding the court as a kind of expert consultant. Accordingly, it would likely make sense to compensate them under 5 U.S.C. § 3109 or a similar statute. *Cf.* U.S. v. Salemo, 81 F.3d 1453 (9th Cir. 1996). It may be that the FISC already enjoys the authority to engage such experts under Section 3109, *cf.* July 2013 Walton-Leahy Letter, *supra* note 184, at 7-9, but legislation could remove doubt and reinforce the validity of the practice. In his January 2014 letter to Congress, Judge Bates stated that "FISA does not currently provide a means for the FISC to solicit the assistance of non-governmental entities in considering issues presented by such requests" by the government for surveillance authority. January 2014 Bates Letter, *supra* note 189, at 3.

197. For a discussion of Rule 11(b), see NSIP, *supra* note 1, at § 5:4. Other subsections of Rule 11, which address other situations in which special memoranda are due, could also be triggers for the use of external advocates. In its August 2013 opinion, the FISC stated that Rule 11 would be implicated if the government sought locational information as part of its bulk telephony metadata collection. August 2013 FISC Opinion, *supra* note 4, at 2 n.2, 4 n.5.

198. The Court of Review has received submissions from amici. *See* In re Sealed Case, 310 F.3d 717, 719 & n.1 (FISCR 2011) (per curiam). The FISA Court has also accepted amicus briefs, albeit not in the context of a FISA application. *See* July 2013 Walton-Leahy Letter, *supra* note 184, at 7-9.

might require a more robust form of adversary system than is commonly understood. One of the main challenges in some cases before the FISC is the intersection of complex law and complex facts, particularly concerning rapidly evolving technology, as Rule 11 itself recognizes.[199] An adversary system, therefore, might require a developed approach for cross-examination or depositions of NSA engineers, and perhaps other methods of factual education, in support of an opposing brief written by advocates with very limited, episodic understanding of the technology in question. With respect to non-technological facts – e.g., concerning a potential target – the process for education might also be challenging, although in different ways. As former FISC Presiding Judge Bates put it, "an advocate would not be able to conduct an independent factual investigation, e.g., by interviewing the target or the target's associates," and often "would impair rather than improve the FISC's ability to receive information and rule on applications in an effective and timely manner."[200] Moreover, these advocates also would not be aware of the FISC's jurisprudence on an ongoing basis, so the time needed for them to come up to speed might be significant. Finally, they would need special arrangements for writing and storing highly classified pleadings.[201] All of these issues could be addressed, perhaps, but the process may be more involved, cumbersome, logistically challenging, and perhaps slower than is commonly understood.[202] If it were used very rarely, and when time is not of the essence, it might be made to work, but it would not be a trivial undertaking.[203]

Another option would be to use full-time, executive branch personnel to present the opposing arguments, such as staff in the National Security Division's Oversight Section. This has the virtue of using lawyers with ongoing

199. These cases represent a very small minority of the docket, but tend to produce more significant rulings because they involve new issues. *See* FISC R. 11; *cf.* July 2013 DNI Response to 26 Senators, *supra* note 27, at 3 (compliance problems have "generally involved human error or highly sophisticated technology issues related to NSA's compliance with particular aspects of the Court's orders."). As Judge Carr, a former Member of the FISA Court, explained in testimony before the Senate Judiciary Committee, the appointment of adversary counsel "would not be frequent, and would not occur in the routine kind of cases . . . . Once in a very great while, however, a FISA application raises a novel, substantial, and very difficult issue of law." Testimony of Judge James G. Carr before the Senate Judiciary Committee (July 31, 2013), *available at* http://www.judiciary.senate.gov/hearings/testimony.cfm?id=0d93f03188977d0d41065d3fa041decd&wit_id=0d93f03188977d0d41065d3fa041decd-0-6.

200. January 2014 Bates Letter, *supra* note 189, at 4.

201. In his January 2014 letter to Congress, Judge Bates described the challenges posed by classified information even for the judges on the FISC, noting that "a lack of secure communication and storage facilities makes it very difficult for eight of the eleven judges to review FISC pleadings or communicate about FISC matters when they are in their home districts" rather than at the FISC itself in Washington, DC. *Id.* at 5.

202. *See* July 2013 SJC Hearing, *supra* note 27, Statement of Bob Litt ("[I]f it would help to have some kind of adversary process built into that, I think that would be entirely appropriate. But we shouldn't be trying to make this mimic a criminal trial, because it's a very different process."). *Cf.* Steve Vladeck, *Making FISC More Adversarial: A Brief Response to Orin Kerr*, LAWFARE (July 8, 2013), http://www.lawfareblog.com/2013/07/making-fisc-more-adversarial-a-brief-response-to-orin-kerr/.

203. *See* January 2014 Bates Letter, *supra* note 189, at 5-7.

technological and legal awareness, and access to classified facilities for writing briefs and other documents. It has been proposed, albeit tentatively, by a thoughtful commentator.[204] But it presents other difficulties, including possible cultural difficulties within the Executive Branch. Apart from dissonance at the working level, the Assistant Attorney General for National Security would have to supervise and evaluate both the government's primary advocates and its opponents, and potentially edit both briefs. And as one commentator has said, at a minimum, "it would still 'look' funny."[205] It would be interesting to obtain the views of the Executive Branch, and the Office of Legal Counsel in particular, as to any statutory, constitutional or other issues that would be raised by having the government literally argue both sides of a legal case.

Finally, a third proposal, potentially the most promising, would be to use FISC personnel to formally oppose the government's positions when needed. As discussed in § 5:3 of NSIP, the FISC currently employs several Legal Advisors, who are more experienced than law clerks in a typical court, and who assist the judges in their work.[206] If desired, Congress could expand the cadre of Legal Advisors,[207] and allow and encourage FISC judges to appoint one or more of them formally as an opposition advocate, or "red team," to write the opposing brief in appropriate cases, whether under circumstances described in Rule 11 or otherwise. This would have the virtues of ensuring long-term legal and technological awareness in the government's opponent, easy access to classified facilities, and much easier access to relevant facts (because NSA engineers and other governmental experts are already quite used to answering pointed, factual questions from Court personnel);[208] it would also avoid the cultural and other

204. Orin Kerr, *A Proposal to Reform FISA Court Decisionmaking*, THE VOLOKH CONSPIRACY (July 8, 2013), http://www.volokh.com/2013/07/08/a-proposal-to-reform-fisa-court-decisionmaking/.

205. Vladeck, *supra* note 202.

206. In a letter to the Senate Judiciary Committee, Presiding Judge Walton of the FISC described the role of the Legal Advisors. He explained that "a proposed application must be submitted by the government no later than seven days before the government seeks to have the matter entertained," and that a Legal Advisor then reviews the application and "will often have one or more telephone conversations with the government to seek additional information and/or raise concerns about the application. A Court attorney then prepares a written analysis of the application for the duty judge, which includes an identification of any weaknesses, flaws or other concerns." After consultations between the Legal Advisor and the judge, the Legal Advisor "will then relay the judge's inclination [to grant or deny the application] to the government, and the government will typically proceed by providing additional information, or by submitting a final application." July 2013 Walton-Leahy Letter, *supra* note 184.

207. If desired, Congress could also increase their pay (and hence, presumably, their seniority and perhaps overall quality, although the current cadre of Legal Advisors is of high quality).

208. *See* July 2013 SJC Hearing, *supra* note 27, Statement of Chris Inglis ("We welcome any and all hard questions."); July 2013 Walton-Leahy Letter, *supra* note 184, at 5-6 ("Under FISA practice, the first set of interactions often take place at the staff level. The Court's legal staff frequently interacts with the government in various ways in the context of examining the legal sufficiency of applications before they are presented in final form to a judge . . . . At the direction of the Presiding Judge or the judge assigned to a matter, Court legal staff sometimes meet with the government in connection with applications and submissions. The Court typically requests such meetings when a proposed application or submission presents a special legal or factual concern about which the Court would like additional

issues noted above. One concern, of course, would be that such an approach would give the opposing lawyers an advantage, through their informal interactions with the FISC judges, but this would probably be manageable. Approaching the issue from the other direction, as long as the role of the "red team" was properly defined and supported by the judges, there would be little risk of the designated Legal Advisors becoming "captured" and not vigorously opposing the government's submissions.

This third approach has one additional feature, which is at least arguably a significant virtue, but which may not be widely understood: it maintains, at least formally, the *ex parte* nature of the FISC's regular docket, even if it supplies an opponent to the government from within the court itself on the rare occasions when opposition is needed. Historically, the Department of Justice has taken very seriously the special obligations of candor that flow from the *ex parte* relationship with the FISA Court,[209] and the institutional and long-term value of balanced, sober presentation. In some cases, indeed, the Department has been very strongly criticized for that approach, and for not being enough of an advocate.[210] Creating a full-blown *inter partes* system in the FISC for a few key

---

information (e.g., a novel use of technology or a request to use a new surveillance or search technique) . . . . Court legal staff may meet with the government as often as 2-3 times a week, or as few as 1-2 times a month.").

209. *Cf., e.g.*, ABA Model Rule 3.3(d) ("In an *ex parte* proceeding, a lawyer shall inform the tribunal of all material facts known to the lawyer that will enable the tribunal to make an informed decision, whether or not the facts are adverse.") As the comment to ABA Model Rule 3.3 explains:

> Ordinarily, an advocate has the limited responsibility of presenting one side of the matters that a tribunal should consider in reaching a decision; the conflicting position is expected to be presented by the opposing party. However, in any *ex parte* proceeding, such as an application for a temporary restraining order, there is no balance of presentation by opposing advocates. The object of an *ex parte* proceeding is nevertheless to yield a substantially just result. The judge has an affirmative responsibility to accord the absent party just consideration. The lawyer for the represented party has the correlative duty to make disclosures of material facts known to the lawyer and that the lawyer reasonably believes are necessary to an informed decision."

Id. In his January 2014 letter to Congress, Judge Bates explained that "the government routinely discloses in an application information that is detrimental to its case," January 2014 Bates Letter, *supra* note 189, at 5, and that "the current process benefits from the government's taking on – and generally abiding by – a heightened duty of candor to the Court," *Id.* at 7.

210. *See* NSIP, *supra* note 1, at § 11:5 & n.21; *see also, e.g.*, 148 Cong. Rec. S8649-01 (reprinting article from *The Washington Post*, Dan Eggen and Susan Schmidt, Secret Court Rebuffs Ashcroft (Aug. 23, 2002)) ("FBI and Justice Department officials have said that the fear of being rejected by the FISA court . . . has at times caused both FBI and Justice officials to take a cautious approach to intelligence warrants. Until the current dispute, the FISA court had approved all but one application sought by the government since the court's inception. Civil libertarians claim that record shows that the court is a rubber stamp for the government; proponents of stronger law enforcement say the record reveals a timid bureaucracy only willing to seek warrants on sure winners."); *cf.* 50 U.S.C. § 1804(d). As Carrie Cordero, formerly of the National Security Division at DOJ, testified before the Senate Judiciary Committee in October 2013:

> On that point, it is worth noting that the FISA process, for approximately the preceding fifteen years, was subject to the exact opposite criticism that it seems to be today: the Department of Justice was accused of being too reticent, too cautious, too unwilling to be

cases might have some benefits, as discussed above, but could also result in the erosion of something that has proven valuable over time.[211] The "red team" proposal is most likely to leave that cultural value intact, while still providing the court with the benefits of well-presented opposing viewpoints.

One of the main disadvantages of the red-team proposal – at least as a political matter – is that it may not be, or appear to be, a sufficiently dramatic change from current practice. A variant on the approach designed to satisfy that concern would involve establishment of something like an Office of Defender of Civil Liberties (ODCL). As a formal matter, ODCL could operate as an arm of the FISC, by rough analogy to the Offices of the Federal Public Defender (FPD), which defend persons charged with federal crimes, and operate formally as arms of the various U.S. District Courts under the courts' plans for providing legal services to the indigent.[212] Unlike FPD attorneys, however, the ODCL lawyers would likely not be busy defending civil liberties all of the time,

---

> aggressive under the law in order to protect the national security. This Committee is very familiar with this history. To provide just a few examples: in May 2000, the Report of the Attorney General's Review Team on the Handling of the Los Alamos National Laboratory Investigation was issued. That report concerned the handling of the Wen Ho Lee case, a counterintelligence investigation, and included a critical analysis of the interaction between, and the legal judgment of, the FBI and the Department of Justice concerning their interpretations of FISA standards, such as probable cause, in the late 1990s. In a separate review of the FISA process, this Committee issued a report in February 2003 on FISA Implementation Failures. That report focused primarily on deficiencies in FBI operations, but focused in significant part on problems that prevented the FBI from "aggressively pursuing FISA applications . . ."
>
> A third example arose five years later. In an exchange of letters in October 2008, New York City Police Commissioner Raymond Kelly criticized the Department of Justice under Attorney General Michael Mukasey's tenure of being unwilling to present close or borderline cases to the FISC for consideration. Attorney General Mukasey strongly rejected the NYPD's claims and defended the Department's practice before the Court, stating in part, "[o]ur successful advocacy before the Court depends on the accuracy of our factual representations and the reliability of our assessments of those facts . . . ." Although today's criticisms of FISA operations have now shifted from targeting one agency (FBI) to another (NSA), for those, like me, who worked in national security operational law components during these years, it is an ironic twist to hear today's criticisms that the Department of Justice attorneys in this process may not be adequately representing both the national security as well as civil liberties interests of Americans in their presentations made to the Court; that we need more lawyers scrutinizing already well-scrubbed applications; and that the government should be putting forth more cautious interpretations of the law.

Carrie Cordero, Statement for the Record, United States Senate, Committee on the Judiciary, "Continued Oversight of the Foreign Intelligence Surveillance Act" (Oct. 2, 2013) (footnotes omitted), *available at* http://www.judiciary.senate.gov/pdf/10-2-13CorderoTestimony.pdf.

211. For an opposing position on this issue, *see* Patricia Bellia, *Brave New World: U.S. Responses to the Rise in International Crime*, 50 Vill. L. Rev. 425, 475-476 (2005) ("In terms of legitimacy, the benefits of having security-cleared opposing counsel argue before the FISC are obvious: doing so would ensure that, despite the secrecy of the FISA process, concerns about FISA's application in particular factual contexts were fully aired. Moreover, use of opposing counsel would relieve any pressure on both OIPR and the FISC itself to act as 'devil's advocate' by narrowly interpreting the statute.").

212. *See* 18 U.S.C. § 3006A(g)(2)(A).

because (as noted above) the FISC is likely to need their services only very rarely (unless the office were given the authority to intervene in any case of its choosing, which would likely mean intervention in many cases). In light of that, it might make sense to allow them to perform such other duties on behalf of the FISC as a FISC judge (or perhaps the FISC's Presiding Judge) designates from time to time, as long as those other duties do not interfere with their principal mission – e.g., the duties of a Legal Advisor. This might, however, significantly exacerbate the problem described above, of the civil liberties advocates having closer access to the judges, at least if they have difficulty shedding their institutional outlook when performing work that should be neutral and detached. It may be easier for the Legal Advisors to adopt an opposition mentality in a few cases than it would be for ODCL attorneys to abandon it in most cases. Creating an ODCL could have far-reaching effects.

In choosing among the various alternatives, of course, one important factor would be the preferences of the FISC itself, since the adversary presentation would be designed in the first instance to aid the court's decisions. Judge James Carr, a former Member of the FISC, wrote an editorial in July 2013 suggesting that the FISC be given discretion to appoint outside advocates to oppose the government's positions.[213] In subsequent testimony, however, Judge Carr was careful to point out that he was not speaking for the FISC or for the Judiciary as a whole.[214]

The January 2014 letter from Judge Bates strongly opposed an ODCL or its equivalent, but endorsed the possibility of outside intervention in important cases as determined by FISC judges:

> The participation of a privacy advocate is unnecessary – and could prove counterproductive – in the vast majority of FISA matters, which involve the application of a probable cause or other factual standard to case-specific facts and typically implicate the privacy interests of few persons other than the specified target. Given the nature of FISA proceedings, the participation of an advocate would neither create a truly adversarial process nor constructively assist the [FISA] Courts in assessing the facts, as the advocate would be unable to communicate with the target or conduct an independent investigation. Advocate involvement in run-of-the-mill FISA matters would substantially hamper the work of the Courts without providing any countervailing benefit in terms of privacy protection or otherwise; indeed, such pervasive participation could actually undermine the Courts' ability to receive complete and accurate information in the matters before them.
>
> In those matters in which an outside voice could be helpful, it is critical that the participation of an advocate be structured in a manner than maximizes

213. Judge James G. Carr, *A Better Secret Court*, N.Y. TIMES, July 23, 2013, at A21.

214. Testimony of Judge James G. Carr before the Senate Judiciary Committee (July 31, 2013), *available at* http://www.judiciary.senate.gov/hearings/testimony.cfm?id=0d93f03188977d0d41065d3fa041decd&wit_id=0d93f03188977d0d41065d3fa041decd-0-6.

