LAWFARE RESEARCH PAPER SERIES

**VOL. 1** **SEPTEMBER 29, 2013** **NO. 4**

# 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 the tangible-things provision of FISA, 50 U.S.C. § 1861, which was added by Section 215 of the USA PATRIOT Act, to acquire telephony metadata in bulk. This paper discusses that use. Disclosure of the bulk metadata collection also contributed to a broader policy debate concerning the transparency of intelligence activities and the role of the FISA Court ("FISC"), among other issues. This paper also discusses those issues.*[1]

* General Counsel, Intellectual Ventures, and former Assistant Attorney General for National Security, U.S. Department of Justice, 2009 to 2011. While at the Justice Department, the author was responsible for supervising the enforcement of all federal criminal laws related to the national counterterrorism and counterespionage programs, and for providing legal oversight of intelligence activities conducted by executive branch agencies.

† This paper is adapted from a draft of the forthcoming 2014 supplement to David S. Kris & J. Douglas Wilson, National Security Investigations and Prosecutions, Chapter 19 (2d ed. 2012) [hereinafter Kris & Wilson, NSIP] available at http://legalsolutions.thomsonreuters.com/law-products/Treatises/National-Security-Investigations-and-Prosecutions-2012-ed/p/100026272 (reviewed on Lawfare on April 10, 2013 at http://www.lawfareblog.com/2013/04/national-security-investigations-prosecutions-2nd-ed-vols-1-2/). As such, it does not address certain basic aspects of Section 215 of the Patriot Act, which are dealt with in other parts of Chapter 19. Following an iterative process of prepublication review that occurred between July and September, 2013, this paper was cleared for publication by the Department of Justice.

[1] These broader issues relate to matters discussed in Kris & Wilson, NSIP Chapter 2 (which deals generally with oversight and regulation of the U.S. Intelligence Community), Chapter 5 (which deals with the FISC), and Chapter 13 (which deals with Congressional oversight of FISA and reporting), but are discussed in this paper because they are best understood in the context of concerns over the bulk metadata collection program.

## I. 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,[2] the authenticity of which the government later acknowledged.[3] The order, directed at a subsidiary of a 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."[4] The order excluded production of metadata concerning "communications wholly originating and terminating in foreign countries."[5]

The FISA Court's order described the metadata to be produced as including "comprehensive routing information, including but not limited to

---

[2] Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," The Guardian (June 5, 2013), available at www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order (hereinafter "215 Bulk Secondary Order").

[3] See, e.g., Testimony of James Cole, Deputy Attorney General, before the House Permanent Select Committee on Intelligence (June 18, 2013) ("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.") [hereinafter June 2013 Open HPSCI Hearing]. See also DNI Statement on Recent Unauthorized Disclosures of Classified Information (June 6, 2013) ("The judicial order that was disclosed in the press is used to support a sensitive intelligence collection operation") [hereinafter June 6, 2013 DNI Statement on Recent Unauthorized Disclosures], 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 Investigation for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-109 [hereinafter August 2013 FISC Opinion and August 2013 FISC Order], available at http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf.

[4] 215 Bulk Secondary Order at 2.

[5] 215 Bulk Secondary Order at 2; see Business Records FISA NSA Review at 15 (June 25, 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 at 10 n.10; 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").

session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile Station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call."[6] 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."[7] 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."[8]

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 had not been confirmed by the government.[9] In 2006, for example, USA Today published an article with the headline, "NSA Has Massive Database of Americans' Phone Calls."[10] 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-

---

[6] 215 Bulk Secondary Order at 2; see August 2013 FISC Opinion 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, e.g., Wikipedia, International Mobile Subscriber Identity, available at http://en.wikipedia.org/wiki/International_mobile_subscriber_identity. An IMEI number is a similar kind of number identified with the telephone itself. See, e.g., Wikipedia, International Mobile Station Equipment Identity, available at http://en.wikipedia.org/wiki/Imei.

[7] 215 Bulk Secondary Order at 2; see August 2013 FISC Opinion 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 Kris & Wilson, NSIP §§ 7:11, 18:2, 18:4.

[8] 215 Bulk Secondary Order at 2. For a discussion of non-disclosure requirements under the tangible-things provision, see Kris & Wilson, NSIP § 19:5.

[9] See, e.g., Hepting v. AT & T, 439 F. Supp. 974, 978 (ND Ca. 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.").

[10] Leslie Cauley, "NSA Has Massive Database of Americans' Phone Calls," USA Today (May 11, 2006), available at http://yahoo.usatoday.com/news/washington/2006-05-10-nsa_x.htm. 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.

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."[11] 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."[12] A 2006 article in the New Yorker magazine alleged more details on the collection,[13] as did a 2008 article in Newsweek.[14]

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).[15] According to the purported draft report, both

---

[11] Leslie Cauley, "NSA Has Massive Database of Americans' Phone Calls," USA Today (May 11, 2006), available at http://yahoo.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

[12] Leslie Cauley, "NSA Has Massive Database of Americans' Phone Calls," USA Today (May 11, 2006), available at http://yahoo.usatoday.com/news/washington/2006-05-10-nsa_x.htm. For an interesting discussion of the legality of the collection in 2007, see PBS Newshour, From The Archives: NSA Surveillance Seven Years Earlier (June 6, 2013), available at http://www.pbs.org/newshour/rundown/2013/06/from-the-archives-nsa-surveillance-seven-years-earlier.html.

[13] Seymour Hersh, Listening In, The New Yorker (May 29, 2006), available at http://www.newyorker.com/archive/2006/05/29/060529ta_talk_hersh.

[14] Daniel Klaidman, Now We Know What the Battle Was About, Newsweek (Dec. 12, 2008), available at 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."

[15] National Security Agency, Office of the Inspector General, Working Draft ST-09-0002 (Mar. 24. 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 also Charlie Savage, New Leak Suggests Ashcroft Confrontation Was Over N.S.A. Program, New York Times (June 27, 2013), available at http://www.nytimes.com/2013/06/28/us/nsa-report-says-internet-metadata-were-focus-of-visit-to-ashcroft.html?pagewanted=all&_r=0. 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 Kris & Wilson, NSIP, Chapters 15 and 16, and "Other Intelligence Activities," without specifying what those other activities involved. See Unclassified Report on the President's Surveillance Program at 6 (July 10, 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, in fact, available the

content and Internet and telephony metadata were collected outside the ambit of FISA beginning in October 2001, shortly after the September 11 attacks.[16] In March 2004, a disagreement between the White House and the Department of Justice, which has been recounted in vivid detail elsewhere,[17] apparently caused the President "to discontinue bulk collection of Internet metadata" under the PSP and seek authorization from the FISA Court,[18] but allowed the remaining elements of the program, including collection of content and telephony metadata, to continue without FISA Court authorization.[19] The court is said to have issued its first order authorizing bulk collection of internet metadata under FISA's pen-trap provisions in July 2004, which "essentially gave NSA the same authority to collect bulk Internet metadata that it had under the PSP," with a few additional limits.[20] However, collection of bulk telephony

---

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.