> assistance to the Courts and minimizes disruption to their work. An advocate appointed at the discretion of the Courts is likely to be helpful, whereas a standing advocate with independent authority to intervene at will could actually be counterproductive.[215]

On January 17, 2014, in a speech delivered at the Department of Justice, President Obama appeared to agree with the approach preferred by the judiciary. He said: "To ensure that the court hears a broader range of privacy perspectives, I am also calling on Congress to authorize the establishment of a panel of advocates from outside government to provide an independent voice in significant cases before the Foreign Intelligence Surveillance Court."[216] This brief statement contains three important elements. First, by referring to a panel of experts from "outside government," the President seemed to be endorsing the first approach described above, in which the FISC calls on advocates from private practice, and rejecting the idea of a permanent ODCL or Public Advocate. Second, by referring to "significant cases," the President seemed to recognize that participation of the outside advocates would be limited. Although he did not say who would determine which cases are "significant" enough to merit such participation, or the criteria used to determine "significance," the likeliest approach seems to be to rely on the judges of the FISC. This was perhaps the most notable aspect of his statement: it did not call for mandatory participation by an outside advocate. Finally, however, by calling on Congress to authorize the panel of advocates, the President obviously left open the possibility that another approach might prevail.[217]

SECRECY, TRANSPARENCY, AND THE SCOPE OF SIGNALS INTELLIGENCE

Apart from their impact on the FISC and its operations, the June 2013 disclosures and ensuing reaction also illustrate the tensions, and the ongoing need to calibrate, between the sometimes-competing values of secrecy and transparency. This tension exists both (1) within the federal government, and (2) between the federal government as a whole and the American people.[218] As

---

215. January 2014 Bates Letter, *supra* note 189, at 2 (bullet points omitted, emphasis added).

216. POTUS Sigint Speech, *supra* note 49.

217. In its report, the PCLOB made a similar recommendation: "Congress should enact legislation enabling the FISC to hear independent views, in addition to the government's views, on novel and significant applications and in other matters in which a FISC judge determines that consideration of the issues would merit such additional views." PCLOB Report, *supra* note 55, at 17.

218. The disclosures also seem destined to be viewed in the historical context of the immediately antecedent (and somewhat overlapping) national debate concluding that traditional newsgathering techniques, such as encouraging and/or accepting leaks of classified documents, and then publishing them, should be protected, at least to some significant degree. *See, e.g.*, Department of Justice, Report on Review of News Media Policies 3 (July 12, 2013) ("[T]he Department will modify its policy concerning search warrants covered by the PPA [the Privacy Protection Act of 1980, 42 U.S.C. § 2000aa] involving members of the news media to provide that work product materials may be sought under the 'suspect exception of the PPA only when the member of the news media is the focus of a criminal investigation for conduct not connected to ordinary newsgathering activities"), *available at*

to the first part of this issue, the historical record shows that the Executive Branch met its legal disclosure obligations to Congress. As to the second part, however, concerning disclosure to the public, it is clear that the American People did not understand that the bulk metadata collection was occurring or appreciate the legal interpretation that underlies it. Such a lack of understanding is, of course, the general rule with respect to classified intelligence activity; but the reaction to the June 2013 disclosures, and a particular focus on the perils of "secret law," suggests that that rule may be subject to change, potentially with profound consequences.

1. The standards governing information-sharing between the Executive Branch and Congress in this area are clear, as discussed in Chapter 13 of NSIP. Under FISA, the Intelligence Committees, and in some cases the Judiciary Committees – but not the rest of Congress – are to be kept "fully informed" of most intelligence activities, including significant interpretations of FISA.[219] Of particular relevance here, FISA provides that on an annual basis, "the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate concerning all requests for the production of tangible things under section 1861 of this title."[220] That "fully informed" obligation does not extend to Congress as a whole, or to any Member outside the specified committees.

In 2004 and 2008, Congress directly addressed the issue of "secret law" by amending FISA to provide specifically for briefings, and submission of documents, on all significant interpretations of FISA. Again, however, Congress provided that the briefings and documents would be provided only to the Intelligence and Judiciary Committees, not the rest of Congress:

> On a semiannual basis, the Attorney General shall submit to the Permanent Select Committee on Intelligence of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Committees on the Judiciary of the House of Representatives and the Senate, in a manner consistent with the protection of the national security . . . a summary of significant legal interpretations of this chapter involving matters before the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review, including interpretations presented in applications or pleadings filed with the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review by the Department of Justice; and . . . copies of all decisions, orders, or opinions of the Foreign Intelligence Surveillance

---

http://www.justice.gov/iso/opa/resources/220201371216285179689 3.pdf. Historians may also seek to view the disclosures against the background of public assessments the nature of the threat posed by international terrorism, and the armed conflict with al Qaeda and its affiliates, a dozen years after 9/11.

219. *See, e.g.*, 50 U.S.C. §§ 1801(a)(1) (electronic surveillance), 1826 (physical searches), 1846(a) (pen/trap surveillance), 1862(a) (tangible things), 1881f (FISA Amendments Act).

220. 50 U.S.C. § 1862(a).

> Court or Foreign Intelligence Surveillance Court of Review that include significant construction or interpretation of the provisions of this chapter.[221]

These legal standards reflect long-standing traditions governing disclosures owed to Congress by the Executive Branch in the area of intelligence. They represent the fundamental balancing of secrecy and transparency between the two political branches, and the essential idea behind creation of the Intelligence Committees in 1976 and 1977, as discussed in §§ 2:6-2:7 of NSIP. Recent times have witnessed an increasing effort by the Judiciary Committees also to become involved in classified matters regulated by law, but the balance remains solidly struck in favor of mandatory disclosure to the (two or four) committees, and against general disclosure of highly classified information to Congress as a whole.[222]

a. The record shows that the government met its disclosure obligations to Congress. Senators Diane Feinstein and Saxby Chambliss, Chair and Vice Chair of the Senate Intelligence Committee, responded to the June 2013 FISA Court order by observing, as Senator Feinstein put it, that "this is the exact three-month renewal of what has been the case for the past seven years. This renewal is carried out by the court under the business records section of the Patriot Act. Therefore, it is lawful. It has been briefed to Congress."[223] The two senators also issued a written statement on the Committee's website explaining that "[t]he executive branch's use of this authority has been briefed extensively to the Senate and House Intelligence and Judiciary Committees, and detailed information has been made available to all members of Congress prior to each congressional reauthorization of this law."[224]

---

221. 50 U.S.C. § 1871(a). The Senate Intelligence Committee's report on its activities from January 2009 to January 2011 noted that the "Committee utilized reporting required under provisions in FISA and the USA PATRIOT Act Improvement and Reauthorization Act, including the annual and semi-annual reports from the Attorney General, the DNI, and relevant inspectors general," and had "benefited from being able to review decisions, orders, and opinions, as well as the related pleadings, applications, and memoranda of law, that include 'significant construction or interpretation of any provision' of FISA that are required to be submitted to the oversight committees under 50 U.S.C. 1871(c)." S. Rep. No. 112-3, at 31 (Mar. 17, 2011) [hereinafter SSCI March 2011 Activities Report]. The report explained that "[t]hese documents were routinely the subject of subsequent briefings by officials of the Department of Justice and the Intelligence Community, in Committee spaces and at the relevant agencies." *Id.* at 31.

222. *See* L. ELAINE HALCIN AND FREDERICK M KAISER, CONG. RESEARCH SERV., RL32525, CONGRESSIONAL OVERSIGHT OF INTELLIGENCE: CURRENT STRUCTURE AND ALTERNATIVES (Mar. 14, 2012) [hereinafter 2012 CRS Oversight Report], *available at* http://assets.opencrs.com/rpts/RL32525_20120314.pdf.

223. Dan Roberts and Spencer Ackerman, *Senator Feinstein: NSA phone call data collection in place* since 2006*,* THE GUARDIAN (June 6, 2013) (emphasis added), http://www.guardian.co.uk/world/2013/jun/06/court-order-verizon-call-data-dianne-feinstein.

224. Press Release, Senate Select Committee on Intelligence, Feinstein, Chambliss Statement on NSA Phone Records Program (June 6, 2013) (emphasis added), *available at* http://www.intelligence.senate.gov/press/record.cfm?id=343993. Given that history, objections to the activity from civil libertarians tended to reflect a basic disagreement with the policy judgments reached and maintained over the preceding seven years by the Executive, Legislative, and Judicial Branches. As Anthony Romero, the head of the American Civil Liberties Union put it: "A pox on all the three houses of government."

Similarly, Representatives Mike Rogers and Dutch Ruppersberger, the Chair and Ranking Member of the House Intelligence Committee, released a statement the day after the FISA Court order was published saying that the collection described in the order

> is consistent with the Foreign Intelligence Surveillance Act (FISA) as passed by Congress, executed by the Executive Branch, and approved by a Federal Court. The FISA business records authorities are used to track foreign intelligence threats and international terrorists. It is important that the American people understand that this information does not include the content of anyone's conversations and does not reveal any individual or organization names. This important collection tool does not allow the government to eavesdrop on the phone calls of the American people. When these authorities are used, they are governed by court-approved processes and procedures. Moreover, the use of these authorities is reviewed and approved by federal judges every 90 days. Additionally, the Committee routinely reviews all FISA activities. Importantly, these activities have led to the successful detection and disruption of at least one terrorist plot on American soil, possibly saving American lives. Understanding the necessity of the public's trust in our intelligence activities and out of an abundance of caution, the Committee will review this matter to ensure that it too complies with the laws established to protect the American people.[225]

Between June 2008 and June 2012, the Senate Intelligence Committee "received and scrutinized un-redacted copies of every classified opinion of the Foreign Intelligence Surveillance Court (FISA Court) containing a significant construction or interpretation of the law, as well as the pleadings submitted by the Executive Branch to the FISA Court relating to such opinions."[226] It also reprinted without rebuttal the government's statement that it had complied with the obligation to produce the interpretive documents.[227]

The Department of Justice wrote a letter to Congress in July 2013 confirming

---

Charlie Savage, Edward Wyatt & Peter Baker, *U.S. Confirms that it Gathers Online Data Overseas*, N.Y. TIMES, June 7, 2013, at A1.

225. Joint Statement by House Intelligence Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger (June 6, 2013), *available at* http://intelligence.house.gov/press-release/joint-statement-house-intelligence-chairman-mike-rogers-and-ranking-member-ca-dutch.

226. S. Rep. No. 12-174, at 7 (June 7, 2012) (additional views of Senator Feinstein) [hereinafter SSCI June 7, 2012 Report].

227. *Id.* at 19 (background paper by the Department of Justice) ("Title VI of FISA requires a summary of significant legal interpretations of FISA in matters before the FISC or the Foreign Intelligence Surveillance Court of Review. The requirement extends to interpretations presented in applications or pleadings filed with either court by the Department of Justice. In addition to the summary, the Department must provide copies of judicial decisions that include significant interpretations of FISA within 45 days. The Government has complied with the substantial reporting requirements imposed by FISA to ensure effective congressional oversight of these authorities. The Government has . . . provided summaries of significant interpretations of FISA, as well as copies of relevant judicial opinions and pleadings.").

that "[t]he classified details of the program have been briefed to the Judiciary and Intelligence Committees on many occasions."[228] Also in July 2013, the DNI wrote to Senator Ron Wyden that "as Congress required, the Executive Branch fully and repeatedly briefed the Intelligence and Judiciary Committees of both Houses about the program and timely provided copies of the relevant classified documents to the Committees."[229] In its August 2013 White Paper, the government explained that

> in early 2007, the Department of Justice began providing all significant FISC pleadings and orders related to [the bulk telephony metadata collection] program to the Senate and House Intelligence and Judiciary Committees. By December 2008, all four committees had received the initial application and primary order authorizing the telephony metadata collection. Thereafter, all pleadings and orders reflecting significant legal developments regarding the program were produced to all four committees.[230]

In the fall of 2009, at least three Members of the House Judiciary Committee, including then-Chairman John Conyers and Representative Jerrold Nadler, separately engaged in explicit, classified correspondence with the Department of Justice concerning the bulk telephony metadata collection program. There is no question, based on this correspondence, that they were aware of the collection under FISA's tangible-things provision (as well as a program of bulk internet metadata collection under FISA's pen-trap provisions).[231] In May 2011, Representative Lamar Smith, then Chairman of the House Judiciary Committee, stated:

> During the last 3 months, the House Judiciary Committee has thoroughly reviewed the Patriot Act and how its provisions are used in national security investigations. The Crime Subcommittee has held three hearings specifically on the Patriot Act, the full committee held oversight hearings of the FBI and the Department of Justice, and all committee members were provided a classified briefing by the administration . . . . The business records provision allows the FBI to access third-party business records in foreign intelligence, international terrorism, and espionage cases. Again, this provision requires the approval of a Federal judge. That means the FBI must prove to a Federal judge that the documents are needed as part of a legitimate national security investigation. [This provision has] been effectively used for the last 10 years without any evidence of misuse or abuse."[232]

---

228. July 16, 2013 Letter to Sensenbrenner, *supra* note 27, at 3.

229. July 2013 DNI Response to 26 Senators, *supra* note 27, at 1.

230. White Paper, *supra* note 27, at 18 (emphasis added).

231. *See* Letters from Ronald Weich, Assistant Attorney General, to The Honorable Bobby Scott, The Honorable John Conyers, Jr., & The Honorable Jerrold Nadler (Dec. 17, 2009), *available at* http://www.dni.gov/files/documents/501/Letter%20AAG%20Weich_Dec2009.pdf. For a discussion of collection under FISA's pen-trap provisions, see NSIP, *supra* note 1, at § 18:4.

232. 157 Cong. Rec. H3738 (May 26, 2011) (emphasis added).

On July 17, 2013, in a hearing of the House Judiciary Committee, there was no rebuttal from any Member when Bob Litt, General Counsel of ODNI, stated that the interpretive documents had been provided to the Committee, or when James Cole, the Deputy Attorney General, later made the same assertion.[233] Chris Inglis, Deputy Director of the NSA, testified in the July 17, 2013 hearing without challenge that "[w]e also offered classified briefings to members of this committee. And I recall participating in one of those briefings."[234]

On March 5, 2009, and again on September 3, 2009, the Department of Justice sent to the Intelligence and Judiciary Committees a series of classified documents pertaining to compliance issues that had arisen in connection with the bulk telephony metadata collection. The September cover letter accompanying those documents explained that "these documents were described, in pertinent part, in briefings provided to the House and Senate Intelligence and Judiciary Committees in March, April, and August 2009."[235]

The Senate Judiciary Committee was sufficiently aware of the bulk metadata collection that it included language in two of its reports designed to ensure continuation of the collection. When the Committee considered amendments to the tangible-things provision in 2009 and 2011 (the amendments ultimately were not enacted), it was careful in doing so to avoid any suggestion that those amendments would undermine the bulk collection program, explaining in Committee reports that the proposed changes to the tangible things provision were "not intended to affect or restrict any activities approved by the FISA court under existing statutory authorities."[236]

---

233. July 2013 HJC Hearing, *supra* note 23, Statement of Bob Litt.

234. July 2013 HJC Hearing, *supra* note 23, Statement of Chris Inglis.

235. Letter from the U.S. Department of Justice to Congressional Intelligence and Judiciary Committees (Sept. 3, 2009) (emphasis added). The letters are available at http://icontherecord.tumblr.com/. The documents themselves, which are also publicly available on the same Intelligence Community website as the letters, are described as "several Foreign Intelligence Surveillance Court (FISC) opinions and Government filings relating to the Government's discovery and remediation of compliance incidents in its handling of bulk telephony metadata under docket number BR 08-13," and "the Government's report to the Court and NSA's end-to-end review describing its investigation and remediation of compliance incidents in its handling of bulk telephony metadata under docket number BR-09-09." *See* IC ON THE RECORD, http://icontherecord.tumblr.com/. For a summary of the nature of the compliance incidents, see note 67.

236. The Senate Judiciary Committee's reports on S. 1692, the USA Patriot Act Sunset Extension Act of 2009, S. Rep. No. 111-92, at 7 (Oct. 28, 2009), and S. 193, the USA Patriot Act Sunset Extension Act of 2011, S. Rep. No. 112-13, at 10 (Apr. 5, 2011), discuss certain proposed minor amendments to the requirements for a tangible-things application. The 2009 report explains that "[t]hese changes are not intended to affect or restrict any activities approved by the FISA court under existing statutory authorities," and the 2011 report explains that "[t]he language in the bill does not raise the standard [for obtaining an order] and is not intended to affect or restrict any activities approved by the FISA Court under existing statutory authorities." Nearly identical language also appears on page 23 of the 2011 report; see also page 24 of the 2009 report. The 2011 report also includes a letter from the Justice Department to the Chairman of the Senate Judiciary Committee dated September 14, 2009, and a similar letter to the Speaker of the House and Majority Leader of the Senate dated February 19, 2010, both stating that some tangible-things orders were "used to support important and highly sensitive intelligence collection operations" of which Members of the Intelligence Committees and their staff

b. Apart from briefings for, and documents submitted to, the four designated committees, the record shows that classified briefings were offered to all Members of Congress. On July 31, 2013, the DNI declassified and released letters and redacted briefing papers provided to the House and Senate Intelligence Committees in December 2009 and February 2011. The letters explained that "making this document [the 2011 briefing paper] available to all Members of Congress, as we did with a similar document in December 2009, is an effective way to inform the legislative debate about reauthorization of Section 215" of the Patriot Act.[237] The letters also stated that "Executive Branch officials will be available nearby [to the Intelligence Committees' SCIFs] during certain, pre-established times to answer questions should they arise."[238]

The classified briefing papers themselves, which are written in relatively plain language and are five pages long, explained that the FISC's "orders generally require production of the business records . . . relating to substantially all of the telephone calls handled by the [telephone] companies," including "both calls made between the United States and a foreign country and calls made entirely within the United States."[239] The briefing papers described the program explicitly as involving "bulk" collection, and stated that it "operate[s] on a very large scale," even though "only a tiny fraction of [the collected] records are ever viewed by NSA intelligence analysts."[240] The briefing papers also described "a number of technical compliance problems and human implementation errors" that were discovered beginning in 2009 "as a result of Department of Justice (DOJ) reviews and internal NSA oversight," but noted that neither the government nor the FISC "found any intentional or bad-faith violations."[241]

The availability of the classified briefings and documents was publicized within Congress. Senators Feinstein and Chambliss wrote two "Dear Colleague" letters, in 2010 and 2011, inviting all Members of Congress to classified

---

(and later, the Judiciary Committees and their staffs, as well as House and Senate leadership) are aware, and offering to "provide additional information to Members or their staff in a classified setting." S. Rep. 113 at 114, 120. In the end, neither of the two bills became law, and the tangible-things provision, along with other provisions of the Patriot Act, was extended to June 1, 2015, without change, by Section 2(a) of Pub. L. No. 112-14, 125 Stat. 216 (May 26, 2011).

237. 2011 Briefing Documents, *supra* note 27, Cover Letter at 1. The Chairman and other Members of the House Judiciary Committee were also informed by letter of the government's plan to make such documents and briefings available. *See* Letters from Ronald Weich, Assistant Attorney General, to The Honorable Bobby Scott, The Honorable John Conyers, Jr., & The Honorable Jerrold Nadler (Dec. 17, 2009), *available at* http://www.dni.gov/files/documents/501/Letter%20AAG%20Weich_Dec2009.pdf.

238. 2011 Briefing Documents, *supra* note 27, Cover Letter at 2.

239. 2011 Briefing Documents, *supra* note 27, Briefing Paper at 3.

240. *Id.* at 1, 3. The publicly released version of the briefing paper redacts more than four lines of text immediately following the statement that the program operates on a "very large scale" and immediately before the statement that analysts only view "a tiny fraction of such records." It therefore appears that the redacted information provides more detail about the precise scope and scale of the collection.

241. *Id.* at 4.

briefings on the bulk collection,[242] and statements in the Congressional Record show that they offered briefings to Members during debates over reauthorization of the Patriot Act. For example, in 2011, Senator Feinstein made the following floor statement:

> The third authority covered by this [proposed] legislation [to reauthorize the Patriot Act] is known as the business records provision and provides the government the same authority in national security investigations to obtain physical records that exist in an ordinary criminal case through a grand jury subpoena . . . . some business records orders have been used to support critically important and highly sensitive intelligence collection activities. The House and Senate Intelligence Committees have been fully briefed on that collection. Information about this sensitive collection has also been provided to the House and Senate Judiciary Committees, and information has been available for months to all Senators for their review. The details on how the government uses all three of these authorities are classified and discussion of them here would harm our ability to identify and stop terrorist attacks and espionage. But, if any Senators would like further details, I encourage them to contact the Intelligence Committee, or to request a briefing from the Intelligence Community or the Department of Justice.[243]

Similarly, Rep. Hastings, a Member of the House Intelligence Committee, stated in February 2010:

> Mr. Speaker, I rise to inform Members that the Intelligence Committee has received a classified document from the Department of Justice that is related to the PATRIOT Act authorities currently set to expire at the end of the month.
>
> The House may consider a 1-year extension of the PATRIOT Act today so the Intelligence Committee will be making this document available for Member review in the committee offices located in HVC-304. Staff from the Intelligence and Judiciary Committees, as well as personnel from the Justice Department and with the Office of the Director of National Intelligence, will be available to answer any questions that Members may have. Members who want to review the document should call the Intelligence Committee to schedule an appointment.[244]

Senator Wyden (a Member of the Intelligence Committee) also cited the availability of a briefing document and encouraged his colleagues to read it, noting that "the Attorney General and the Director of National Intelligence have prepared a classified paper that contains details about how some of the Patriot

242. The "Dear Colleague" letters, dated February 2010 and February 2011, offered Members of Congress the opportunity to review documents related to the collection, and included an offer to meet with DOJ and Intelligence Community personnel. The letters are available at http://big.assets.huffingtonpost.com/SelectCommitteeIntelligenceFeb13.pdf.

243. 157 Cong. Rec. S3210-02 (May 23, 2011) (emphasis added).

244. 156 Cong. Rec. H838 (Feb. 25, 2010) (emphasis added).

Act's authorities have actually been used, and this paper is now available to all members of Congress, who can read it in the Intelligence Committee's secure office spaces."[245] He went on to observe that "[p]roviding this classified paper to Congress is a good first step, and I would certainly encourage all of my colleagues to come down to the Intelligence Committee and read it," although he also strongly urged release of the information to the general public.[246] The Department of Justice also informed the Chairman and other Members of the House Judiciary Committee of its plan to make the information available.[247]

In an unclassified report published in March 2011, the Senate Intelligence Committee emphasized that it had offered a briefing to all Members of Congress concerning the bulk telephony metadata collection:

> Prior to the extension of the expiring FISA provisions in February 2010, the Committee acted to bring to the attention of the entire membership of the Senate important information related to the nature and significance of the FISA collection authority subject to sunset. Chairman Feinstein and Vice Chairman Bond notified their colleagues that the Attorney General and the DNI had provided a classified paper on intelligence collection made possible under the Act and that the Committee was providing a secure setting where the classified paper could be reviewed by any Senator prior to the vote on passage of what became Public Law 111-141 to extend FISA sunsets.[248]

The Attorney General and/or the DNI had themselves offered such briefings in writing as early as 2009, as described in an unclassified letter sent by both officials to the Majority Leader of the Senate and the Speaker of the House on February 19, 2010:

> As we previously noted in a September 14 [2009] letter from the Department of Justice to Senator Patrick Leahy, the business records authority [of FISA] has been used to support important and highly sensitive intelligence collection operations, of which both Senate and House leadership, as well as Members of the Intelligence and Judiciary Committees and their staffs are aware. We can provide additional information to Members concerning these and related operations in a classified setting.[249]

---

245. 156 Cong. Rec. S2108 (Mar. 25, 2010).

246. 156 Cong. Rec. S2108, (Mar. 25, 2010).

247. *See* Letters from Ronald Weich, Assistant Attorney General, to The Honorable Bobby Scott, The Honorable John Conyers, Jr., & The Honorable Jerrold Nadler (Dec. 17, 2009), *available at* http://www.dni.gov/files/documents/501/Letter%20AAG%20Weich_Dec2009.pdf.

248. SSCI March 2011 Activities Report, *supra* note 221, at 31 (emphasis added).

249. Letter from Eric Holder, U.S. Attorney General, and Adm. Dennis C. Blair, Director of National Intelligence, to Senator Harry Reid, Senate Majority Leader, and Speaker Nancy Pelosi, Speaker of the House (February 19, 2010) (emphasis added). The letter is reprinted in S. Rep. No. 112-13 (Apr. 5, 2011).

In 2013, the White House released to members of the news media a list of 13 classified briefings, for members of the Intelligence and Judiciary Committees, Congressional Leadership, the House Democratic Caucus, and others, conducted between 2009 and 2011, on the tangible things provision.[250] It is not clear whether the list is complete, or whether some briefings were intentionally or accidentally omitted (the list appears to omit the briefings conducted in March, April and August 2009, discussed above). The list of briefings, as published in Politico, was as follows:

- May 12, 2009: SSCI Hearing Expiring FISA Provisions (Classified), Justice Dept. National Security Division chief David Kris and National Security Agency Director Keith Alexander
- Sept. 22, 2009: HJC Hearing USA Patriot Act (Unclassified) DOJ NSD Deputy Todd Hinnen
- Sept. 23, 2009: SJC Hearing Reauthorizing the Patriot Act, Kris
- Nov. 29, 2010: Leadership Meeting House and Senate Leadership Staff (Classified)
- Feb. 14, 2011: Senate All Senators were offered the opportunity discuss Sec. 215 of the Patriot Act in the VPOTUS office off of Senate Floor, Director of National Intelligence James Clapper, FBI Director Robert Mueller, Alexander
- Feb. 28, 2011: SJC/SSCI Briefing Patriot Act reauthorization (Classified)
- Feb. 28, 2011: HJC Briefing Patriot Act reauthorization (Classified)
- March 9, 2011: HJC Hearing Patriot Act reauthorization (Unclassified), Hinnen
- March 15, 2011: Meeting Durbin Patriot Act amendment (Classified)
- March 17, 2011: HPSCI Hearing Patriot Act reauthorization, Hinnen, FBI's Sean Joyce, Alexander
- March 30, 2011: HJC Hearing Patriot Act Reauthorization (Unclassified), Hinnen
- May 13, 2011: House Rep Conf Patriot Act Reauthorization, Mueller
- May 24, 2011: House Dem Caucus Patriot Act Reauthorization, Mueller

In July 2013, the DNI wrote to Senator Wyden that "the Executive Branch undertook special efforts to ensure that all Members of Congress had access to information regarding this classified program prior to the USA PATRIOT Act's reauthorization in 2011, including making a detailed classified white paper

250. *See* Josh Gerstein, *Official: 13 Briefings for Hill on Call-Tracking Provision*, POLITICO (June 8, 2013), http://www.politico.com/blogs/under-the-radar/2013/06/official-briefings-for-hill-on-calltracking-legal-165732.html. The Department of Justice confirmed several of these briefings in a letter dated July 16, 2013 sent to Representative Sensenbrenner. July 16, 2013 Letter to Sensenbrenner, *supra* note 27, at 3-4.

available to all Members."[251] The DNI's letter went on to explain that "in December 2009, the Department of Justice and Intelligence Community provided a classified briefing paper to the Senate and House Intelligence Committees that could be made available to all Members of Congress regarding the telephony metadata program. Both Intelligence Committees made this document available to all Members prior to the February 2010 reauthorization of Section 215. That briefing paper was then updated and provided to the Senate and House Intelligence Committees again in February 2011 for all Members in connection with the reauthorization that occurred later that year."[252]

Many Members of Congress acknowledged having been briefed, or at least having had the opportunity to be briefed, on the bulk collection program.[253] For example, the Senate Majority Leader, Harry Reid, said: "For senators to complain that 'I didn't know this was happening,' we've had many, many meetings

---

251. July 2013 DNI Response to 26 Senators, *supra* note 27, at 1.

252. *Id.* at 1. *See also* White Paper, *supra* note 27 at 17-18. Although the House Intelligence Committee did notify Members of the House of the classified documents and briefings in 2010 (when it was led by Chairman Sylvestre Reyes), it may not have done so in 2011 (when it was led by Chairman Mike Rogers). *See* White Paper, *supra* note 27, at 18 n.13; US EPIC BIO, *supra* note 153, at 11 & nn. 3-4 (referring only to the 2010 documents). In the summer of 2013, the House Intelligence Committee denied requests from certain Members of the House to view certain classified materials concerning FISA. *See* Glenn Greenwald, *Members of Congress Denied Access to Basic Information About FISA*, THE GUARDIAN (Aug. 4, 2013), http://www.theguardian.com/commentisfree/2013/aug/04/congress-nsa-denied-access; *see also* Josh Gerstein, *House panel nixes Grayson's Request for Syria Intelligence*, POLITICO (Oct. 18, 2013), http://www.politico.com/blogs/under-the-radar/2013/10/house-panel-nixes-graysons-request-for-syria-intelligence-175396.html?hp=r22. The Rules of the House Intelligence Committee set out a detailed procedure under which Members of Congress who do not serve on the Committee may gain access to classified information. Under Rule 14(f), the Committee considers written requests for access by non-Members using at least the following criteria:

> (A) The sensitivity to the national defense or the confidential conduct of the foreign relations of the United States of the information sought;
>
> (B) The likelihood of its being directly or indirectly disclosed;
>
> (C) The jurisdictional interest of the member making the request; and
>
> (D) Such other concerns, constitutional or otherwise, as may affect the public interest of the United States.

The Rules also contain detailed provisions under which the Committee can, on its own initiative, bring matters to the full House. *See* Rules of Procedure for the House Permanent Select Committee on Intelligence, 113th Cong., *available at* http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/HPSCI%20Rules%20of%20Procedure%20-%20113th%20Congress.pdf. The Senate Intelligence Committee has similar rules. *See* Rules of Procedure for the Select Committee on Intelligence, United States Senate, Rules 9.5, 9.9, *available at* http://www.intelligence.senate.gov/pdfs113th/sprt1137.pdf. Regardless of any intra-congressional issues in 2011, as a matter of inter-branch relations, it is clear that the Executive Branch provided the materials with the intent that they be made available to all Members of Congress, as they had been in 2009.

253. *See, e.g.*, June 2013 Open HPSCI Hearing, Statement of Chairman Mike Rogers ("The committee has been extensively briefed on these efforts over [sic] a regular basis as part of our ongoing oversight responsibility . . . . the collection efforts under the business records provision [and] in Section 702 of the Foreign Intelligence Surveillance Act are legal, court-approved and subject to an extensive oversight regime."), Statement of Ranking Member Dutch Ruppersberger ("I reiterate a lot of what the Chairman has said . . . . Both of these authorities are legal. Congress approved and reauthorized both of them over the last two years.").

that have been both classified and unclassified that members have been invited to . . . . If they don't come and take advantage of this, I can't say enough to say they shouldn't come and say 'I wasn't aware of this,' because they've had every opportunity to be aware of these programs."[254] Senator Leahy acknowledged receiving classified briefings.[255] Even Senators Wyden and Udall, perhaps the most outspoken Congressional critics of the program, conceded in March 2012 that the existence of the program, and underlying legal interpretation, "has been acknowledged on multiple occasions by the Justice Department and other executive branch officials," and noted that the Executive Branch had, "to its credit, provided this information in documents submitted to Congress."[256]

---

254. Michael McAuliff and Sabring Siddiqui, *Harry Reid: If Lawmakers Didn't Know About NSA Surveillance, It's Their Fault*, THE HUFFINGTON POST (June 11, 2013), http://www.huffingtonpost.com/2013/06/11/harry-reid-nsa_n_3423393.html.

255. July 2013 SJC Hearing, *supra* note 27, Statement of Senator Leahy ("Like so many others, I'll get the classified briefings, but then of course you can't talk about them.").

256. Letter from Senator Ron Wyden to Senator Tom Udall (Mar. 15, 2012) *available at* https://www.documentcloud.org/documents/325953-85512347-senators-ron-wyden-mark-udall-letter-to.html [hereinafter Wyden-Udall Letter of March 15, 2012]. Although the letter credits the briefings offered to Congress, it observes that "the executive branch has worked hard to keep the government's official interpretation of the Patriot Act secret from the American public," and notes that while Members of Congress were offered briefings, they generally "do not have any staff who are cleared to read them," and apparently did not take advantage of the offers: "we can state with confidence that most of our colleagues in the House and Senate are unfamiliar with these documents." *Id.* at 2. The concerns of Senators Udall and Wyden were reported by the news media at the time. *See, e.g.*, Charlie Savage, *Public Said to be Misled on Use of the Patriot Act*, N.Y. TIMES, at A15, Sept. 22, 2011, *available at* http://www.nytimes.com/2011/09/22/us/politics/justice-dept-is-accused-of-misleading-public-on-patriot-act.html?_r=0.

Another letter sent to the Attorney General by Senators Wyden and Udall in 2011 accused unnamed officials in the Department of Justice of "misleading" Congress by drawing analogies between tangible-things orders and grand jury subpoenas. Letter from Senators Wyden and Udall to Attorney General Holder (Sept. 21, 2011), *available at* http://www.documentcloud.org/documents/250829-wyden-udall-letter-to-holder-on-wiretapping.html. Apart from the extensive briefings for Congress described in the text, there are a number of difficulties with that claim, some of which were pointed out in a responsive letter from DOJ dated October 19, 2011 and available at http://images.politico.com/global/2012/03/dojltrwyden.pdf. Chief among those difficulties are (1) as noted in the text, the statute explicitly provides that the FISC "may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation," 50 U.S.C. § 1861(c)(2)(D), making some analogy to grand jury practice more or less inevitable in any reasonably complete description of the statute; and (2) many members of Congress, who by their own accounts were fully informed about the bulk collection, used and continue to use analogies to the grand jury when they describe the statute for their colleagues, including:

• In a 2011 report of the Senate Judiciary Committee, Senators Grassley, Hatch, Kyl, Sessions, Graham, Cornyn and Coburn stated that the tangible things provision "allows officials to ask a court for an order to obtain tangible things, including business records, in national security terrorism cases . . . . In criminal matters, similar records may be obtained using a grand jury subpoena, without any need for court approval." S. Rep. No. 112-13, at 34 (Apr. 5, 2011); *see id.* at pages 37, 43, 45; *see also* S. REP. NO. 109-86 (June 16, 2005).