[16] NSA IG Working Draft Report 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. NSA IG Working Draft Report 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," NSA IG Working Draft at 30, but others did.

[17] See, e.g., Dan Eggen & Paul Kane, Gonzales Hospital Episode Detailed, Washington Post (May 16, 2007) (reporting on "vivid" Congressional testimony by James Comey), available at http://www.washingtonpost.com/wp-dyn/content/article/2007/05/15/AR2007051500864.html. See also Memorandum for the Attorney General (May 6, 2004), available at http://www.justice.gov/olc/docs/memo-president-surveillance-program.pdf [hereinafter May 2004 OLC PSP Opinion].

[18] NSA IG Working Draft 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. NSA IG Working Draft at 37.

[19] NSA IG Working Draft at 37. See also NSA IG Working Draft 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. NSA IG Working Draft at 38. For a discussion of a similar theory in a different context, see Kris & Wilson, NSIP § 7:9.

[20] NSA IG Working Draft 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." NSA IG Working Draft 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 whether the collection was interrupted or modified in any way thereafter. ODNI has confirmed, however, that the bulk pen-trap

metadata is described as having 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.[21] The FISC issued its first order authorizing bulk collection of telephony metadata under FISA's tangible-things provision in May 2006,[22] and continued to do so at 90-day intervals thereafter.[23]

## II. 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.[24] In

---

collection of internet metadata ended in 2011. See Charlie Savage, New Leak Suggests Ashcroft Confrontation Was Over N.S.A. Program, New York Times (June 27, 2013) (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"), available at http://www.nytimes.com/2013/06/28/us/nsa-report-says-internet-metadata-were-focus-of-visit-to-ashcroft.html?pagewanted=all&_r=0. At a July 17, 2013 hearing of the House Judiciary Committee, government witnesses confirmed the pen-trap bulk collection. See House Judiciary Committee, Oversight of the Administration's use of FISA Authorities, July 17, 2013 (video of the hearing is available at http://judiciary.house.gov/hearings/113th/hear_07172013.html).

[21] See NSA IG Working Draft 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 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").

[22] In re Application of the Federal Bureau of Investigation for an order Requiring the Production of Tangible Things from [Redacted], No. BR 06-05 (May 24, 2006) [hereinafter May 2006 Order], available at http://www.dni.gov/files/documents/section/pub_May%2024%202006%20Order%20from%20FISC.pdf.

[23] NSA IG Working Draft at 40; see August 2013 FISC Opinion and Order. As described in Kris & Wilson, NSIP §§ 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 at 38-39, and ultimately authorized by the Protect America Act of 2007 and the FISA Amendments Act of 2008.

[24] There were several disclosures made by the government through official channels. 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," [hereinafter June 6, 2013 ODNI Statement], 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.

2. On June 15, the government released to the news media a short background briefing paper on the recent disclosures, [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" [hereinafter June 2013 NSA Section 215 Factsheet], 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, Director of NSA, to Senators Wyden and Udall (June 25, 2013) [hereinafter June 25, 2013 Alexander Letter], 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. House Permanent Select Committee on Intelligence, How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries, June 18, 2013 [hereinafter June 2013 HPSCI Open Hearing] (video of the hearing is 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 entitled "NSA Surveillance Leaks: Facts and Fiction" [hereinafter June 2013 Newseum Program], available at http://www.odni.gov/index.php/newsroom/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 Senenbrenner to the Attorney General on June 6, 2013 [hereinafter July 16, 2013 Letter to Sensenbrenner]. See also Letter from DOJ 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. House Judiciary Committee, Oversight of the Administration's use of FISA Authorities, July 17, 2013 [hereinafter July 2013 HJC Hearing] (video of the hearing is available at http://judiciary.house.gov/hearings/113th/hear_07172013.html).

8. On July 19, 2013, Bob Litt, General Counsel of ODNI, gave a speech at the Brookings Institution, entitled, Privacy, Technology and National Security: An Overview of Intelligence Collection [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 [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. Senate Judiciary Committee, Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs [hereinafter July 2013 SJC Hearing], available at http://www.judiciary.senate.gov/hearings/testimony.cfm?id=0d93f03188977d0d41065d3fa041decd&wit_id=0d93f03188977d0d41065d3fa041decd-0-6.

September 2013, the FISA Court released an opinion and order (issued in August 2013) that re-authorized the bulk collection of telephony metadata and explained the court's reasoning.[25] 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;[26] the court also issued a "Primary Order" to the government,[27] setting out various requirements and limits on the collection and use of the telephony metadata.[28] The primary and secondary orders are issued by the FISC every 90 days,[29] and have been renewed consistently since May 2006—including after the unauthorized disclosures.[30] Altogether, as of July 2013, "the court [had]

---

11. Also on July 31, 2013, ODNI declassified various documents relating to the bulk metadata collection. See DNI Clapper Declassifies and Releases Telephone Metadata Collection Documents (July 31, 2013) [hereinafter 2009 Briefing Documents, 2011 Briefing Documents, and 215 Bulk Primary Order], 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.

12. On August 9, 2013, the government released an Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act [hereinafter White Paper], available at http://publicintelligence.net/doj-bulk-telephony-collection/.

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 http://icontherecord.tumblr.com/.

14. On September 17, 2013, the FISA Court released an opinion and order, dated August 29, 2013 reauthorizing the bulk metadata collection [hereinafter August 2013 FISC Opinion and August 2013 FISC Order], available at http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf.

[25] August 2013 FISC Opinion and August 2013 FISC Order.

[26] 215 Bulk Secondary Order at 1.

[27] See June 2013 HPSCI Open Hearing, 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, 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.

[28] See June 2013 HPSCI Open Hearing, 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 . . . .").

[29] June 2003 NSA Section 215 Backgrounder at 1; July 16, 2013 Letter to Sensenbrenner at 1.

[30] ODNI, 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-

authorized the program on 34 separate occasions by 14 different judges."[31] 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,[32] and in public remarks in July 2013, the General Counsel of the NSA referred to "three providers" possessing relevant metadata.[33]

2. The metadata collected does not, of course, include the contents[34] of any communication; nor does it include any subscriber's identity,[35] or data about a subscriber's physical location (other than the area code of a telephone number).[36] 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."[37]

---

foreign-intelligence-surveillance-court-renews-authority-to-collect-telephony-metadata; Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act (Aug. 9, 2013) at 1 [hereinafter White Paper], available at http://publicintelligence.net/doj-bulk-telephony-collection/; August 2013 FISC Opinion and Order.