• A 2011 report of the House Judiciary Committee contained similar language: "The Section 215 business records authority allows the Federal government to seek approval from the FISA Court of orders granting the government access to any tangible items (including books, records, papers, and other documents) in foreign intelligence, international terrorism, and clandestine intelligence cases.

Although at least one Member of the House Judiciary Committee publicly stated that he intentionally eschews classified briefings – on the ground that they

---

This authority is similar to the widely-used grand jury subpoena authority in criminal investigations." H.R. REP. NO. 112-79, pt. 1 (May 18, 2011).

• In 2011, as part of the debate over reauthorizing the USA Patriot Act, Senator Feinstein, Chair of the Senate Intelligence Committee, advised her colleagues:

> The third authority covered by this [proposed] legislation is known as the business records provision and provides the government the same authority in national security investigations to obtain physical records that exist in an ordinary criminal case through a grand jury subpoena . . . . some business records orders have been used to support critically important and highly sensitive intelligence collection activities. The House and Senate Intelligence Committees have been fully briefed on that collection. Information about this sensitive collection has also been provided to the House and Senate Judiciary Committees, and information has been available for months to all Senators for their review. The details on how the government uses all three of these authorities are classified and discussion of them here would harm our ability to identify and stop terrorist attacks and espionage. But, if any Senators would like further details, I encourage them to contact the Intelligence Committee, or to request a briefing from the Intelligence Community or the Department of Justice.

157 Cong. Rec. S3210-02 (May 23, 2011).

• Representative Mike Rogers, Chair of the House Intelligence Committee, also made explicit comparisons to the grand jury in urging reauthorization of Section 215 of the USA Patriot Act:

> If you believe today that going in and trying to get someone's business records to prove that they were at a place, with a subpoena from a grand jury, is a bad idea, then we should stop doing it. Today you can do it. You can go to the library and get someone's records. As a matter of fact, during the first part of this debate someone talked about how they went in and got all this information on whoever checked out a book on Osama bin Laden and what a horrible thing it was. That wasn't even a FISA warrant. It was a criminal warrant. That happened under the criminal code. That can happen tomorrow. And when this expires at the end of this month, they will still continue to be able to do that. But [if the expiring Patriot Act provisions, including Section 215, are not reauthorized] you will not be able to go to a FISA court and get a roving wiretap or a court order, by the way, to get records that will help in an ongoing terrorism investigation. It really is mind-boggling.

157 Cong. Rec. H731 (Feb. 14, 2011). *See also* 157 Cong. Rec. H621 (Feb. 10, 2011).

• Even after the June 2013 disclosures, the Department of Justice continues to analogize to the grand jury. *See* June 2013 HPSCI Open Hearing, *supra* note 27, Statement of James Cole (explaining that the statute is "quite explicitly limited to things that you could get with a grand jury subpoena; those kinds of records. Now, it's important to know prosecutors issue grand jury subpoenas all the time and do not need any involvement of a court or anybody else, really, to do so. Under this program, we need to get permission from the court to issue this ahead of time, so there is court involvement with the issuance of these orders, which is different from a grand jury subpoena. But the type of records – just documents, business records, things like that – are limited to those same types of records that we could get through a grand jury subpoena."). At the hearing, no Member of the House Intelligence Committee voiced any objection to this statement.

• A July 16, 2013 letter from the Department of Justice to Representative Sensenbrenner further noted that "the FISC may only require the production of items that can be obtained with a grand jury subpoena or any other court order directing the production of records or tangible things." July 16, 2013 Letter to Sensenbrenner, *supra* note 27, at 1.

• On July 17, 2013, Chairman Bob Goodlatte opened a hearing of the House Judiciary Committee by explaining that "Similar to grand jury or administrative subpoenas, a FISA business records order cannot be used to search a person's home to acquire the content of e-mails, or listen to telephone calls." July 2013 HJC Hearing, *supra* note 23.

Although the Wyden-Udall letter did not identify any DOJ officials by name, I was one of several over the years since 2006 who referred to grand juries in describing the tangible things provision. I

are a "rope-a-dope operation"[257] – none appears credibly to have denied the fact that briefings occurred or that the relevant interpretive documents were delivered.[258]

---

testified before the Senate Judiciary Committee in 2009 that the tangible-things provision was "roughly analogous" to the authority available to FBI agents investigating criminal matters through the use of grand jury subpoenas, and also stated that "[a]s many Members are aware, some of these [Section 215] orders were used to support important and highly sensitive intelligence collections. The Department can provide additional information to Members or their staff in a classified setting." Testimony of David Kris, Assistant Attorney General, before the Senate Judiciary Committee (Sept. 23, 2009), *available at* http://www.justice.gov/ola/testimony/111-1/2009-09-23-nsd-kris-patriot-act.pdf. *See also* Peter Wallsten, *Lawmakers Say Administration's Lack of Candor on Surveillance Weakens Oversight*, WASH. POST, July 10, 2013, *available a*t http://www.washingtonpost.com/politics/lawmakers-say-administrations-lack-of-candor-on-surveillance-weakens-oversight/2013/07/10/8275d8c8-e97a-11e2-aa9f-c03a72e2d342_story.html.

257. Representative James Sensenbrenner was quoted in the Washington Post as follows:

> Sensenbrenner, who had access to multiple classified briefings as a member of the Judiciary Committee, said he does not typically attend such sessions. He called the practice of classified briefings a "rope-a-dope operation" in which lawmakers are given information and then forbidden from speaking out about it. Members are not permitted to discuss information disclosed in classified briefings. "It's the same old game they use to suck members in," he said.

Id. Representative Sensenbrenner did not explain how or why he expected to receive a classified briefing and also be authorized to discuss that briefing publicly.

258. One notable example of a Member of Congress who denied knowledge of the bulk collection was Representative Sensenbrenner, who wrote a letter to the Attorney General on June 6, 2013, explaining that he had "closely monitored and relied on testimony from the Administration about how the [Patriot] Act was being interpreted to ensure that abuses had not occurred," and had been "left with the impression that the Administration was using the business records provision sparingly, and for specific materials," in contrast to the "recently released FISA order," which "could not have been drafted more broadly." *See* Letter from Rep. James Sensenbrenner to Attorney General Eric Holder (June 6, 2013), *available at* http://sensenbrenner.house.gov/uploadedfiles/sensenbrenner_letter_to_attorney_general_eric_holder.pdf.

As evidence that he had not been properly informed, Representative Sensenbrenner cited in his letter the testimony of a DOJ official, as follows, with the ellipsis included in the letter:

> Section 215 has been used to obtain driver's license records, hotel records, car rental records, apartment leasing records, credit card records, and the like. It has never been used against a library to obtain circulation records . . . On average we seek and obtain section 215 orders less than 40 times per year.

This description of the government's use of the tangible things provision, Representative Sensenbrenner asserted, did not adequately advise the Committee of the classified bulk collection program.

Unfortunately for Representative Sensenbrenner, the ellipsis in his letter replaced the following sentence from the DOJ official's testimony:

> Some orders have also been used to support important and highly sensitive intelligence collection operations, on which this committee and others have been separately briefed.

Statement of Todd Hinnen, Acting Assistant Attorney General for National Security, before the House Judiciary Subcommittee on Crime, Terrorism and Homeland Security (Mar. 9, 2011), *available at* http://www.justice.gov/nsd/opa/pr/testimony/2011/nsd-testimony-110309.html. *See also* Wells Bennett, *Sensenbrenner on DOJ Testimony Regarding 215*, LAWFARE, June 7, 2013, *available at* http://www.lawfareblog.com/2013/06/sensenbrenner-on-doj-testimony-regarding-section-215/; Adam Serwer, *Patriot Act Architect Cries Foul on NSA Program, but Skipped Briefings*, MSNBC, June 14, 2013 (noting the ellipsis in Rep. Sensenbrenner's letter, and observing, "Maybe Sensenbrenner wouldn't have been as surprised, had he attended classified briefings on the National Security Agency's program over the

Such a highly classified briefing for all Members of Congress, rather than just for those serving on the Intelligence Committees (and perhaps also the Judiciary Committees), is very unusual.[259] It is understandable that the Executive Branch wanted to brief all Members of Congress "as an effective way to inform the legislative debate about reauthorization of Section 215" of the Patriot Act.[260] But the briefings were, without question, a departure from the legal requirements and cultural and historical norms in this area. As Senator Feinstein stated in July 2013, referring to the bulk telephony metadata collection program, "Balancing privacy rights with our nation's security is difficult to achieve, but I know of no federal program for which audits, congressional oversight and scrutiny by the Justice Department, the intelligence community and the courts are stronger or more sustained."[261]

The briefings and other historical evidence raise the question whether Con-

---

last three years"), *available at* http://tv.msnbc.com/2013/06/14/sensenbrenner-furious-that-he-wasnt-briefed-on-nsa-programs-skipped-the-briefings/. Representative Sensenbrenner made similar claims in a judicial proceeding, where they were characterized by the court as "curious":

> Congressman Sensenbrenner asserts in an amicus brief that "he was not aware of the full scope of the [telephony metadata collection] program when he voted to reauthorize section 215" and that "had he been fully informed he would not have voted to reauthorize section 215 without change." Br. of Amicus Curiae, F. James Sensenbrenner ("Amicus Br.") at 9-10 (ECF No. 56). This is a curious statement: Congressman Sensenbrenner not only had access to the five-page report made available to all Congressmen, but he also, as "a long-serving member of the House Judiciary Committee," "Amicus Br. at 1, was briefed semi-annually by the Executive Branch that included "a summary of significant legal interpretations of section 215 involving matters before the FISC" and "copies of all decisions, orders, or opinions of the FISC that include significant construction or interpretation of section 215." 50 U.S.C. § 1871.

ACLU Opinion, *supra* note 113, at *16.

Another Member of Congress who complained of being misled was Rep. Jerrold Nadler, also of the House Judiciary Committee. In a Washington Post story published in July 2013, Rep. Nadler was quoted as saying, "The national security state has grown so that any administration is now not upfront with Congress," and that "It's an imbalance that's grown in our government, and one that we have to cleanse." The article also quoted Rep. Nadler as follows: "'I don't know if it was an outright lie, but it was certainly misleading to what was going on,' said Nadler, who was chairman of the committee that heard from Hinnen in 2009." Peter Wallsten, *Lawmakers Say Administration's Lack of Candor on Surveillance Weakens Oversight*, WASH. POST DIGITAL (July 10, 2013), http://www.washingtonpost.com/politics/lawmakers-say-administrations-lack-of-candor-on-surveillance-weakens-oversight/2013/07/10/8275d8c8-e97a-11e2-aa9f-c03a72e2d342_story.html.

As it turns out, however, Rep. Nadler was in fact aware of the bulk metadata collection in 2009, and (as discussed in the text) wrote to the Department of Justice about the collection at that time. In response, DOJ sent him a letter in December 2009 noting that the government was making available to all Members of Congress information about the bulk collection and compliance issues that had arisen. Letter from Ronald Weich, Assistant Attorney General, to Rep. Jerrold Nadler (Dec. 17, 2009), *available at* http://www.dni.gov/files/documents/501/Letter%20AAG%20Weich_Dec2009.pdf. There is no question whatsoever, based on the letters he exchanged with the Department of Justice, that Rep. Nadler was aware of the bulk metadata collection program in 2009.

259. For a more complete discussion of Congressional oversight of national security matters, see NSIP, *supra* note 1, at § 13:1 *et seq.*

260. 2011 Briefing Documents, *supra* note 27, Cover Letter at 1.

261. Senator Dianne Feinstein, *Make NSA Programs More Transparent*, WASH. POST DIGITAL (July 31, 2013), http://www.washingtonpost.com/opinions/senate-intelligence-committee-chair-reform-nsa-programs/2013/07/30/9b66d9f2-f93a-11e2-8e84-c56731a202fb_story.html.

gress's repeated reauthorization of the tangible things provision effectively incorporates the FISC's interpretation of the law, at least as to the authorized scope of collection, such that even if it had been erroneous when first issued, it is now – by definition – correct. There is a basic principle of statutory construction that "Congress is presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statute without change,"[262] as it did repeatedly with the tangible things provision. It would have been relatively easy, as a technical matter – not necessarily as a political matter – for Congress to enact legislation expressly authorizing, modifying,[263] or forbidding bulk collection under the tangible things provision.[264] A one-sentence bill to forbid bulk collection of telephony metadata narrowly failed to pass the House of Representatives in July 2013.[265] (For the

---

262. Lorillard v. Pons, 434 U.S. 575, 580 (1978); *see also* Keene Corp. v. United States, 508 U.S. 200, 212-13 (1993). *Cf.* In re Sealed Case, 310 F.3d 717, 735 (FISCR 2002) ("In short, even though we agree that the original FISA did not contemplate the 'false dichotomy,' the Patriot Act actually did-which makes it no longer false.")

263. One possibility, discussed briefly at the June 2013 HPSCI hearing, and again at the July 2013 SJC hearing, would be to store data with providers, requiring them to keep it for 5 years, and then conduct emergency or court-authorized queries based on a showing of reasonable suspicion. Depending on the number of "hops" and perhaps other factors, however, that disaggregation may be technically challenging unless the providers link and make uniform their databases; another possible approach could be to use a third party custodian for all participating providers' data, even if the infrastructure for the data had to be supplied by NSA. Appropriate legislation, developed in coordination with the government and the providers, could support and require such an approach. *See* July 2013 SJC Hearing, *supra* note 27, Statement of Chris Inglis ("I think we can take a look at whether this is stored at the provider, so long as you have some confidence you can do this in a timely way."). *See also* Review Group Report, *supra* note 113, at 17 ("In our view, the current storage by the government of bulk meta-data creates potential risks to public trust, personal privacy, and civil liberty. We recognize that the government might need access to such meta-data, which should be held instead either by private providers or by a private third party.").

264. Such legislation might also have expressed Congressional intent, in line with the *Steel Seizure* case, that the President not act unilaterally in this area, as may have been the case before 2006, leaving the Executive Branch to rely on any inviolable Article II authority or to use grand juries or other extant statutory authorities. For a discussion of FISA's "exclusivity provision" governing electronic surveillance, and the *Steel Seizure* case. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952), *see* NSIP, *supra* note 1, at § 15:3.

It is extremely interesting to consider whether, under current law and the FISA Court's orders interpreting it, the government's theory of "relevance" would permit an approach in which the haystacks of metadata remain at the providers. As discussed in the text, the government's theory is that it must collect the haystacks to find the needles representing terrorist communications, and that the haystacks are therefore relevant. Leaving the metadata with the telecommunications providers and simply running queries against it (directly or through the providers) would not necessarily accord with that theory. The providers might agree voluntarily to run queries if otherwise permitted to do so, and in that event the results of those queries would likely establish relevance to collect the responsive records, but it is far from clear that FISA's tangible things provision could be used to compel the providers to run the queries in the first place. This does not, of course, call into question Congress's ability to enact new legislation that would compel providers to retain and query the data under certain conditions.

265. *See* Office of the Clerk of the U.S. House of Representatives-Final Vote Results for Roll Call 412, http://clerk.house.gov/evs/2013/roll412.xml. The bill provided as follows:

> None of the funds made available by this Act may be used to execute a Foreign Intelligence Surveillance Court order pursuant to section 501 of the Foreign Intelligence Surveillance Act

longer term, of course, a failure to enact legislation restricting or terminating the bulk metadata collection, and/or a reenactment of Section 215 of the Patriot Act without change or with changes that permit the program to continue, after the public debate that has occurred, would be extremely telling.)

Of course, it would be ridiculous to presume that Congress adopted a classified interpretation of a law of which it could not have been aware. As described above, however, the historical record shows that many Members were aware, and that all Members were offered briefings on the FISC's interpretation, even if they did not attend the briefings. Even in an ordinary legislative setting, of course, many Members may not actually be aware of a prior judicial interpretation, but that has never been formally part of the doctrine.[266] Here, post-disclosure briefings, conducted in July 2013, also drew sparse attendance, apparently to a degree that frustrated Senator Feinstein, who was quoted as saying, "It's hard to get this story out. Even now we have this big briefing – we've got [NSA Director] Alexander, we've got the FBI, we've got the Justice Department, we have the FISA Court there, we have [DNI] Clapper there – and people [Members of Congress] are leaving."[267] Although the Supreme Court has never applied the presumption of Congressional awareness and adoption in this setting, the government would seem to have some arguments that it should

---

of 1978 (50 U.S.C. 1861) that does not include the following sentence: "This Order limits the collection of any tangible things (including telephone numbers dialed, telephone numbers of incoming calls, and the duration of calls) that may be authorized to be collected pursuant to this Order to those tangible things that pertain to a person who is the subject of an investigation described in section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861).''

159 Cong. Rec. H5023 (July 24, 2013).

266. *Cf.* William N. Eskridge, Jr., *Interpreting Legislative Inaction*, 87 MICH. L. REV. 67, 81 ("While the Court in these cases often invokes the reenactment rule without a specific showing that Congress was aware of the judicial interpretations, the Court usually makes an effort to demonstrate that Congress 'must' have been aware of the interpretations."). *But cf., e.g.*, Zuber v. Allen, 396 U.S. 168, 185 n.21, 192-194 (1969) (With respect to the doctrine of legislative acquiescence, rather than reenactment, "the verdict of quiescent years cannot be invoked to baptize a statutory gloss that is otherwise impermissible. This Court has many times reconsidered statutory constructions that have been passively abided by Congress. Congressional inaction frequently betokens unawareness, preoccupation, or paralysis. It is at best treacherous to find in Congressional silence alone the adoption of a controlling rule of law. Its significance is greatest when the area is one of traditional year-by-year supervision, like tax, where watchdog committees are considering and revising the statutory scheme." (internal quotation and citation omitted)).

267. According to *The Hill*, a briefing for Senators on June 13, 2013 attracted less than half of the Senate. Alexander Bolton, *Senators Skip Classified Briefing on NSA Snooping to Catch Flights Home*, THE HILL (June 15, 2013) ("Only 47 of 100 senators attended the 2:30 briefing, leaving dozens of chairs in the secure meeting room as [DNI] Clapper, [NSA Director] Alexander and other senior officials told lawmakers about classified programs to monitor millions of telephone calls and broad swaths of Internet activity . . . . The exodus of colleagues exasperated Senate Intelligence Committee Chairwoman Diane Feinstein (D-Calif.), who spent a grueling week answering colleagues' and media questions about the program. 'It's hard to get this story out. Even now we have this big briefing – we've got Alexander, we've got the FBI, we've got the Justice Department, we have the FISA Court there, we have Clapper there – and people are leaving'"), http://thehill.com/homenews/senate/305765-senators-skip-classified-briefing-on-nsa-snooping-to-catch-flights-home.

be applied. On the other hand, there would be no serious argument that the FISC's decisions established a "public" understanding of the tangible things provision before it was reauthorized, and that could undermine reliance on the doctrine.[268] In his speech in January 2014, the President seemed to endorse the argument that Congress had been adequately briefed, observing that "the telephone bulk collection program was subject to oversight by the [FISC] and has been reauthorized repeatedly by Congress," even though "it has never been subject to vigorous public debate."[269]

Evaluating these arguments in August 2013, the FISA Court concluded without difficulty that Congress had been sufficiently briefed, and so had incorporated the FISC's interpretation in reauthorizing the law. The court explained: "Congress re-authorized Section 215 of the PATRIOT Act without change in 2011,"[270] and was sufficiently aware of the FISC's interpretation of the statute to satisfy the legal requirements for ratification through reenactment. In December 2013, a district judge in the Southern District of New York reached the same conclusion: "viewing all the circumstances presented here in the national security context, this Court finds that Congress ratified section 215 as interpreted by the Executive Branch and the FISC, when it reauthorized FISA."[271]

In October 2013, the FISC released an opinion again authorizing the bulk collection.[272] This opinion, written by Judge Mary McLaughlin, was noteworthy in at least three respects. First, it explicitly endorsed the August 2013 opinion, including the ratification argument, which had been written by another FISC judge; but the October opinion stated that this was "the first time" that Judge McLaughlin herself had "entertained an application requesting the bulk production of call detail records," making clear that she was not locked in to a prior position.[273] Second, unlike the August opinion, which had explicitly disclaimed any reliance on the government's White Paper and (at least implicitly) publicly-available criticism of the White Paper and the FISC's own prior rulings, including constitutional attacks based on the Supreme Court's decision in U.S. v. Jones,[274] the October opinion explicitly discussed Jones and concluded that it posed no barrier to the collection.[275] Third, although Judge

268. *See* Jerman v. Carlisle, McNellie, Rini, Kramer & Ulrich LPA, 559 U.S. 573, 130 S. Ct. 1605, 1626 & n.1 (2010).

269. POTUS Sigint Speech, *supra* note 49.

270. August 2013 FISC Order, *supra* note 4, at 24. The court did not discuss the issue of the House Intelligence Committee possibly refusing to honor the Executive Branch's request to provide information to all Members of the House in 2011, as discussed above.

271. ACLU Opinion, *supra* note 113, at *16.

272. October 11, 2013 FISC Opinion, *supra* note 29.

273. *Id.* at 3.

274. 132 S. Ct. 945 (2013). *See* August 2013 FISC Opinion, *supra* note 4 at 3 n.4.

275. Judge McLaughlin stated:

> Justice Soyomayor stated in her concurring opinion in Jones that it "may be necessary" for the Supreme Court to "reconsider the premise that an individual has no reasonable expectation of

McLaughlin of course did not say so in her opinion, she was appointed to the federal bench by President Clinton – a notable fact in light of the media attention paid to the composition of the FISC in the context of its rulings on bulk metadata collection, as discussed above. Whatever the FISC's actual motivations for writing and releasing the October opinion, therefore, it could be viewed as noteworthy in that it was written by a Democratically-appointed judge who had not previously reviewed the bulk collection program and who specifically addressed and rejected the main constitutional claim advanced by critics of the program since its public debut.

2. Unlike Members of Congress, most Americans had no opportunity to become aware of the bulk collection program, at least through official channels. While reasonable minds may disagree as to whether the FISC was correct (in the first instance) to accept the government's legal interpretation of the tangible things provision – particularly the argument that the bulk metadata is "relevant" – it seems clear that the interpretation was not obvious, not something that would inevitably have occurred to an outside observer. This is probably the case even after accounting for media reporting (based on prior leaks) that bulk telephony metadata collection was in fact occurring, as noted above.[276] And the government, by determining that the interpretation was classified, or at least that disclosure of the interpretation would inevitably result in disclosure of classified information, kept the information from the public. The following exchange between Chairman Goodlatte and Bob Litt, the General Counsel of ODNI, at a July 2013 hearing of the House Judiciary Committee, captures the point:

> QUESTION: Did you think a program of this magnitude gathering information involving a large number of people involved with telephone companies could be indefinitely kept secret from the American People?
>
> ANSWER: Well, we tried.[277]

a. At one level, of course, keeping classified information from the American People is exactly what the Intelligence Community is supposed to do, because there is no way to inform the American People without also informing the People's adversaries. There is no serious debate about that general proposition, which amounts only to the familiar idea that some information is indeed properly classified. The United States is a representative democracy, not a direct

---

privacy in information voluntarily disclosed to third parties," . . . . But Justice Sotomayor also made clear that the Court undertook no such reconsideration in Jones."

October 11, 2013 FISC Opinion, *supra* note 29, at 5.

276. As explained in Chapter 15 of NSIP, *supra* note 1, it was possible, based solely on publicly available information, to guess at the legal arguments now disclosed to have underlay the TSP, in part because the government confirmed the existence of the TSP after it was leaked in 2005, much as it did eight years later with respect to the bulk metadata collection after it was leaked in June 2013.

277. July 2013 HJC Hearing, *supra* note 23, Statement of Bob Litt.

one, and in respect of classified matters, the Intelligence Committees "serve as the proxy for the American people."[278] As Senator Chambliss, the Vice Chair of the Senate Intelligence Committee, explained in 2012, "In matters concerning the FISA Court, the congressional Intelligence and Judiciary Committees serve as the eyes and ears of the American people. Through this oversight, which includes being given all significant decisions, orders, and opinions of the court, we can ensure that the laws are being applied and implemented as Congress intended."[279]

To be sure, as NSIP and this paper illustrate, there are many situations in which, through extremely intense, prolonged effort, it is possible to find ways to disclose legal interpretations of FISA and other statutes without harming national security.[280] But there are obviously many other situations in which, despite such efforts, no solution emerges. As explained in the Foreword to the First Edition, NSIP "is not what we would have written for an audience of government officials with security clearances and a need to know." The result, in the vocabulary preferred by proponents of transparency, is that there may effectively be areas of "secret law" – i.e., the application of public laws to secret facts – that cannot be disclosed. This is true with respect to FISA and also to many other statutes, as well as the Constitution itself.

For example, the covert action statute[281] could be interpreted and applied in ways that may be extraordinarily important, but about which very, very few Members of Congress, let alone the American People, ever learn.[282] The statute defines covert action to exclude "traditional" military and law-enforcement activities,[283] provides that a covert action finding "may not authorize any action that would violate the Constitution or any statute of the United States,"[284] and

278. *Congressional Oversight of Intelligence Activities, Before the Senate Select Committee on Intelligence*, 110th Cong. 15 (Nov. 13, 2007) (statement of Lee Hamilton), *available at* http://www.intelligence.senate.gov/pdfs/110794.pdf.

279. 158 Cong. Rec. S8411 (Dec. 27, 2012) (statement of Sen. Chambliss). For an interesting assessment of the evolution of oversight by the Intelligence Committees, written by a longtime observer, see Steven Aftergood, *Intelligence Oversight Steps Back from Public Accountability*, SECRECY NEWS (Jan. 2, 2013), http://blogs.fas.org/secrecy/2013/01/public_accountability/. As former Representative Jane Harman put it in July 2013, "the tradition has always been that the Members of the Intelligence Committees, which are leadership committees . . . were trusted with a lot of secrets that weren't shared with others; the reason for that was . . . sources and methods have to be protected." Aspen Institute, Counterterrorism, National Security and the Rule of Law (July 18, 2013) (statement of Jane Harman at approximately 1:05:32), *available at* http://aspensecurityforum.org/2013-video. The Constitution itself provides for secret proceedings in Congress: Under Article I, Section 5, Clause 3, each House of Congress "shall keep a journal of its proceedings, and from time to time publish the same, excepting such parts as may in their judgment require secrecy." U.S. CONST. art. I, §5, cl. 3.

280. *See* 28 C.F.R. § 17.18. The prolonged, intense prepublication review process for the first edition of NSIP is described in the Preface and Foreword, and the review process for this paper is described in note 1, *supra*.

281. 50 U.S.C. § 413b.

282. *See generally* ALFRED CUMMING AND RICHARD A. BEST, JR., CONG. RESEARCH SERV., R40691, SENSITIVE COVERT ACTION NOTIFICATIONS: OVERSIGHT OPTIONS FOR CONGRESS (Jan. 10, 2006).

283. 50 U.S.C. § 413b(e)(2).

284. 50 U.S.C. § 413b(a)(5).

specifically warns that "No covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or media."[285] Without making any comment, express or implied, on any actual or hypothetical covert action, or even acknowledging that any covert action of any kind has ever actually taken place, it is quite obvious that each of those elements of the statute could raise enormously difficult and complex interpretive questions, some of which might affect many Americans.[286] Yet it might be impossible, in many cases, to explain those interpretations without revealing the most sensitive classified information.[287]

With respect to bulk metadata collection, the Intelligence Community seems to have concluded, over a long period of time across two Presidential Administrations, that the legal interpretation was so embedded in its factual and operational context that revealing it would harm national security. Nor did any Member of Congress, including Senators Wyden and Udall, or the FISA Court itself, find a satisfactory way to reveal the legal issue without causing collateral damage. The FISC rejected as unrealistic a request from the Senate Intelligence Committee to prepare unclassified summaries of its opinions, explaining that "in most cases, the facts and legal analysis are so inextricably intertwined that excising the classified information from the FISC's analysis would result in a remnant void of much or any useful meaning."[288] Until the June 2013 unauthorized disclosures, none of the three branches of government had found a safe way to disclose to the public the "secret law" underlying the bulk telephony metadata collection program.

The difficulty, as Senators Wyden and Udall explained in their many public statements on this issue, arises when a leak reveals "secret law" involving a

---

285. 50 U.S.C. § 413b(f).

286. Put differently, it would be easy for even a relatively competent law professor, with no classified information, to write a challenging law school exam based on the language of the covert action statute.

287. For a humorous take on the potential implications of this very serious issue taken to a ridiculous extreme, see *231 CIA Agents Killed in Overt Ops Mission*, THE ONION (Mar. 6. 2013), http://www.theonion.com/articles/231-cia-agents-killed-in-overt-ops-mission,31553/?ref=auto.

288. Senators Wyden and Udall, along with Senators Feinstein and Merkley, sent a letter to the FISA Court in February 2013, in which they "request[ed] that the Court consider writing summaries of its significant interpretations of the law in a manner that separates the classified facts of the application under review from the legal analysis, so as to enable declassification." Letter from Senators Ron Wyden, Tom Udall, Dianne Feinstein, & Jeff Merkley to the FISA Court (Feb. 13, 2013), *available* at http://www.fas.org/irp/agency/doj/fisa/fisc-021313.pdf. In a letter dated March 27, 2013, Judge Walton, the Presiding Judge of the Court, replied that there were "serious obstacles . . . regarding your request for summaries of FISC opinions," including the risk of "misunderstanding or confusion regarding the court's decision or reasoning," and for "FISC opinions specifically . . . the very real problem of separating the classified facts from the legal analysis . . . . As members of Congress who have seen the opinions know, most FISC opinions rest heavily on the facts presented in the particular matter before the court. Thus, in most cases, the facts and the legal analysis are so inextricably intertwined that excising the classified information from the FISC's analysis would result in a remnant void of much or any useful meaning." Letter from Judge Walton, the Presiding Judge of the FISA Court, to Senator Dianne Feinstein (Mar. 27, 2013), *available at* http://www.fas.org/irp/agency/doj/fisa/fisc-032713.pdf.

non-obvious legal interpretation underlying the collection of information pertaining to many, many Americans. As the Senators wrote in 2012, "[w]e believe most Americans would be stunned to learn the details of how these secret court opinions have interpreted [the tangible things provision]. As we see it, there is now a significant gap between what most Americans think the law allows and what the government secretly claims the law allows."[289] Senator Wyden predicted in the Congressional Record that "when the American People find out how their government has secretly interpreted the Patriot Act, they are going to be stunned and they are going to be angry."[290] For some observers, it may be puzzling that a massive, unauthorized disclosure of classified information, concerning an intelligence program effectively endorsed by all three branches of government over many years, would produce a political demand for greater disclosures and transparency. For other observers, however, the main problem is that so many aspects of so many intelligence programs were classified (or existed) in the first place.

b. As of this writing, it appears that the issue of "secret law" could be addressed in one or more of three ways that differ from the status quo. First, perhaps the Executive Branch and Congress could work together on ways to make classified briefings more accessible and understandable to Members not serving on the Intelligence or Judiciary Committees. As noted elsewhere, surveillance law today is staggeringly complex,[291] and the complexity poses significant challenges for both providers and recipients of classified briefings. It might also be helpful for one or both branches to keep and regularly publish a formal log of briefings, including when they are offered, when and where they are conducted, their duration, the names (or at least the agency affiliations) of the briefers, the names of invitees, the names of attendees, and the subject-matter of the briefing (with a classified annex as necessary).

This first approach would maintain the essential balance struck in the 1970s, and reflected in statutes like 50 U.S.C. § 1871, in which the Intelligence (and Judiciary) Committees continue to serve as the proxy for the rest of Congress, and the American People, in oversight of classified intelligence activities, but would allow for more briefings of the full Congress. Of course, if this approach takes hold sufficiently, and particularly if a comprehensive log is indeed maintained and published, Members of Congress who eschew classified briefings might be criticized for dereliction of duty, and the Executive Branch might be criticized for failing to provide adequate briefings of intelligence activities later revealed through other means. Apart from that, however, this first approach would not directly increase the general public's knowledge about the operational and other details of intelligence activity.

289. Wyden-Udall Letter of March 15, 2012, *supra* note 256, at 2.

290. 157 Cong. Rec. S3372 (May 26, 2011).

291. *See* David Kris, *Thoughts on a Blue Sky Overhaul of Surveillance Laws*, LAWFARE (May 18-21, 2013), http://www.lawfareblog.com/author/dkris/.

Second, Congress could take measures to help ensure broader public understanding, still without departing too far from the traditional approach. One obvious possibility would be to revive the annual reports from the Intelligence Committees that were required for the first five years of FISA's existence.[292] Those reports, which were very well done and extremely informative, are cited throughout this treatise. Such public reporting could be conducted pursuant to statute or even in the absence of new legislation. It would require considerable and sustained effort from the two political branches, working together, but it could be done. Of course, as noted above, significant limits would remain, meaning that much would need to remain secret, but it would be reasonable to expect at least incremental gains in transparency and public understanding. It would facilitate a more informed debate over the broad policy choices and challenges in the area, but limit disclosure of operational details and related information concerning specific intelligence programs. In some cases, those details are important to understanding the programs and their legality, so this approach would not allow for a "fully and currently informed" public debate.

Third and finally, we could significantly re-calibrate the balance between secrecy and transparency, revealing significantly more information publicly, and thus reducing reliance on proxy oversight through select Congressional Committees. Although the matter is not entirely clear,[293] that appears to be the Obama Administration's intent, at least to a substantial degree.[294] In June 2013, President Obama stated through a spokesperson that he "welcomes the discus-

---

292. *See* 50 U.S.C. § 1808(b).

293. As the President noted in January 2014, "[t]he challenge is getting the details right, and that is not simple." POTUS Sigint Speech, *supra* note 49. Moreover, the Administration has not publicly described the philosophical approach underlying the already-significant disclosures it has made, the limits on such disclosures, or a comparison between the current attitude and historical standards – although such thinking may well exist behind the scenes.