[31] July 2013 SJC Hearing, Statement of Jim Cole; White Paper at 1.

[32] July 2013 Litt Speech at 11; see White Paper at 3 ("certain providers"), 13.

[33] Aspen Institute, Counterterrorism, National Security and the Rule of Law (July 18, 2013), statement of Raj De, video available at http://aspensecurityforum.org/2013-video (remark is at approximately 18:06 in video).

[34] August 2013 FISC Opinion at 2 n.2. For a discussion of the term "contents" as used in FISA and Title III, the federal wiretap statute, see Kris & Wilson, NSIP §§ 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 at 2.

[35] June 2013 HPSCI Open Hearing, 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 at 2 n.2.

[36] August 2013 FISC Opinion at 2 n.2, 4 n.5; June 6, 2013 ODNI Statement at 1; June 2013 NSA Section 215 Backgrounder 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, 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 at 4 n.5.

[37] June 2013 HPSCI Open Hearing, Statement of Chris Inglis; see June 2013 HPSCI Open Hearing, Statement of James Cole ("It is the number that was dialed from, the number

3. Once collected, the metadata is stored by NSA in restricted databases with limited access.[38]

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."[39] The queries may not relate to any other foreign intelligence purpose, such as counter-espionage.[40] The government submits and the FISA Court approves a specific list of terrorist groups or targets to which a query must relate.[41]

---

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").

[38] June 2013 IC Backgrounder at 2; June 2013 NSA Section 215 Backgrounder 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, 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 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 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 at 4-5 & nn.2-3.

[39] June 2013 IC Backgrounder at 1; see June 2013 HPSCI Open Hearing, Statement of Chris Inglis; July 17, 2013 HJC Hearing, Statement of James Cole; July 16, 2013 Letter to Sensenbrenner at 2; August 2013 FISC Order at 6-11.

[40] June 2013 HPSCI Open Hearing, Statement of Chris Inglis ("It cannot be used to do anything other than terrorism"); July 16, 2013 Letter to Sensenbrenner at 2; July 2013 Litt Speech 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 at 7-9.

[41] June 2003 NSA Section 215 Backgrounder 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, 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 at 2 ("the 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."); July 16, 2013 Letter to Sensenbrenner at 2 (RAS standard requires link to "a specific foreign terrorist organization that was previously identified to and approved by the court"); July 2013 Litt Speech at 14 ("the Government's applications to collect the telephony metadata have identified the particular terrorist entities that are the subject of the investigations").

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), and all queries appear to require approvals from at least two persons before being implemented; 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.[42] 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 other elements of the Executive Branch.[43] 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.[44] 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

---

[42] June 2003 NSA Section 215 Backgrounder at 1; June 2013 HPSCI Open Hearing, 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."), Statement of Chris Inglis ("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 at 7-10; White Paper 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 at 7.

[43] June 2013 NSA Section 215 Backgrounder 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, 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 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 at 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 at 7.

[44] 215 Bulk Primary Order at 10; August 2013 FISC Order 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 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 c, 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 at 9-10.

disseminated by NSA.[45] The Congressional Intelligence Committees also receive regular reporting.[46]

6. In 2012, "less than 300 unique identifiers met this [RAS] standard and were queried,"[47] although it is clear that at least some of the identifiers were used in multiple queries,[48] and that initial queries may produce two additional "hops"—i.e., numbers that are connected to numbers that are responsive to queries.[49] As the government explained, "Under the FISC's order, the NSA may also obtain information concerning second and third-tier contacts of the identifier (also referred to as 'hops'). The first 'hop' refers to the set of numbers directly in contact with the seed identifier. The second 'hop' refers to the set of numbers found to be in direct contact with the first 'hop' numbers, and the third 'hop' refers to the set of numbers found to be in direct contact with the second 'hop' numbers."[50] Some of the querying is automated and

---

[45] June 2013 NSA Section 215 Backgrounder at 1; June 2013 HPSCI Open Hearing, 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 at 16.

[46] See June 2013 NSA Section 215 Backgrounder at 2. For a discussion of Congressional oversight of FISA, see discussion in text, *infra*, and Kris & Wilson, NSIP § 13:1 et seq.

[47] June 2013 IC Backgrounder at 1; July 16, 2013 Letter to Sensenbrenner 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 Senate Judiciary Committee, Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs, 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 . . . .") available at http://www.judiciary.senate.gov/hearings/testimony.cfm?id=0d93f03188977d0d41065d3fa041decd&wit_id=0d93f03188977d0d41065d3fa041decd-0-6 [hereinafter July 2013 SJC Hearing].

[48] June 2013 HPSCI Open Hearing, Statement of Chris Inglis ("So only less than 300 numbers were actually approved for query against that database. Those might have been queried multiple times, and therefore, there might be some number greater than that of actual queries against the database.").

[49] July 17, 2013 HJC Hearing, 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, 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 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.").

[50] White Paper at 4.

some is manual.[51] In 2012, NSA "provided a total of 12 reports to FBI, which altogether 'tipped' less than 500 numbers" generated by the queries.[52]

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."[53] The government did not, of course, foreclose data mining, contact chaining,[54] or other analysis with respect to metadata responsive to queries,[55] or of metadata collected using methods or programs other than the FISC's bulk collection order under the FISA tangible things provision.[56] Moreover, NSA technicians may access the metadata to make the

[51] 215 Bulk Primary Order at 11.

[52] July 2013 SJC Hearing, Statement of Chris Inglis.

[53] June 2013 HPSCI Open Hearing, Statement of Keith Alexander; see August 2013 FISC Order 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 (Feb. 17, 2009) [hereinafter 08-13 US Memo], available at www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf.

[54] 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, November 20, 2007, at 2, 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 at 6.

[55] See August 2013 FISC Order at 11-13.

[56] 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 12333 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 at 15; August 2013 FISC Order 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

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.[57]

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.[58]

---

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 12333. 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 Kris & Wilson, NSIP § 16:5 & nn.14, 31, § 16:12 & nn.16, 18, § 16:17. For a discussion of DOD 5240-1.R, see Kris & Wilson, NSIP §§ 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 metadata associated with persons in the United States, contained in NSA's databases. Wainstein Contact Chaining Memo 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 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 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. See Wainstein Contact Chaining Memo 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 Kris & Wilson, NSIP § 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 at 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.

[57] See 215 Bulk Primary Order at 5-6; August 2013 FISC Order at 5-6.

[58] June 2013 NSA Section 215 Backgrounder at 1; June 2013 HPSCI Open Hearing, 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, Statement of Chris Inglis; 215 Bulk

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,[59] and is purged automatically from NSA's systems on a rolling basis.[60] 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.[61]

10. The bulk telephony metadata collection program has suffered a number of compliance issues,[62] and the FISA Court has been very concerned

---

Primary Order 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 Kris & Wilson, NSIP § 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 (June 22, 2009) (square bracketed material referring to NSA and ellipsis in original) [hereinafter "June 22, 2009 Order"], available at http://www.dni.gov/files/documents/section/pub_Jun%2022%202009%20Order.pdf.

[59] For a discussion of USSID-18, and the five-year retention period, see Kris & Wilson, NSIP §§ 2:7, 2:18.

[60] June 2013 NSA Section 215 Backgrounder at 2; June 2013 HPSCI Open Hearing, 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 at 14; August 2013 FISC Order at 14.

[61] June 2013 HPSCI Open Hearing, Statement of Chris Inglis.

[62] See June 2013 HPSCI Open Hearing, Statement of Bob Litt ("when compliance problems are identified . . . the vast majority of them are self-identified by NSA"), 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."), 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 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, Business Records FISA NSA Review at 3-6 (June 25, 2009) [hereinafter NSA End-to-End Review], available at http://www.dni.gov/files/documents/section/pub_NSA%20Business%20Records%20FISA%20Review%2020130909.pdf; (2) inadvertent manual queries of the metadata using 14 non-RAS approved selectors by 3 analysts over a period of approximately 11 weeks, NSA End-to-End Review at 6; (3) omitting the required review by NSA's Office of General Counsel of approximately 3,000 RAS determinations between 2006 and 2009, NSA End-to-End Review at 7; (4) failure to audit a database of query results, NSA End-to-End Review 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, NSA End-to-End Review 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, NSA End-to-End Review at 11-12; (7) sharing query results with the 98% of NSA analysts not authorized to access the metadata database, NSA End-to-End Review 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, NSA End-to-End Review at 15; cf. August 2013 FISC Order 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 at 15-16; (10) mistaken inclusion of unminimized query results in a database available to analysis from other U.S. intelligence agencies, NSA End-to-End Review at 16; (11) sharing of query results without the required approvals, NSA End-to-End Review 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 (Nov. 5, 2009) [hereinafter FISC Nov. 5, 2009 Supplemental Opinion and Order], 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

about the 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[63]: 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."[64]

## III. ANALYSIS

The bulk telephony metadata order from the FISC raises at least five legal 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 and finally, 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. *Relevance*

As explained in National Security Investigations and Prosecutions §§ 19:2-19:3, 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

---

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 at 5 n.8.

[63] June 2013 HPSCI Open Hearing, Statement of Keith Alexander ("I don't know of any inaccurate RAS numbers that have occurred since 2009").

[64] July 2013 DNI Response to 26 Senators 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." July 2013 DNI Response to 26 Senators at 3.

States person solely upon the basis of activities protected by the first amendment."[65] 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.[66] 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.[67]

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.[68] As discussed in National Security Investigations and Prosecutions § 2:18, 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

---

[65] 50 U.S.C. § 1861(a)(1).

[66] 50 U.S.C. § 1861(a)(2).

[67] 50 U.S.C. § 1861(c)(1), (c)(2)(D). As discussed in Kris & Wilson, NSIP § 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.

[68] As discussed in Kris & Wilson, NSIP § 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 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 (H.R. Conf. Rep. 109-333, 109th Cong., 1st Sess. at 90-91 (Dec. 8, 2005)):

> 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.

As discussed in the text, the FISC issued its first bulk telephony metadata collection order in May 2006, after this language was in effect.

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.[69]

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."[70] These investigations have an extremely wide aperture when it comes to the terrorist groups in question,

---

[69] DOG at 18. See also DOG 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 DIOG § 8, 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.

[70] July 2013 Litt Speech at 14; see June 2003 NSA Section 215 Backgrounder 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, 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 at 14 ("the Government's applications to collect the telephony metadata have identified the particular terrorist entities that are the subject of the investigations.").

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.[71]

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."[72] 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,"[73] and that bulk collection is necessary to find the relevant connections between terrorists.[74] "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."[75]

This reasoning, echoed by the government in its White Paper[76] and a letter to Congress,[77] is quite similar to arguments made in favor of relevance by

---

[71] See White Paper at 6-7 (noting that "there have been numerous FBI investigations in the last several years to which the telephony metadata records are relevant").

[72] August 2013 FISC Opinion at 18.

[73] August 2013 FISC Opinion at 19.

[74] August 2013 FISC Opinion at 19-22.

[75] August 2013 FISC Opinion at 22.

[76] See White Paper 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 at 3 n.4.

[77] 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 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

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."[78] As a former

---

retained by telecommunications service providers." July 16, 2013 Letter to Sensenbrenner at 2. 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." July 16, 2013 Letter to Sensenbrenner at 2; see July 2013 Litt Speech 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 at 2.

[78] Paul Rosenzwieg, Answering the 215 Relevance Question . . . And Tracking Paul Revere, Lawfare (June 12, 2013), available at 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 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

government official put it in testimony before the House Judiciary Committee in July 2013, "the telephone metadata is 'relevant' to counterterrorism investigations because the use of the database is essential to conduct the link analysis of terrorist phone numbers . . . and this type of analysis is a critical building block in these investigations. In order to 'connect the dots,' we need the broadest set of telephone metadata we can assemble, and that's what this program enables."[79]

---

> 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.

[79] Testimony of Stephen Bradbury before the House Judiciary Committee at 3 (July 17, 2013), available at http://judiciary.house.gov/hearings/113th/07172013/Bradbury%2007172013.pdf [hereinafter Bradbury HJC Testimony]. 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?" Ben Wittes, a Correction and a Reiteration, Lawfare (June 6, 2013), available at 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

As discussed in National Security Investigations and Prosecutions §§ 19:1 and 19:5, 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."[80] In the grand jury context, where the test governing a challenged 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,"[81] the results often depend on the facts, as illustrated by three cases discussed below.

In *In re Grand Jury Proceedings*,[82] 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."[83] 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

---

> 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 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?

[80] 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.

[81] 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 Kris & Wilson, NSIP § 22:1.

[82] 616 F.3d 1186 (10th Cir. 2010).

[83] 616 F.3d at 1202.

relevancy adopted" by the Supreme Court.[84] Although it appears to require an all-or-nothing approach with respect 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*.[85] 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.[86] 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.[87] 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."[88] 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.[89] 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

---

[84] 616 F.3d 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. 616 F.3d at 1191-92.

[85] 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.

[86] 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." 846 F. Supp. at 12.

[87] Id.

[88] Id.

[89] Id. at 13.

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*.[90] 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[91]:

> 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.[92]

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.[93] 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."[94]

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."[95] 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.[96]

---

[90] 827 F.2d 301 (8th Cir. 1987).