294. *Cf.* Jack Goldsmith, Alexander and Inglis *Letter to the NSA-CSS Family and the USG's Unconscionably Weak Defense of NSA*, LAWFARE (Sept. 20, 2013), *available at* http://www.lawfareblog.com/2013/09/alexander-and-inglis-letter-to-the-nsacss-family-and-the-usgs-unconscionably-weak-defense-of-nsa/. It is far from clear that his views are aligned with those of the President and the President's closest advisors, but Chris Inglis, NSA's departing Deputy Director, described an important distinction between transparency in aid of broad policy debate, and transparency concerning operational matters, in an interview given a week before the President's January 2014 speech:

> [W]e're trying to strike that right balance. The balance today I think has a policy component of whether it's broadly permissible, useful, effective to give the kinds of authorities to NSA that we do. And that I think should have a fuller public discussion. But when you get down to the very discreet, right, somewhere between strategic and tactical choices about how you then implement that, I think that we need to then have a closed in discussion between three branches of government, those who stand in the shoes of the American public, so that we can have a fully informed decision that then results from that fully informed dialogue. But I am not at this point saying that I would bring all of NSA's capabilities out into the open. Not because I'm in any way, shape or form thinking that the American public would be shocked or outraged by those but because I really don't think we can afford to give those capabilities away to our adversaries.

Chris Inglis NPR Interview, *supra* note 56.

sion of the trade-off between security and civil liberties,"[295] and that he "look[s] forward to continuing to discuss these critical issues with the American people" as well as with Congress.[296] At a press conference held on August 9, 2013, the President stated:

> we can, and must, be more transparent. So I've directed the intelligence community to make public as much information about these programs as possible. We've already declassified unprecedented information about the NSA, but we can go further . . . . probably what's a fair criticism is my assumption that if we had checks and balances from the courts and Congress, that that traditional system of checks and balances would be enough to give people assurance that these programs were run probably – that assumption I think proved to be undermined by what happened after the leaks . . . . What I'm going to be pushing the IC to do is rather than have a trunk come out here and leg come out there and a tail come out there, let's just put the whole elephant out there so people know exactly what they're looking at.[297]

In his January 2014 speech at the Department of Justice, President Obama promised to "reform programs and procedures in place to provide greater transparency to our surveillance activities," and noted that the government had "declassified over 40 opinions and orders" of the FISC. The speech identified two additional initiatives directly in support of transparency.

First, the President directed the DNI, in consultation with the Attorney General, "to annually review for the purposes of declassification any future opinions of the [FISC] with broad privacy implications, and to report to me and to Congress on these efforts." This may effectively mirror in a public fashion the obligations currently owed by statute to the Intelligence and Judiciary

---

295. Josh Gerstein and Tim Mak, *White House: Obama 'Welcomes' Surveillance Debate*, POLITICO (June 5, 2013), *available at* http://www.politico.com/story/2013/06/report-nsa-verizon-call-records-92315.html.

296. Statement by the Press Secretary on the Amash Amendment (July 23, 2013) ("In light of the recent unauthorized disclosures, the President has said that he welcomes a debate about how best to simultaneously safeguard both our national security and the privacy of our citizens. The Administration has taken various proactive steps to advance this debate including the President's meeting with the Privacy and Civil Liberties Oversight Board, his public statements on the disclosed programs, the Office of the Director of National Intelligence's release of its own public statements, ODNI General Counsel Bob Litt's speech at Brookings, and ODNI's decision to declassify and disclose publicly that the Administration filed an application with the Foreign Intelligence Surveillance Court. We look forward to continuing to discuss these critical issues with the American people and the Congress."), *available at* http://www.whitehouse.gov/the-press-office/2013/07/23/statement-press-secretary-amash-amendment; *see also* The White House, Office of the Press Secretary, Background on the President's Statement on Reforms to NSA Programs ("President Obama believes that there should be increased transparency and reforms in our intelligence programs in order to give the public confidence that these programs have strong oversight and clear protections against abuse."), *available at* http://www.whitehouse.gov/the-press-office/2013/08/09/background-president-s-statement-reforms-nsa-programs.

297. Remarks by the President in a Press Conference, August 9, 2013 (emphasis added) [hereinafter August 2013 Remarks by the President], *available at* http://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference.

Committees of Congress under 50 U.S.C. § 1871. Regular efforts to review and declassify FISA Court opinions have been ongoing for years,[298] but the Presidential imprimatur may help the Intelligence Community lean forward in assessing what can be disclosed without harming national security. As the President noted, "we have declassified over 40 opinions and orders"[299] from the FISC since the June 2013 unauthorized disclosures, which is in itself an unprecedented level of transparency.[300]

Second, the President also seemed to endorse increased disclosure of specific investigative details in some cases, including to the subjects of national security investigations. He directed the Attorney General "to amend how we use national security letters," which (the President explained) "can require companies to provide specific and limited information to the government without disclosing the orders to the subject of the investigation."[301] Under the amended approach, "this secrecy will not be indefinite," and "will terminate within a fixed time unless the government demonstrates a real need for further secrecy."[302] As discussed in § 20:8 of NSIP, the FBI annually issues tens of thousands of national security letters. It is possible to imagine a process under which the President's directive results only in a (potentially significant) administrative burden for the FBI and DOJ, by requiring periodic re-certification of the basis for the initial secrecy directive that is always invoked for each NSL,[303] with directives being allowed to lapse only rarely and after relatively long periods of

298. *See* June 2013 HPSCI Open Hearing, *supra* note 27, Statement of Bob Litt ("It's been a very difficult task . . . . The facts frequently involve classified information, sensitive sources and methods. And what we've been discovering is that when you remove all the information that needs to be classified, you're left with something that looks like Swiss cheese and is not really very comprehensible"); July 2013 SJC Hearing, *supra* note 27, Statement of Bob Litt ("[W]e should strive for the maximum possible transparency about the activities of the court, consistent with the need to protect sensitive sources and methods. We have been working for some time to declassify the court's opinions to the extent possible. But legal discussions and court opinions don't take place in a vacuum. They derive from the facts of the particular – of the particular case. And I want to quote here from Judge Walton, who is now chief judge of the FISA court, who said in a letter to the foreign – to the Senate Intelligence Committee, quote, 'Most FISC opinions rest heavily on the facts presented in the particular matter before the court. Thus in most cases, the facts and legal analysis are so inextricably intertwined that excising the classified information from the FISC analysis would result in a remnant void of much or any useful meaning,' close quote. That's an excellent and pithy summary of the challenge we face in trying to declassify these opinions.").

299. POTUS Sigint Speech, *supra* note 49.

300. On January 27, 2014, the Department of Justice announced an agreement to settle litigation in the FISA Court brought by telecommunications providers and other companies. Under the terms of the agreement, providers may publish certain data about information requests from the government, in the aggregate, in bands of 1000 (e.g., 0-999 requests, 1000-2000 requests), divided into content and non-content categories, with a time lag between receipt of the requests and publication of the data. *See* Notice filed in the Foreign Intelligence Surveillance Court, Nos. 13-03 to 13-07 (Jan. 27, 2014), *available at* http://legaltimes.typepad.com/files/fisa-notice-1.pdf. Publicly available pleadings filed in the FISA Court after June 2013 are available at http://www.uscourts.gov/uscourts/courts/fisc/index.html.

301. POTUS Sigint Speech, *supra* note 49.

302. *Id.*

303. For a discussion of the certification process, see NSIP, *supra* note 1, at § 20:10.

time. But it is also possible to imagine a more significant effect, where the FBI discloses large numbers of NSLs after relatively short periods of secrecy.

Of course, as the President recognized, a central "challenge is getting the details right, and that is not simple." Moreover, it remains unclear whether and to what extent increased transparency will extend further, to other intelligence programs – e.g., those involving Humint or covert action – that have not been subjected to the same level of prior, unauthorized disclosure.[304] The focus since June 2013 has been on signals intelligence, because that was the subject of the unauthorized disclosures, but the logic animating efforts towards transparency could extend further, to other forms of intelligence activity. To some observers, the President and his closest advisors seem to be charting a course for an environment in which the basic existence of all (or most) intelligence programs, or at least signals intelligence programs, is publicly disclosed, with information about certain operational details (e.g., providers and targets) still mostly secret. They may face resistance from the Intelligence Community in staying that course over time, but if they are successful, it would represent a very significant re-calibration.

The effects of such a broad re-calibration could be felt in at least two ways beyond the government's own, voluntary actions. First, official disclosures of previously classified information will resonate through FOIA and State Secrets doctrine, where the government's litigating positions will be tested for consistency with the logic implicit in the voluntary transparency.[305] It therefore may be difficult to predict exactly how such official disclosures may beget additional disclosures as compelled by the courts, especially in the absence of any overtly described philosophical approach.

Second, and perhaps more importantly, there is a potential interaction be-

---

304. In a July 2013 speech, Bob Litt, General Counsel of ODNI, reiterated that "[e]ven before the recent disclosures, the President said that we welcomed a discussion about privacy and national security, and we are working to declassify more information about our activities to inform that discussion." July 2013 Litt Speech, *supra* note 27, at 21-22. But he also recognized that the "level of detail in the current public debate certainly reflects a departure of the historic understanding that the sensitive nature of intelligence operations demanded a more limited discussion," and that the "discussion can, and should, have taken place without the recent disclosures." *Id.* at 22. As Mr. Litt put it at the July 2013 SJC hearing, "we are having a public debate now, but that public debate is not without cost." July 2013 SJC Hearing, *supra* note 27, Statement of Bob Litt. At his August press conference, President Obama said that although "Mr. Snowden's leaks triggered a much more rapid and passionate response" than otherwise would have been the case, "I actually think we would have gotten to the same place." August 2013 Remarks by the President, *supra* note 297. On the other hand, he also said that the disclosures "put[] at risk our national security and some very vital ways that we are able to get intelligence that we need to secure the country," and that the voluntary disclosures were designed to address the unfortunate fact that:

> Once the information is out, the administration comes in, tries to correct the record. But by that time, it's too late or we've moved on, and a general impression has, I think, taken hold not only among the American public but also around the world that somehow we're out there willy-nilly just sucking in information on everybody and doing what we please with it.

Id.

305. *See* 5 U.S.C. § 552; U.S. v. Reynolds, 345 U.S. 1 (1953).

tween increased transparency and the scope of intelligence activity. Intelligence activity that helps the U.S. government when done covertly may harm it when done overtly. For example, clandestine surveillance of foreign government officials may aid U.S. foreign policy – e.g., by giving U.S. treaty negotiators insight into their foreign counterparts' instructions. As such, foreign policy makers may support and even require such surveillance from the Intelligence Community. On the other hand, however, transparent surveillance of foreign government officials may have precisely the opposite effect, creating challenges that cause policy makers to require less surveillance.[306] If less surveillance leads to a perceived intelligence failure, of course, resulting demands to expand surveillance may cause the pendulum to swing back.[307]

---

306. In October 2013, revelations that the NSA had allegedly been spying on world leaders, including the German Chancellor, created a diplomatic furor. *See, e.g.*, James Kanter and Alan Cowell, *Amid New Storm in U.S.-Europe Relationship, a Call for Talks on Spying*, N.Y. TIMES, Oct. 26, 2013, at A4. Regardless of the sincerity of these expressions of shock and outrage, they clearly had an impact on U.S. policymakers.

It is worth recalling that the debate about surveillance of foreign governmental and diplomatic personnel is not new. The 1978 legislative history of FISA makes absolutely clear that the law was intended to allow surveillance of foreign diplomatic facilities in the United States. *See* H.R. Rep. No. 95-1283, at 27 (1978) (FISA authorizes surveillance of "foreign embassies and consulates and similar 'official' foreign governmental establishments"); S. Rep. No. 95-604, at 19 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904. This approach represented a dramatic change from the position of at least some elements of the United States government in the years prior to World War II, perhaps best summarized by a 1929 statement attributed to U.S. Secretary of State Henry Stimson, that "gentlemen do not read each other's mail." More context for that statement is provided from a 1982 New York Times review of James Bamford's book about the NSA, The Puzzle Palace:

> FIFTY-THREE years ago, in the early months of Herbert Hoover's Administration, Secretary of State Henry L. Stimson was presented with a small batch of Japanese telegrams that had been deciphered by a highly secret American code-breaking organization known as the Black Chamber. Appalled at the invasion of another nation's private communications, Stimson immediately cut off funding to the cryptologists with the admonition "Gentleman do not read each other's mail." It was not one of the more prescient decisions in American history. Driven by the exigencies of World War II and then the Cold War and drawing on advances in computers and electronics, in 1952 the Government created a new version of the Black Chamber – the National Security Agency, which is the largest, most sensitive and potentially most intrusive American intelligence agency.

Philip Taubman, *Sons of the Black Chamber*, N.Y. TIMES, Sept. 19, 1982, at A9.

307. One outside observer described the pendulum effect in more stark terms:

> This is speculation. I have no hard facts or evidence to support it. But I am convinced to a moral certainty that NSA is scaling back certain collection.
>
> That is not something I say with pleasure or triumph but, rather, with frustration, sadness, and worry.
>
> Imagine you were a high-level decision-maker in a clandestine intelligence agency. Imagine that you had played by the rules Congress had laid out for you, worked with oversight mechanisms to fix errors when they happened, and erected strict compliance regimes to minimize mistakes in a mind-bogglingly complex system of signals intelligence collection. Imagine further that when the programs became public, there was a firestorm anyway. Imagine that nearly half of the House of Representatives, pretending it had no idea what you had been doing, voted to end key collection activity. Imagine that in response to the firestorm, the President of the United States – after initially defending the intelligence community – said that what was really needed was more transparency and described the debate as healthy.

c. As of this writing, the Obama Administration has determined not only to increase the transparency of intelligence collection, but also to decrease its scope, albeit perhaps not as much as some observers would prefer. As Lisa Monaco, the President's Counterterrorism Advisor, put it in an editorial in USA Today, the Administration created an outside Review Group "to ensure that privacy and civil liberties are appropriately protected," will give "even greater focus to ensuring that we are balancing our security needs with . . . privacy concerns," and will attempt to "ensure we are collecting information because we *need* it and not just because we *can*."[308]

In December 2013, the Review Group released its report,[309] the basic thrust of which, as one of its members explained in an editorial, is that "we [have] reached a point where it was necessary to re-calibrate our policies and priorities in order to better preserve our nation's core commitment to the values of

---

> Imagine that journalists construed every fact they learned in light of the need to keep feeding at the trough of a source who had stolen a huge volume of highly classified materials and taken it to China and Russia.
>
> What would you do? Here's what: You'd take a hard look at your most forward-leaning programs – and you'd turn them off. You would do this using words like "prudential" and "current environment" – of course standing by the programs' legality in some formal sense, just as the president has stood by you in some formal sense. But just as the president has let the intelligence community swing in the wind, limiting his own exposure by making the problem all your own, you would cut your losses. You wouldn't even be wrong to do so.
>
> And you would do it knowing somewhere in your heart that some day, the pendulum would swing the other way and there would be recriminations for turning those programs off, just as there are now recriminations for having such programs online. You would even know that many of the same people would be responsible for the mutually contradictory recriminations. You would know that after some big attack or intelligence failure, the scoop that you turned off collection tailored to the sort of information you needed to stop that event would be just as irresistible to the Washington Post and the Guardian as was the story that you ran riot over Americans' civil liberties. You would know that the papers would be just as careless with the facts. You would know that the same members of Congress who are today outraged at what your agency is doing would wax outraged then at what it isn't doing. And you would know that almost nobody will bother to know what they are talking about before having very strong opinions about how you fell down on the job and thus bear responsibility for both the smoldering ruins of some federal building somewhere and for destroying American values.
>
> As I say, I have no evidence that this scaling back is taking place, and I don't know what the programs or activities on the blade end of the prudential meat axe look like – so until you look out over those smoldering ruins, feel free to disregard this post and regard it as the alarmist fear-mongering of an apologist for the national security state. But for the record, I dissent from the retrenchment I believe is going on. And here's the standard I would propose for the reevaluation of collection programs and activities that might seem too edgy today given the circumstances: If they were lawful and defensible and necessary pre-Snowden, they are lawful and defensible and necessary today.

Benjamin Wittes, *Recriminations, Pendulum Swings, and What is Probably Happening at NSA*, LAWFARE (Sept. 13, 2013), *available at* http://www.lawfareblog.com/2013/09/recriminations-pendulum-swings-and-what-is-probably-happening-at-nsa/.

308. Lisa Monaco, *Obama Administration: Surveillance Policies Under Review*, USA TODAY (Oct. 24, 2013), *available at* http://www.usatoday.com/story/opinion/2013/10/24/nsa-foreign-leaders-president-obama-lisa-monaco-editorials-debates/3183331/.

309. Review Group Report, *supra* note 113.

personal privacy and individual freedom."[310] The President stated soon thereafter that he "thought they did an excellent job," and promised to deliver a more "definitive" assessment of the Review Group's recommendations in January 2014.[311] In his January 2014 speech, and an accompanying Presidential Policy Directive on signals intelligence,[312] the President made several determinations and issued several directives to the Attorney General and the Director of National Intelligence (DNI). Many of the President's directives leave options open, and require choices to be made, so their full effect is difficult to measure as of this writing.

First, as noted above, the President endorsed creation of an outside "panel of advocates" to "provide an independent voice in significant cases before the Foreign Intelligence Surveillance Court."[313] He called on Congress to enact legislation on this topic, which injects a significant degree of uncertainty until the legislation is finalized.

Second, the President directed the Attorney General and the DNI to adopt what amount to more stringent minimization procedures under Section 702 of the FISA Amendments Act, 50 U.S.C. § 1881a. The President did not mention

---

310. Geoffrey R. Stone, *Inside the President's Review Group: Protecting Security AND Liberty*, HUFFINGTON POST (Dec. 21, 2013), *available at* http://www.huffingtonpost.com/geoffrey-r-stone/inside-the-presidents-rev_b_4485016.html. The Review Group offered 46 recommendations in six categories:

> • Surveillance of U.S. persons (e.g., "important restrictions on the ability of the Foreign Intelligence Surveillance Court (FISC) to compel third parties (such as telephone service providers) to disclose private information to the government," and "similar restrictions on the issuance of National Security Letters . . . [including] prior judicial review except in emergencies," as well as putting an "end" to the current bulk telephony metadata collection program and "transition[ing] to a system in which such metadata is held privately," and requiring greater transparency).
>
> • Surveillance of Non-U.S. persons (e.g., not targeting any non-U.S. person "based solely on that person's political views or religious convictions");
>
> • Setting Priorities and Avoiding Unjustified or Unnecessary Surveillance (e.g., "with a small number of closely allied governments, meeting specific criteria, the US Government should explore understandings or arrangements regarding intelligence collection guidelines and practices with respect to each others' citizens (including, if and where appropriate, intentions, strictures, or limitations with respect to collections)");
>
> • Organizational Reform (e.g., splitting NSA from CyberCommand, and creating a Public Interest Advocate to oppose the government in the FISC).
>
> • Global Communications Technology (e.g., the U.S. government should be "fully supporting and not undermining efforts to create encryption standards [and] making clear that it will not in any way subvert, undermine, weaken, or make vulnerable generally available commercial encryption [and] (3) supporting efforts to encourage the greater use of encryption"); and
>
> • Protecting What We Do Collect (e.g., reverting to need-to-know principles, rather than need-to-share principles, governing the dissemination of classified information within the government).

311. Press Conference by the President (Dec. 20, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/12/20/press-conference-president.

312. Presidential Policy Directive – Signals Intelligence Activities (Jan. 17, 2014) [hereinafter PPD-28], *available at* http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

313. POTUS Sigint Speech, *supra* note 49.

the FISA Court in this directive, so it may be that the restrictions will be internal to the executive branch, rather than official (and judicially enforceable) FAA minimization procedures,[314] but they will still restrict the government's behavior, even if they do not create rights in any individual.[315]

These new restrictions, the President said, will be "on government's ability to retain, search, and use in criminal cases communications between Americans and foreign citizens incidentally collected under Section 702" of the FISA Amendments Act, 50 U.S.C. § 1881a.[316] To understand these new restrictions, including what they mean and how they may work in practice, it is necessary first to understand the pre-existing rules, beginning with the idea of "incidental" collection.

As discussed in Chapter 17 of NSIP, Section 702 of the FAA allows the government to target non-U.S. persons reasonably believed to be located abroad. Incidental collection occurs under Section 702, as it does under all forms of electronic surveillance, because the government collects both sides of communications involving its surveillance target. In particular, under Section 702, when the government targets a non-U.S. person located abroad, it will acquire his communications with all interlocutors, including any who happen to be U.S. persons (or are located in the United States). Such incidental collection does not violate the FAA's explicit ban on "reverse targeting," in which, for example, the government pretends to be interested in Smith, a non-U.S. person located abroad, but is actually seeking information from or about Jones, a U.S. person (and hence an invalid target), with whom Smith communicates.[317] Properly targeting Smith will still result in incidental collection of some statements made by Jones.

Under existing procedures, the NSA generally may not retain information

---

314. For a discussion of the FAA, and minimization procedures issued under it, see NSIP, *supra* note 1, at Chapter 17.

315. *See, e.g.*, U.S. v. Caceres 440 U.S. 741 (1979).

316. POTUS Sigint Speech, *supra* note 49.

317. For a discussion of reverse targeting and querying under Section 702 of the FAA, see NSIP, *supra* note 1, at Chapter 17. Chris Inglis, the Deputy Director of NSA, explained this issue in an interview conducted in January 2014:

> So let's say that I'm going after . . . the head of Al-Qaeda worldwide . . . . I collect some of his communications . . . . and they're now in a pile that I expect an analyst to then understand . . . . . The only way the U.S. persons could've gotten into that pile is that they are, in fact, on the other side of the communication of [him] . . . . And the 702 provision goes so far as to say that we cannot use [it] . . . to reverse-target Americans . . . . That's expressly prohibited by the law . . . . So let's say some clever person says, you know, I'm not authorized to target Chris Inglis overtly, unless I go get a warrant and he's not done anything to show himself as being a threat to the nation. But I know that he's always in contact with somebody that I am legitimately authorized to go after or I could make some plausible case for that. So why I don't go after Party B because I know that Chris is always in contact with him and I'll just collect enough communications that gives me insight into Chris Inglis? That is expressly prohibited by the law. It's written in that you cannot use that as a back door, as a 702 back door, the authority being 702, to target Chris Inglis. It's called reverse targeting.

Chris Inglis NPR Interview, *supra* note 56.

acquired under Section 702 that is recognized to be "of" or "concerning" a U.S. person,[318] but it is permitted to retain such information in two main instances. First, NSA may retain U.S. person information if it constitutes "foreign intelligence information" as defined in FISA, including both "protective" and "affirmative" foreign intelligence information.[319] That is, NSA may retain U.S. person information that is necessary to the ability of the United States to "protect" against several specified threats to national security, such as attack, sabotage, espionage, and terrorism; and it also may retain U.S. person information if it is affirmatively necessary to the national defense, national security, or the conduct of the foreign affairs of the United States.[320] Second, NSA may also retain U.S. person information if it constitutes evidence of a crime, including crimes that are wholly unrelated to foreign intelligence and national security (e.g., gambling or child pornography).[321] And NSA may also share such information with law enforcement agencies for use in a criminal prosecution of the U.S. person.[322] Finally, under pre-existing rules, although information acquired from "upstream" collection under Section 702 may not be queried using U.S. person identifiers (e.g., a U.S. person's name, email address, or telephone number[323]),

318. Minimization Procedures Used by the National Security Agency in Connection with Acquisition of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, §§ 3(b), (c) (Oct. 31, 2011) [hereinafter 2011 NSA 702 Minimization Procedures], *available at* http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf. The minimization procedures define communications "of" a U.S. person as all communications "to which a United States person is a party," and communications "concerning" a U.S. person as "all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly-available information about the person." *Id.* at §§ 2(c), (b). For a more complete discussion of minimization, see NSIP, *supra* note 1, at Chapter 9.

319. 2011 NSA 702 Minimization Procedures, *supra* note 318, at §§ 3(b)(4), 6(a)(3). For a discussion of FISA's definition of "foreign intelligence information," as set forth in 50 U.S.C. §§ 1801(e)(1) and (2), see NSIP, *supra* note 1, at §§ 8:1 *et seq.*

320. *See* 50 U.S.C. §§ 1801(e)(1)-(2) (definitions of "foreign intelligence information"), 1881(a) (incorporating these definitions for purposes of Section 702 of the FAA).

321. 2011 NSA 702 Minimization Procedures, *supra* note 318, at §§ 3(b)(4), 6(a)(3). Section 2.3(i) of Executive Order 12,333 provides for Intelligence Community elements to have procedures that allow collection, retention and dissemination of "Incidentally obtained information that may indicate involvement in activities that may violate Federal, state, local, or foreign laws." This may need to be changed in light of the President's speech.

322. 2011 NSA 702 Minimization Procedures, *supra* note 318, at § 6(b)(8) ("dissemination of intelligence reports based on communications of or concerning a U.S. person may only be made to a recipient requiring the identity of such person for the performance of official duties . . . if . . . the communication or information is reasonably believed to contain evidence that a crime has been, is being, or is about to be committed"). Since 1978, FISA has allowed use of lawfully collected information for any kind of criminal prosecution, even while restricting the purpose of the collection. As discussed in Chapters 9 and 17 of NSIP, *supra* note 1, under 50 U.S.C. § 1801(h)(3), "minimization procedures" are defined to include procedures that "notwithstanding [other elements of minimization] . . . allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." 50 U.S.C. § 1801(h)(3).

323. Under the NSA Section 702 minimization procedures (§ 2(f)), identification of a U.S. person means:

information collected from "downstream" collection (e.g., directly from Internet Service Providers) may be so queried, as long as there is a valid foreign intelligence purpose for the querying.[324]

The new restrictions will presumably limit both the retention and dissemination of U.S. person information that is evidence of a crime. One possible approach would be to retain only evidence of "foreign intelligence crimes," such as espionage or terrorism, but that would essentially eliminate law-enforcement retention and dissemination altogether, because evidence of such crimes is always independently "foreign intelligence information."[325] Another approach, perhaps more likely, is to identify a group of more serious crimes, whether or not related to foreign intelligence, as to which evidence obtained through Section 702 may be retained and disseminated.[326]

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

---

> (1) the name, unique title, or address of a United States person; or (2) other personal identifiers of a United States person when appearing in the context of activities conducted by that person. A reference to a product by brand name, or a manufacturer's name or the use of a name in a descriptive sense, e.g., 'Monroe Doctrine,' is not an identification of a United States person.

Office of the Dir. of Nat'l Intelligence, *Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended*, *available at* http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf.

324. 2011 NSA 702 Minimization Procedures, *supra* note 318, at § 3(b)(6) ("Magnetic tapes or other storage media containing communications acquired pursuant to section 702 may be scanned by computer to identify and select communications for analysis. Computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, will be limited to those selection terms reasonably likely to return foreign intelligence information. Identifiers of an identifiable U.S. person may not be used as terms to identify and select for analysis any Internet communication acquired through NSA's upstream collection techniques.").

325. For a discussion of "foreign intelligence crimes" and "ordinary crimes" as used in FISA, see NSIP, *supra* note 1, at Chapters 10-11.

326. One existing and recent effort to define and identify such crimes appears in Part VI of the Department of Justice's July 2013 Report on Review of News Media Policies, and many other definitions also could be found. U.S. Department of Justice, *Report on Review of News Media Policies* (July 12, 2013), *available at* http://www.justice.gov/iso/opa/resources/2202013712162851796893.pdf. The crimes listed in Part VI include a crime involving "(i) death; (ii) kidnapping; (iii) substantial bodily harm; (iv) conduct that constitutes a criminal offense that is a specified offense against a minor as defined in 42 U.S.C. § 16911; or (v) incapacitation or destruction of critical infrastructure as defined in 42 U.S.C. § 5195c(e)." *Id.*

exception), before querying may occur. Depending on the choices made in these areas, the new restrictions announced by the President could be fairly modest, or more substantial in their impact.

Third, the President announced a two-phase approach to modifying the collection of telephony metadata in bulk. "Effective immediately," he said, "we will only pursue phone calls that are two steps removed from a number associated with a terrorist organization instead of the current three."[327] Moving from three "hops" to two "hops" is at least a symbolic modification, and may in fact reduce somewhat the scope of NSA's querying. It is not clear whether the President intended this two-hop limit to be incorporated into FISA Court minimization procedures (assuming the court is willing), or whether it will simply become an Executive Branch policy, even if the court continues to permit three hops.

The President also directed the Attorney General "to work with the Foreign Intelligence Surveillance Court so that . . . the [bulk telephony metadata] database can be queried only after a judicial finding or in the case of a true emergency."[328] As the President recognized, this will require the court's cooperation, likely through adoption of new minimization procedures. For a period of time in 2009, in response to compliance incidents, the FISA Court required the government to submit RAS nominations to the court for approval before querying, subject to a very narrow emergency exception in the case of an imminent threat to life, with after-the-fact reporting to the court of such emergency queries due by the end of the next business day.[329] It is far from clear that the FISA Court enjoyed that protocol, or that it will happily adopt it again now. On the other hand, rejecting an initiative announced by the President of the United States in a major speech would be significant, and so it is likely that when the Attorney General proposes new minimization procedures requiring judicial review of non-emergency RAS findings, the court will, at least to some degree, go along. The main question will be whether the government

---

327. POTUS Sigint Speech, *supra* note 49.

328. POTUS Sigint Speech, *supra* note 49. The President's exact words were:

> Effective immediately, we will only pursue phone calls that are two steps removed from a number associated with a terrorist organization instead of the current three. And I have directed the Attorney General to work with the Foreign Intelligence Surveillance Court so that during this transition period, the database can be queried only after a judicial finding or in the case of a true emergency.

Id. There is some interpretive doubt here, but it may be the President's intent that, unless and until new minimization procedures requiring FISA Court approval of RAS findings are in place, the database may only be queried if there is a "true emergency." *Id.* If that is indeed the case, it could conceivably have affected efforts to prepare for the Winter Olympics in Sochi, Russia, which began on February 6, 2014.

329. Under the protocol for RAS findings approved in 2009, the standard for emergency querying of the database was an "imminent threat to human life," with notification to the court due no later than "5:00 p.m., Eastern Time on the next business day after such [emergency] access." In re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things from [Redacted], No. BR 09-01 (FISA Ct. Mar. 5, 2009), *available at* http://www.dni.gov/files/documents/11714/FISC%20Order,%20BR%2009-01.pdf.

proposes, and the court approves, the 2009 emergency protocol, or the more generous, standard FISA protocol for emergencies set out in 50 U.S.C. § 1805(e).[330]

The second phase of the President's directive concerning bulk telephony metadata is far more ambitious: by March 28, 2014,[331] he directed the identification of "options for a new approach that can match the capabilities and fill the gaps that the Section 215 program was designed to address without the government holding this metadata itself."[332] The President recognized that there were "difficult problems" with alternatives in which "the [telecommunications] providers or a third party retain the bulk records," and that "more work needs to be done" on other approaches. As of this writing, it is not clear that a viable alternative will be found and/or implemented by March 28, although some possibilities do exist.[333]

Fourth and finally, the President announced that he had "taken the unprecedented step" of extending to non-U.S. persons certain minimization and other protections governing retention and use of information that heretofore have been applied only to U.S. persons.[334] The President was correct in his characterization of this initiative, which represents a major conceptual shift. Depending on how it is implemented, the initiative could also yield some significant operational consequences.[335]

---

330. Under 50 U.S.C. § 1805(e), "the Attorney General may authorize the emergency employment of electronic surveillance" if, among other things, he "reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained." 50 U.S.C. § 1805(e). In such a case, he must then submit an application to the court within 7 days. *Id.*

331. March 28, 2014 may be the expiration date for the bulk telephony metadata collection order in effect at the time of the President's speech, which was issued by the FISC on January 3, 2014 and publicized by the government on that date. *See* IC ON THE RECORD, http://icontherecord.tumblr.com.

332. POTUS Sigint Speech, *supra* note 49.

333. One possibility would involve NSA continuing to collect, format and maintain physical custody of the data as it does today. But NSA would segregate repositories containing the data so that access is available only through specially credentialed members of a consortium of participating telecommunications providers, or perhaps some other entity from within the government or elsewhere. To be sure, co-locating representatives from providers in government offices has been associated with problems in the past, *see, e.g.*, Department of Justice, Office of the Inspector General, *A Review of the FBI's Use of Exigent Letters and Other Informal Requests for Telephone Records* (Jan. 2010), *available at* http://www.justice.gov/oig/special/s1001r.pdf, and there would certainly be technical issues (including, e.g., non-query access to the data, for maintenance and other non-substantive purposes), but with appropriate attention to oversight, those problems could probably be avoided. Moreover, the cost of third-party personnel to staff the access point would be a tiny, tiny fraction of the cost of moving the data and maintaining it in the (less secure) private sector. The idea might not work, of course, but it seems worth exploring, especially if it can be credibly described as NSA not having "possession" of the data because of the access limits that require the participation of a third party before the data may be queried.

334. POTUS Sigint Speech, *supra* note 49. In particular, the President "directed the DNI, in consultation with the Attorney General, to develop these safeguards [for non-U.S. persons], which will limit the duration that we can hold personal information, while also restricting the use of this information." *Id.*

335. As one thoughtful commentator put it, the President's speech and PPD together were "a defense that signals a great deal more change spiritually than it promises in practical terms, but one that also has

The President elaborated on the conceptual shift through a Presidential Policy Directive, PPD-28, issued on the same day as his speech.[336] The PPD's fundamental insight is that signals intelligence must "take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside."[337] It provides that "all persons have legitimate privacy interests in the handling of their personal information," and it explicitly recognizes the "legitimate privacy and civil liberties concerns of U.S. citizens and citizens of other nations."[338] Section 1 of the PPD, which sets out its basic principles, states that "[p]rivacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities," and that "the United States shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, general, sexual orientation or religion."[339] Section 2, which prescribes limits on bulk collection (discussed below), explains that the limits "are intended to protect the privacy and civil liberties of all persons, whatever their nationality and regardless of where they might reside." Section 4, which applies to the safeguarding of personal information, repeats the idea that "[a]ll persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside," and the recognition that "all persons have legitimate privacy interests in the handling of their personal information."[340] This is in stark contrast to the language of Executive Order 12333, the main internal charter for the U.S. Intelligence Community, which focuses almost exclusively on privacy protections for U.S. persons.[341] As the President said, therefore, PPD-28 represents an unprecedented change in U.S. intelligence policy, at least at the rhetorical level.