[91] Id. at 302.

[92] Id.

[93] Id.

[94] Id. at 305.

[95] Id.

[96] 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

In the context of administrative or civil subpoenas, which are expressly cross-referenced along with grand jury subpoenas in FISA's tangible things provision,[97] 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 metadata orders.[98] For example, in *Gonzales v. Google*,[99] in connection with a facial challenge to the Child Online Protection Act,[100] the Department of Justice issued a subpoena to Google "to compile and produce a massive amount of information,"[101] 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."[102] In *High Point SARL v. Sprint Nextel Corp*.,[103] 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."[104] 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

---

"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 HVJLT 543 (Spring 2011).

[97] 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").

[98] See July 2013 Litt Speech at 15 ("the 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.").

[99] 234 F.R.D. 674 (N.D. Ca. 2006).

[100] 47 U.S.C. § 231.

[101] 234 F.R.D. at 678.

[102] 234 F.R.D. at 682.

[103] Civil Action No. 09–2269–CM–DJW, 2011 WL 4526770 (D. Kan. Sept. 28, 2011).

[104] 2011 WL 4526770 at *12.

versus data), by geographic location, and by supplier or manufacturer of the Infrastructure Products."[105]

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 relevance?[106] 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 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."[107] 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.[108] On the other hand, as the government itself has

---

[105] 2011 WL 4526770 at *10.

[106] 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. 174(I) at 17-18, 109th Cong., 1st Sess. (July 18, 2005).

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

[108] See, e.g., June 2013 IC Backgrounder 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, and Declaration of

argued,[109] 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.[110] 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.[111] 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.[112]

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.[113] This raises a separate interpretive question about whether the singular can include the plural,[114] but with respect to the scope of the

---

Lieutenant General Keith B. Alexander, United States Army, Director of the National Security 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 [hereinafter FBI Value Affidavit, NSA Value Affidavit], 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 at 5-6.

[109] July 16, 2013 Letter to Sensenbrenner at 2.

[110] See June 2013 IC Backgrounder at 1.

[111] June 2013 HPSCI Hearing, 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 at 2.

[112] July 16, 2013 Letter to Sensenbrenner at 2; August 2013 FISC Opinion at 18-23; see also Bradbury HJC Testimony at 3 ("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.").

[113] See, e.g., August 2013 FISC Opinion at 5 (referring to "one of the identified international terrorist organizations").

[114] 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

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.[115] 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.

B. *Production to NSA*

FISA's tangible things provision is unusual in that it discriminates among federal agencies, referring specifically to the FBI rather than any other agency.[116] It authorizes certain FBI officials to make the necessary application,[117] and requires approval from a high-ranking FBI official if the tangible things sought are particularly sensitive (e.g., library patron lists).[118] 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,"[119] 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."[120] 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

---

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").

[115] June 2003 NSA Section 215 Backgrounder 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, 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]").

[116] This is not unprecedented—for example, national security letter statutes apply in various ways to various agencies, as discussed in Kris & Wilson, NSIP, Chapter 20—but most other provisions of FISA do not distinguish between agencies.

[117] 50 U.S.C. § 1861(a)(1).

[118] 50 U.S.C. § 1861(a)(3).

[119] 50 U.S.C. § 1861(g)(1).

[120] 50 U.S.C. § 1861(b)(2)(B).

States person."[121] 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."[122]

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.[123] But the order directs "the Custodian of Records [to] produce to the National Security Agency (NSA) . . . an electronic copy of the [specified] tangible things,"[124] and the nondisclosure directive refers to the fact "that the FBI or NSA has sought or obtained tangible things under this Order."[125] 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 National Security Investigations and Prosecutions § 9:3, in situations where one agency is providing technical assistance to another (e.g., decryption), and it is very likely 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.

C. *Timing*

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 available."[126] 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."[127] The FISC's conclusion, apparently accepted by the Custodian of Records, is that a rolling production ending on the last day of the period

---

[121] 50 U.S.C. § 1861(h).

[122] 50 U.S.C. § 1861(d)(1).

[123] 215 Bulk Secondary Order at 1; August 2013 FISC Opinion at 1; August 2013 Order at 1.

[124] 215 Bulk Secondary Order at 1-2.

[125] 215 Bulk Secondary Order at 2; see 215 Bulk Secondary Order at 3.

[126] 50 U.S.C. § 1861(c)(2)(B).

[127] 215 Bulk Secondary Order at 1-2; see August 2013 FISC Order at 3.

specified in the order is within the statutory language.[128] 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."[129] 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.[130] 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.

D. *Restrictions On Use and Dissemination*

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.[131] As explained in National Security Investigations and Prosecutions § 9:10, the tangible things provision requires the government to adopt minimization procedures governing retention and dissemination of information (there is no requirement for minimization at the acquisition stage of a tangible things collection, because the scope of the authorized acquisition is defined by the court's order itself).[132] 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,[133] but also because of how they reveal the FISA Court and

---

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

[129] John K. Villa, 2 Corporate Counsel Guidelines, § 5:17 (2012).

[130] See Chevron v. Salazar, 275 F.R.D. 437, 449 (SDNY 2011); U.S. v. IBM, 83 F.R.D. 92, 96 (SDNY 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.").

[131] See 215 Bulk Primary Order at 4-17.

[132] See 50 U.S.C. § 1861(g).

[133] See Kris & Wilson, NSIP §§ 19:13-19:15. With respect to the possible Fourth Amendment rights of telephone company customers, see Smith v. Maryland, 442 U.S. 735

the government working with what is sometimes referred to as "big data." As discussed in a 2009 essay,[134] "the overwhelming increase in the volume and

(1979) (no Fourth Amendment rights in telephone dialing information conveyed by the customer to the telephone company); United States v. Miller, 425 U.S. 435 (1976) (no Fourth Amendment rights of a customer in his bank records held by the bank); SEC v. O'Brien, 467 U.S. 735, 743 (1984) (rejecting constitutional challenges to enforcement of administrative subpoena: "It 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. Relying on that principle, the Court has held that a customer of a bank cannot challenge on Fourth Amendment grounds the admission into evidence in a criminal prosecution of financial records obtained by the Government from his bank pursuant to allegedly defective subpoenas, despite the fact that he was given no notice of the subpoenas") (citation omitted). 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). In its August 2013 opinion, the FISC concluded that there was no Fourth Amendment violation in the collection, and also noted that none of the providers had invoked the statutory procedure to challenge the orders in the FISC. August 2013 FISC Order at 6-9, 14-16.