The degree of substantive change that will follow from PPD-28 is less certain. Its directives can be divided into several groups according to their likely operational impact. At the outset, in some respects, the PPD serves what might be termed an educational function, explaining certain protections that already

---

a few big wild cards that could, like a jack-in-a-box, spring out a few months from now as more substantial changes than they now appear to be." Benjamin Wittes, *The President's Speech and PPD-28: A Guide for the Perplexed*, LAWFARE (Jan. 20, 2014) [hereinafter Wittes Guide for the Perplexed], *available at* http://www.lawfareblog.com/2014/01/the-presidents-speech-and-ppd-28-a-guide-for-the-perplexed/#.Ut3S7KNOkdV.

336. PPD-28, *supra* note 312.

337. *Id.* at 1 (Introduction).

338. *Id.* at 1-2 (Introduction).

339. *Id.* at 3 (Principles). Interestingly, "national origin" is not among the protected classes listed in the PPD, although it may have been thought to be superfluous in light of references to the other categories.

340. PPD-28, *supra* note 312, at 5 (Safeguards). Section 3 of the PPD, which governs the process for Sigint, does not specifically refer to non-U.S. persons.

341. *See* United States Intelligence Activities, Exec. Order No. 12,333 §§ 1.1(b), 2.3, 2.4, 2.5, 3 C.F.R. 200 (1981) [hereinafter EO 12,333]. PPD-28 expressly cites and borrows some terms from EO 12,333, *see, e.g.*, PPD-28, *supra* note 312, at 1 n.1 (Introduction). For a discussion of EO 12,333 and related procedures, see NSIP, *supra* note 1, at Chapter 2.

exist in the way the U.S. Intelligence Community does business.[342] These include the requirement that all Sigint "shall be authorized by statute" or other authority, and be conducted strictly in accordance with the Constitution and U.S. laws;[343] that Sigint may not be used to offer a competitive advantage to U.S. businesses;[344] that Sigint requirements are to be established through the inter-agency process on an annual basis;[345] and probably that Sigint "shall be conducted exclusively where there is a foreign intelligence or counterintelligence purpose."[346]

In three other, related areas, the PPD may or may not lead to significant change. First, it requires that Sigint "should be as tailored as possible,"[347] which differs slightly from the pre-existing requirement in EO 12333 that the Intelligence Community "shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad,"[348]

---

342. Another way of putting this, as one commentator has, is that the PPD uses "values-based statements as justifications for policies that already exist, at least de facto, for purely functional reasons." Wittes Guide for the Perplexed, *supra* note 335.

343. PPD-28, *supra* note 312, at 2-3 (Section 1(a)).

344. *Id.* at 3 (Section 1(c)). The PPD is careful to note that "[c]ertain economic purposes, such as identifying trade or sanctions violations or government influence or direction, shall not constitute competitive advantage" for these purposes. *Id.* at 3 n.4.

345. *Id.* at 4 (Section 3).

346. *Id.* at 3 (Section 1(b)). The PPD cross-references Executive Order 12,333's definition of these terms. *Id.* at 2 n.2 (Introduction). Under Executive Order 12,333 §§ 3.5(a) and (e), "*Counterintelligence* means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or their agents, or international terrorist organizations or activities," and "*Foreign intelligence* means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists." EO 12,333 §§ 3.5(a), (e). For a discussion of the meaning of these terms, see NSIP, *supra* note 1, at § 2:7. Under Section 2.3 of Executive Order 12,333, the Intelligence Community may collect not only foreign intelligence and counterintelligence, but also, among others:

> Information obtained in the course of a lawful foreign intelligence, counterintelligence, international drug or international terrorism investigation . . . . Information needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of international terrorist organizations . . . . Information needed to protect foreign intelligence or counterintelligence sources, methods, and activities from unauthorized disclosure . . . . . Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility . . . . [and] Information arising out of a lawful personnel, physical, or communications security investigation.

EO 12,333 § 2.3. Most of these additional categories can, in most cases, probably be fit under the broad rubric of "a foreign intelligence or counterintelligence purpose" as described by PPD-28, but there may be exceptions to that general rule. It is not clear why the PPD omitted these categories of information, and/or why it did not simply cross-reference Section 2.3 here, as it did elsewhere. If there was an intent to exclude some forms of Sigint, the intent was not communicated clearly.

347. PPD-28, *supra* note 312, at 3 (Section 1(d)).

348. EO 12,333 § 2.4. The PPD "is not intended to alter the rules applicable to U.S. persons in Executive Order 12,333." PPD-28, *supra* note 312, at 5 n.9. Thus, as a technical matter, the PPD sets the "as tailored as feasible" standard for Sigint directed at non-U.S. persons located abroad, and the executive order continues to require the "least intrusive" standard for all collection techniques (including but not limited to Sigint) used in the U.S. or against U.S. persons abroad. It is not clear that there is

but also applies to Sigint collection directed against non-U.S. persons abroad. The extent of this tailoring, like the extent of the dignity and respect afforded to non-U.S. persons' privacy, will determine its significance.[349] A requirement that each instantiation of EO 12333 surveillance abroad be reviewed and approved individually by a high-level, inter-agency panel, for example, could substantially hinder the speed and agility (and perhaps, therefore, the effectiveness) of such surveillance, even if most surveillance is ultimately approved as sufficiently tailored.

Second, in the same vein, the PPD instructs the Intelligence Community to prioritize "appropriate and feasible alternatives to signals intelligence," such as information "from diplomatic and public sources" (but also presumably including Humint and other intelligence disciplines).[350] Again, the degree of such prioritization will determine the effects of this requirement. For example, if proponents of Sigint within the U.S. Intelligence Community must rebut a presumption against collection in each case, the effects could be substantial. Again, those effects could arise not only because of the ultimate scope of Sigint that is permitted, but also because of the demands of the process itself. If, on the other hand, the prioritization means only that the United States will attempt to work cooperatively with foreign partners on Sigint conducted in their territory, or will try to use overt diplomatic channels more frequently to gather information from or about allied government leaders (e.g., the Chancellor of Germany), it may not have as much of an impact.

Third, with respect to data collected in bulk,[351] the PPD provides that it may

---

any meaningful difference in these two formulations in practice. The concept of "narrow tailoring" is typically associated with jurisprudence involving the First Amendment rather than the Fourth Amendment. *See, e.g.*, Boos v. Barry, 485 U.S. 312 (1988). Perhaps it is meant to address or create a presumption against bulk collection, although the PPD elsewhere addresses bulk collection directly, and it is not impossible to imagine some forms of "tailored bulk collection."

349. One thoughtful commentator assessed the PPD this way:

> The United States is now on record as a formal matter of presidential policy announcing that it respects the privacy of non-citizens abroad and takes that into account when it conducts espionage; it doesn't just disseminate and retain information about people willy nilly with no regard for the information's importance relative to that material's value to foreign intelligence. That's an amazing statement. But it actually does not require a revolution – or even much change – in intelligence affairs to implement. The reason is that the US, at least in the modern age, has not disseminated or retained willy nilly private information about foreign individuals without regard for its intelligence value – not because the intelligence community has been especially concerned about foreigners' privacy rights as such, but because indiscriminate collection and dissemination is inimical to good intelligence product.

Wittes Guide for the Perplexed, *supra* note 335. Although the PPD certainly does not "require" a profound change in intelligence affairs, it could produce such change depending on how it is implemented over time.

350. PPD-28, *supra* note 312, at 3 (Section 1(d)).

351. The PPD defines "bulk" collection as "the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.)." PPD-28, *supra* note 312, at 3 n.5 (Section 2). This definition does not refer explicitly to what may be the key feature of bulk collection,

be used only for counterintelligence or protective intelligence purposes and law enforcement, not for affirmative foreign intelligence collection.[352] As noted above, the bulk telephony metadata program may only be used for counterterrorism, and so with respect to that particular program, the PPD represents an expansion of permitted purposes (of course, adherence to the narrower requirements set by the FISA Court is still required). However, the PPD provides for changes to the permitted purposes of bulk collection over time,[353] not all of which must be made public.[354] Much will depend, therefore, on whether those permitted purposes are held static, expanded, or contracted over time. Implemented aggressively, each of the foregoing three directives could have a non-trivial effect on signals intelligence operations; but there is also room to apply them in ways that do not substantially curb existing activities.

The final element of the PPD is the one the President emphasized in his speech: its command that, "[t]o the maximum extent feasible consistent with the national security," the government adopt "policies and procedures . . . for safeguarding personal information collected from signals intelligence activities," and that those procedures be "applied equally to the personal information of all persons, regardless of nationality."[355] Conceptually, as noted above, this is a major change in U.S. policy. But the immediate, operational impact of the PPD in this area is probably more modest. The new policies and procedures required by the PPD are due within one year, must be disclosed publicly to the

---

which is that it allows long-term storage (e.g., not merely for buffering or processing) of large quantities of data that may later be queried using selectors that are unknown at the time of the collection.

352. The PPD describes the permitted uses of data collected in bulk as "detecting and countering"

> (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied Armed Forces or other U.S or allied personnel; and (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section.

Id.

This list does not include the "affirmative" foreign intelligence purposes listed in statutes like 50 U.S.C. § 1801(e)(2) – i.e., "information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to . . . (A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States." 50 U.S.C. § 1801(e)(2). For a discussion of the difference between affirmative foreign intelligence and foreign counterintelligence, and FISA's definition of "foreign intelligence information," see NSIP, *supra* note 1, at §§ 8:1 *et seq.* The PPD is careful to state that short-term buffering of bulk data, for processing and selecting a narrower set of desired data – e.g., selecting certain communications from a large communications facility – is not itself bulk collection. PPD-28, *supra* note 312, at 3 n.5.

353. *Id.* at 4 (Section 2) (requiring at least annual reviews of permitted uses of signals intelligence collected in bulk).

354. *Id.* at 4 (Section 2) (requiring the DNI to maintain "a list of the permissible uses of signals intelligence collected in bulk," which shall be "made publicly available to the maximum extent feasible, consistent with the national security").

355. *Id.* at 5 (Section 4(a)).

maximum extent possible consistent with national security, and must do all of the following:[356]

- Retention: allow retention of personal information "only if the retention of comparable information concerning U.S. persons would be permitted under section 2.3 of Executive Order 12333,"[357] and "subject to the same retention periods as applied to comparable information concerning U.S. persons." Absent a determination of comparability, there is a five-year cap on retention "unless the DNI expressly determines that continued retention is in the national security interests of the

356. *Id.* at 7 (Section 4(b)).

357. As discussed in NSIP, *supra* note 1, at § 2:7, Section 2.3 of Executive Order 12,333 provides for procedures established by the head of each Intelligence Community element and approved by the Attorney General that "shall permit collection, retention, and dissemination of the following types of information:"

> (a) Information that is publicly available or collected with the consent of the person concerned;
>
> (b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the Federal Bureau of Investigation (FBI) or, when significant foreign intelligence is sought, by other authorized elements of the Intelligence Community, provided that no foreign intelligence collection by such elements may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;
>
> (c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international drug or international terrorism investigation;
>
> (d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of international terrorist organizations;
>
> (e) Information needed to protect foreign intelligence or counterintelligence sources, methods, and activities from unauthorized disclosure. Collection within the United States shall be undertaken by the FBI except that other elements of the Intelligence Community may also collect such information concerning present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for any such employment or contracting;
>
> (f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;
>
> (g) Information arising out of a lawful personnel, physical, or communications security investigation;
>
> (h) Information acquired by overhead reconnaissance and not directed at specific United States persons;
>
> (i) Incidentally obtained information that may indicate involvement in activities that may violate Federal, state, local, or foreign laws; and
>
> (j) Information necessary for administrative purposes.

EO 12,333 § 2.3.

In addition, Section 2.3 provides that "elements of the Intelligence Community may disseminate information to each appropriate element within the Intelligence Community for purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it, except that information derived from signals intelligence may only be disseminated or made available to Intelligence Community elements in accordance with procedures established by the Director in coordination with the Secretary of Defense and approved by the Attorney General." *Id.*

United States."[358] This requirement is likely to be significant mainly with respect to data repositories that do not hold U.S. person data, because mixed repositories are likely already subject to the retention standards because of the difficulty of parsing information held within them.

- Dissemination: allow dissemination of personal information "only if the dissemination of comparable information concerning U.S. persons would be permitted under section 2.3."[359] Given the breadth of permitted dissemination under Section 2.3, this is not likely to be a major problem for the Intelligence Community.
- Data Security and Access: provide that "personal information shall be processed and stored under conditions that provide adequate protection and prevent access by unauthorized persons," and "limited to authorized personnel," who have received "appropriate and adequate training," and "with a need to know the information to perform their mission."[360] The U.S. Intelligence Community already tries to meet these standards for all of its Sigint, because the data is classified. It is interesting, and perhaps understandable in the wake of the unauthorized disclosures, that the PPD strongly endorses "need to know" principles, but there have been periods, after September 11, 2001, when "need to share" was the more dominant paradigm in certain areas,[361] and the nature of modern, classified intelligence networks, in which consumers pull information they need rather than having producers of intelligence push it to select recipients, may make old-fashioned "need to know" principles difficult to implement fully.
- Data Quality: provide that "personal information shall be included in intelligence products only as consistent with applicable IC standards for accuracy and objectivity."[362] Here, again, the Intelligence Community today tries to meet standards of accuracy and objectivity in all of its reporting.[363]

---

358. PPD-28, *supra* note 312, at 6 (Section 4(a)(i)).

359. *Id.* In addition, within 180 days, the DNI, in consultation with the Attorney General, must "prepare a report evaluating possible additional dissemination and retention safeguards for personal information collected through signals intelligence, consistent with technical capabilities and operational needs." *Id.* Obviously, the recommendations adopted from this report may or may not be significant.

360. *Id.* at 6 (Section 4(a)(ii).

361. *See, e.g.*, RICHARD A. BEST, JR., CONG. RESEARCH SERV., R41818, INTELLIGENCE INFORMATION: NEED-TO-KNOW VS. NEED-TO-SHARE (June 6, 2011) ("Unauthorized disclosures of classified intelligence are seen as doing significant damage to U.S. security. This is the case whether information is disclosed to a foreign government or published on the Internet. On the other hand, if intelligence is not made available to government officials who need it to do their jobs, enormous expenditures on collection, analysis, and dissemination are wasted. These conflicting concerns require careful and difficult balancing.").

362. PPD-28, *supra* note 312, at 7 (Section 4(a)(iii)).

363. *See, e.g.*, EO 12,333 ("Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is

- Oversight: "include appropriate measures to facilitate oversight over the implementation of safeguards protecting personal information, to include periodic auditing."[364] Oversight and auditing remain an integral part of current intelligence operations, as discussed above and in Chapter 13 of NSIP, so this directive does not require a major change from current practice.

* * *

The unauthorized disclosures that began in June 2013, and the government's reaction to them, provoked a very strong public reaction. Indeed, it may be that the recurring cycle of U.S. intelligence expansion and retrenchment is now entering a period of significant retrenchment, although future events could obviously alter the swing of the pendulum. As part of that process, the President and his closest advisors have taken several bold steps to re-calibrate significantly the balance between secrecy and transparency in favor of the latter; and they have also taken at least some steps to reduce the scope of signals intelligence. But the President's January 2014 speech and PPD-28 will be fully understandable only in hindsight. Years from now, they may be viewed as the first articulation of a new paradigm of transparency, privacy, and internationalism in U.S. intelligence. However, it is also possible that they will be viewed as a collection of fairly modest changes, largely cosmetic in nature, that were designed to placate critics in the United States and abroad. Either way, the result will be praised by some and condemned by others. As Justice Stewart explained in his concurring opinion in the Pentagon Papers case more than 40 years ago, national security policy demands "judgment and wisdom of a high order,"[365] and only time will tell whether we now possess those virtues in sufficient measure.

---

essential to the national security of the United States"); CIA, Directorate of Intelligence ("Members of the DI help provide timely, accurate, and objective all-source intelligence analysis on the full range of national security and foreign policy issues to the President, Cabinet, and senior policymakers in the US government."), *available at* https://www.cia.gov/offices-of-cia/intelligence-analysis/index.html.

364. PPD-28, *supra* note 312, at 7 (Section 4(a)(iv)). When a "significant compliance issue occurs involving personal information of any person, regardless of nationality," the policies and procedures must ensure that the DNI is promptly informed. *Id.*

365. New York Times v. U.S., 403 U.S. 713, 728-29 (1971) (Stewart, J., concurring) ("In the absence of the governmental checks and balances present in other areas of our national life, the only effective restraint upon executive policy and power in . . . national defense . . . may lie in an enlightened citizenry . . . . Yet it is elementary that the maintenance of an effective national defense requires both confidentiality and secrecy."). Justice Stewart wrote:

> I should suppose that moral, political, and practical considerations would dictate that a very first principle of that wisdom would be an insistence upon avoiding secrecy for its own sake. For when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion. I should suppose, in short, that the hallmark of a truly effective internal security system would be the maximum possible disclosure, recognizing that secrecy can best be preserved only when credibility is truly maintained.

Id.

***