Most claims to the contrary—that there is a constitutional violation—have relied on a combination of arguments that Smith v. Maryland is outdated and/or the logic of Justice Sotomayor's concurring opinion in U.S. v. Jones, 132 S. Ct. 945, 957 (2012) (citations omitted). 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." See, e.g., Laura K. Donohue, NSA surveillance may be legal — but it's unconstitutional, Washington Post (June 21, 2013), available at http://articles.washingtonpost.com/2013-06-21/opinions/40110321_1_electronic-surveillance-fisa-nsa-surveillance; Testimony of Jameel Jaffer and Laura W. Murphy, ACLU, before the Senate Judiciary Committee at 6-7 (July 31, 2013), available at https://www.aclu.org/files/assets/testimony.sjc_.073113.final_.pdf. As a matter of current constitutional law, those claims (however compelling as a policy matter) are probably best characterized as aspirational. 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, The Volokh Conspiracy (July 17, 2013), available at http://www.volokh.com/2013/07/17/metadata-the-nsa-and-the-fourth-amendment-a-constitutional-analysis-of-collecting-and-querying-call-records-databases/.

[134] See David Kris, Modernizing the Foreign Intelligence Surveillance Act: Progress to Date and Work Still to Come, in Ben Wittes ed., Legislating the War on Terror: An Agenda for Reform at 217 (Georgetown 2009) [hereinafter FISA Modernization Paper]. Mr. Kris is 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, Protecting America's Freedom in the Information Age (Oct. 2002), available at http://belfercenter.hks.harvard.edu/files/part_1.pdf. See also July 2013 Litt Speech at 6 ("So on the one hand there are vast amounts of data that contains intelligence needed to protect

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."[135] 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 compliance shortfalls.[136] It is only to say that, on average, big-data collection regimes will inherently pose greater compliance challenges than traditional collection regimes.

### E. *Applicability to Other Business Records*

Finally, 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. At a June 2013 hearing of the House Intelligence Committee,[137] a July 2013 hearing of the House Judiciary

---

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)).

[135] FISA Modernization Paper at 218.

[136] 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 Kris & Wilson, NSIP, Chapter 17. 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.

[137] June 2013 HPSCI Open Hearing. 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?

Committee,[138] and a July hearing of the Senate Judiciary Committee,[139] 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.[140] 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."[141] The government explained that the telephony metadata is "relevant" to FBI investigations in part because it involves communications, "in which connections between individual data points are important, and analysis of bulk metadata is the only practical means to find those otherwise invisible connections."[142] Additional insight into any other bulk metadata collection, perhaps not involving communications, will need to await further disclosures.

## IV. 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

---

> 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.

[138] July 2013 HJC Hearing, 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.").

[139] July 2013 SJC Hearing, Statement of Senator Leahy ("if our phone records are relevant, why wouldn't our credit card records [be relevant]?").

[140] July 2013 DNI Response to 26 Senators at 3.

[141] White Paper at 5 (italics in original).

[142] White Paper at 5.

in the current process for selecting FISA Court judges, under which the Chief Justice makes the appointments,[143] the vast majority of the Members of the FISC were appointed by Republican Presidents,[144] 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.

A. *Selection Method for Judges*

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.[145] In response, one commentator has observed, "the claim that Chief Justice Roberts's appointments have 'reshaped' the Court to favor the executive branch 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."[146] 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.

---

[143] For a discussion of the FISC, including the Chief Justice's authority to appoint judges to it, see Kris & Wilson, NSIP § 5:1 et seq. and especially § 5:3.

[144] For the current membership of the FISA Court, see Federation of American Scientists, https://www.fas.org/irp/agency/doj/fisa/court2013.html.

[145] See, e.g., Senator Richard Blumenthal, FISA Court Secrecy Must End, Politico (July 14, 2013) ("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."), available at http://www.politico.com/story/2013/07/fisa-court-process-must-be-unveiled-94127.html.

[146] Steven Aftergood, Did Justice Roberts Reshape the FISA Court, Secrecy News (July 29, 2013), available at http://blogs.fas.org/secrecy/2013/07/roberts-reshape/. See also Editorial, More Independence for the FISA Court, New York Times (July 28, 2013) ("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."), available at http://www.nytimes.com/2013/07/29/opinion/more-independence-for-the-fisa-court.html?ref=surveillanceofcitizensbygovernment&_r=0. 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. July 2013 Walton-Leahy Letter at 2 n.2, 3 n.6 ("the approval rate for Title III wiretap applications . . . . is higher than the approval rate for FISA applications"). Chief Justice Roberts was confirmed in September 2005, and the FISA Court approved the bulk telephony metadata collection in May 2006.

More broadly, it is important to consider the context in which the FISA Court initially approved the bulk collection. Unverified media reports (discussed above) state that bulk telephony metadata collection was occurring before May 2006; even if that is not the case, perhaps such collection could have occurred at that time based on voluntary cooperation from the telecommunications providers. If so, 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.[147]

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 there are fewer FISC judges (11) than regional courts of appeals (13).[148] That is effectively how the selection process apparently worked, informally, at least some of the time in the past.[149]

### B. Inter Partes *Litigation*

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. All of the plausible 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.[150]

---

[147] 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).

[148] 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 Kris & Wilson, NSIP § 5:3.

[149] 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.

[150] 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.

First, the FISC could call on external lawyers, in private practice, on a case-by-case basis as desired in the court's discretion.[151] 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."[152] 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 quite challenging, especially in the FISC as opposed to the Court of Review. At the outset, it might require a more robust form of adversary system than is commonly understood. One of the main challenges in some cases before the FISC is the intersection of complex law and complex facts, particularly concerning rapidly evolving technology, as Rule 11 itself recognizes.[153] 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. 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

---

[151] 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, but legislation could remove doubt and reinforce the validity of the practice.

[152] For a discussion of Rule 11(b), see Kris & Wilson, NSIP § 5:3. 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 at 2 n.2, 4 n.5.

[153] 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 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.

writing and storing highly classified pleadings. All of these issues could be addressed, perhaps, but the process may be more involved, cumbersome, logistically challenging, and perhaps slower than is commonly understood.[154] If it were used very rarely, and when time is not of the essence, it might be made to work, but it would not be a trivial undertaking.

Another option would be to use full-time, executive branch personnel to present the opposing arguments, such as staff in the National Security Division's Oversight Section. This has the virtue of using lawyers with ongoing 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.[155] 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."[156] 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 National Security Investigations and Prosecutions § 5:3, 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.[157] If

---

[154] See July 2013 SJC Hearing, Statement of Bob Litt ("if 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), available at http://www.lawfareblog.com/2013/07/making-fisc-more-adversarial-a-brief-response-to-orin-kerr/.

[155] Orin Kerr, A Proposal to Reform FISA Court Decisionmaking, The Volokh Conspiracy (July 8, 2013), available at http://www.volokh.com/2013/07/08/a-proposal-to-reform-fisa-court-decisionmaking/.

[156] Steve Vladeck, Making FISC More Adversarial: A Brief Response to Orin Kerr, Lawfare (July 8, 2013), available at http://www.lawfareblog.com/2013/07/making-fisc-more-adversarial-a-brief-response-to-orin-kerr/

[157] 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

desired, Congress could expand the cadre of Legal Advisors,[158] 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);[159] it would also avoid the cultural and other 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,[160] and the institutional and long-term

---

additional information, or by submitting a final application." Letter from Judge Reggie Walton to Senator Patrick Leahy (July 29, 2013) [hereinafter July 2013 Walton-Leahy Letter], available at http://www.leahy.senate.gov/download/honorable-patrick-j-leahy.

[158] 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).

[159] See July 2013 SJC Hearing, Statement of Chris Inglis ("We welcome any and all hard questions"); July 2013 Walton-Leahy Letter 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 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.").

[160] 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*

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.[161] Creating a full-blown *inter partes* system in the FISC for a few key cases might have some benefits, as discussed above, but could also result in the erosion of something that has proven valuable over time.[162] 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.[163] Unlike FPD attorneys, however, the ODCL lawyers would likely not be busy defending civil liberties all of the time, because (as noted above) the FISC is likely to need their services only very rarely. 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

---

*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."

[161] See Kris & Wilson, NSIP § 11:5 & n.21; see also, e.g., 148 Cong. Rec. S8649-01 (reprinting article from 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).

[162] 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, 475-76 (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.").

[163] See 18 U.S.C. § 3006A(g)(2)(A).

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.[164] 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.[165]

## V. SECRECY AND TRANSPARENCY

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.[166] As to the first part of this issue, the historical record shows reasonably clearly 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

---

[164] Judge James G. Carr, A Better Secret Court, New York Times (July 22, 2013), available at http://www.nytimes.com/2013/07/23/opinion/a-better-secret-court.html?ref=foreignintelligencesurveillanceactfisa.

[165] 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.

[166] 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 at 3 (July 12, 2013) ("the 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 http://www.justice.gov/iso/opa/resources/2202013712162851796893.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.

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.

A. *Intrafederal Information Sharing*

The standards governing information-sharing between the Executive Branch and Congress in this area are clear, as discussed in Chapter 13 of National Security Investigations and Prosecutions. 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.[167] 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."[168] 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 Court or Foreign Intelligence

[167] 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).

[168] 50 U.S.C. § 1862(a).

> Surveillance Court of Review that include significant construction or interpretation of the provisions of this chapter.[169]

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 National Security Investigations and Prosecutions §§ 2:6-2:7. 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.[170]

1. *Disclosure to Intelligence and Judiciary Committees*. — 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."[171] 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

---

[169] 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. 3, 112th Cong., 1st Sess. 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." SSCI March 2011 Activities Report at 31.

[170] See L. Elaine Halcin and Frederick M Kaiser, Congressional Oversight of Intelligence: Current Structure and Alternatives, CRS (March 14, 2012), available at http://assets.opencrs.com/rpts/RL32525_20120314.pdf [hereinafter 2012 CRS Oversight Report].

[171] Dan Roberts and Spencer Ackerman, "Senator Feinstein: NSA phone call data collection in place 'since 2006,'" The Guardian (June 6, 2013) (emphasis added), available at http://www.guardian.co.uk/world/2013/jun/06/court-order-verizon-call-data-dianne-feinstein.

information has been made available to all members of Congress prior to each congressional reauthorization of this law."[172]

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.[173]

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."[174] It also

---

[172] Press Release of Intelligence Committee, "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." Charlie Savage, Edward Wyatt and Peter Baker, "U.S. Confirms that it Gathers Online Data Overseas," New York Times (June 6, 2013), available at www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html?pagewanted=all&_r=0.

[173] 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).

[174] S. Rep. No. 174, 112th Cong., 2d Sess. at 7 (June 7, 2012) (additional views of Senator Feinstein) [hereinafter SSCI June 7, 2012 Report].

reprinted without rebuttal the government's statement that it had complied with the obligation to produce the interpretive documents.[175]

The Department of Justice wrote a letter to Congress in July 2013 confirming that "[t]he classified details of the program have been briefed to the Judiciary and Intelligence Committees on many occasions."[176] 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."[177] 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.[178]

Representative Lamar Smith, then Chairman of the House Judiciary Committee, stated in May 2011:

> 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

---

[175] SSCI June 7, 2012 Report 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.").

[176] July 16, 2013 Letter to Sensenbrenner at 3.

[177] July 2013 DNI Response to 26 Senators at 1.

[178] White Paper at 18 (emphasis added).

> legitimate national security investigation. [This provision has] been effectively used for the last 10 years without any evidence of misuse or abuse."[179]

Although at least one Member of the House Judiciary Committee publicly stated that he intentionally eschews classified briefings—on the ground that they are a "rope-a-dope operation"[180]—none appears to have denied the fact that briefings occurred for, or that the relevant interpretive documents were delivered to, the Judiciary Committees. 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.[181] 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."[182]

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."[183]

---

[179] 157 Cong. Rec. H3738, May 26, 2011 (emphasis added).

[180] Representative 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." Peter Wallsten, Lawmakers Say Administration's Lack of Candor on Surveillance Weakens Oversight, Washington Post, available at 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. Representative Sensenbrenner did not explain how or why he expected to receive a classified briefing and also be authorized to discuss that briefing publicly.

[181] July 2013 HJC Hearing, Statement of Bob Litt.

[182] July 2013 HJC Hearing, Statement of Chris Inglis.

[183] 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

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."[184]

2. *Disclosure to Members of Congress*. — 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.[185] 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."[186]

---

http://icontherecord.tumblr.com/. For a summary of the nature of the compliance incidents, see note 62.

[184] The Senate Judiciary Committee's reports on S. 1692, the USA Patriot Act Sunset Extension Act of 2009, S. Rep. No. 92, 111th Cong., 1st Sess. at 7 (Oct. 28, 2009), and S. 193, the USA Patriot Act Sunset Extension Act of 2011, S. Rep. No. 13, 112th Cong., 1st Sess. 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 (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).

[185] 2011 Briefing Documents, Cover Letter at 1.

[186] Id. at 2.

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."[187] 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."[188] 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."[189]

The availability of the classified briefings and documents was well publicized within Congress. Senators Feinstein and Chambliss wrote two "Dear Colleague" letters, in 2010 and 2011, inviting all Members of Congress to classified briefings on the bulk collection,[190] 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

[187] Id. at 3.

[188] 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.

[189] Id. at 4.

[190] 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.

> 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.[191]

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.[192]

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 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."[193] 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.[194]

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

---

[191] 157 Cong. Rec. S3210-02, May 23, 2011 (emphasis added).

[192] 156 Cong. Rec. H838, Feb. 25, 2010 (emphasis added).

[193] 156 Cong. Rec. S2108, Mar. 25, 2010.

[194] Id.

> 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.[195]

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.[196]

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.[197] 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)

---

[195] SSCI March 2011 Activities Report at 31 (emphasis added).

[196] The letter is reprinted in S. Rep. No. 13, 112th Cong., 1st Sess. 119-120 (Apr. 5, 2011) (emphasis added).

[197] See Josh Gerstein, Official: 13 Briefings for Hill on Call-Tracking Provision, Politico (June 8, 2013), available at 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 at 3-4.

• 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 available to all Members."[198] 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."[199]

---

[198] July 2013 DNI Response to 26 Senators at 1.

[199] Id. See also White Paper 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 at 18 n.13. 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, August 4, 2013, available at http://www.theguardian.com/commentisfree/2013/aug/04/congress-nsa-denied-access. 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

Many Members of Congress[200] acknowledged having been briefed, or at least having had the opportunity to be briefed, on the bulk collection

---

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.

[200] One notable example of a Member of Congress who denied knowledge of the bulk collection was Congressman James 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 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.

program.[201] For example, the Senate Majority Leader, Harry Reid, said: "For senators to complain that 'I didn't know this was happening,' we've had many, many meetings that have been both classified and unclassified that members have been invited to. . . . If they don't come and take advantage of this, I can't say enough to say they shouldn't come and say 'I wasn't aware of this,' because they've had every opportunity to be aware of these programs."[202] Senator Leahy acknowledged receiving classified briefings.[203] 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."[204]

---

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, Lawfare, "Sensenbrenner on DOJ Testimony Regarding 215" (June 7, 2013), available at http://www.lawfareblog.com/2013/06/sensenbrenner-on-doj-testimony-regarding-section-215/; Adam Serwer, MSNBC, Patriot Act Architect Cries Foul on NSA Program, but Skipped Briefings (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 last three years."), available at http://tv.msnbc.com/2013/06/14/sensenbrenner-furious-that-he-wasnt-briefed-on-nsa-programs-skipped-the-briefings/.

[201] 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").

[202] Video of Senator Reid is available at http://www.huffingtonpost.com/2013/06/11/harry-reid-nsa_n_3423393.html.

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

[204] The letter, dated March 15, 2012, is 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." Wyden-Udall Letter of March 15, 2012 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, New

York Times (Sept. 21, 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 of September 21, 2011, from Senators Wyden and Udall to Attorney General Holder, 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. 13, 112th Cong., 1st Sess. at 34; see also pages 37, 43, 45 (Apr. 5, 2011); see also S. Rep. No. 86, 109th Cong. 1st Sess. 19 (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. This authority is similar to the widely-used grand jury subpoena authority in criminal investigations." H.R. Rep. No. 79(I), 112th Cong., 1st Sess. at 2 (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.

Such a highly classified briefing for all Members of Congress, rather than just for those serving on the Intelligence Committees (and perhaps also the

---

• 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 (157 Cong. Rec. H731, February 14, 2011): "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." See also 157 Cong. Rec. H621, February 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, 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 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.

Although the Wyden-Udall letter did not identify any DOJ officials by name, Mr. Kris was one of several over the years since 2006 who referred to grand juries in describing the tangible things provision. He 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." This testimony is 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, Washington Post, available at 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.

Judiciary Committees), is very unusual.[205] 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.[206] 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."[207]

The briefings and other historical evidence raise the question whether Congress'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,"[208] 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,[209] or forbidding bulk collection under the tangible things provision.[210] A one-sentence bill to forbid bulk collection of telephony

---

[205] For a more complete discussion of Congressional oversight of national security matters, see Kris & Wilson, NSIP § 13:1 et seq.

[206] 2011 Briefing Documents, Cover Letter at 1.

[207] Senator Dianne Feinstein, Make NSA Programs More Transparent, Washington Post (July 31, 2013), available at http://www.washingtonpost.com/opinions/senate-intelligence-committee-chair-reform-nsa-programs/2013/07/30/9b66d9f2-f93a-11e2-8e84-c56731a202fb_story.html.

[208] Lorillard v. Pons, 434 U.S. 575, 580 (1978); see also Keene Corp. v. United States, 508 U.S. 200, 212–213 (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.").

[209] 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, 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.").

[210] 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

metadata narrowly failed to pass the House of Representatives in July 2013.[211] (For the 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, 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.[212] Here, post-disclosure briefings, conducted in July 2013, also drew

---

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 and Tube Co. v. Sawyer, 343 U.S. 579 (1952), see Kris & Wilson, NSIP § 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.

[211] See 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 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).

[212] 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.

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."[213] 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 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.[214]

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,"[215] and was sufficiently aware of the FISC's interpretation of the statute to satisfy the legal requirements for ratification through reenactment.

### B. *Information Sharing with the Public*

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

---

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)).

[213] 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'"), available at http://thehill.com/homenews/senate/305765-senators-skip-classified-briefing-on-nsa-snooping-to-catch-flights-home.

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

[215] August 2013 FISC Order 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.

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.[216] 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.[217]

1. 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 one, and in respect of classified matters, the Intelligence Committees "serve as the proxy for the American people."[218] 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."[219]

---

[216] As explained in Kris & Wilson, NSIP, Chapter 15, 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.

[217] July 2013 HJC Hearing, Statement of Bob Litt.

[218] Congressional Oversight of Intelligence Activities, S. Hrg. No. 794, 110th Cong., 1st Sess. 11 (Nov. 13, 2007) (statement of Lee Hamilton), available at http://www.intelligence.senate.gov/pdfs/110794.pdf.

[219] 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), available at 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

To be sure, as this paper and National Security Investigations and Prosecutions 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.[220] But there are obviously many other situations in which, despite such efforts, no solution emerges. As explained in the Foreword to the First Edition of NSIP, that treatise "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[221] 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.[222] The statute defines covert action to exclude "traditional" military and law-enforcement activities,[223] provides that a covert action finding "may not authorize any action that would violate the Constitution or any statute of the United States,"[224] and specifically warns that "No covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or media."[225] 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

---

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, video available at http://aspensecurityforum.org/2013-video (remark is at approximately 1:05:32 in 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."

[220] See 28 C.F.R. § 17.18. The prolonged, intense prepublication review process for the first edition of the book from which this paper is excerpted can be found in Kris & Wilson, NSIP, Preface and Foreword.

[221] 50 U.S.C. § 413b.

[222] See generally Alfred Cumming and Richard A. Best, Jr., Sensitive Covert Action Notifications: Oversight Options for Congress, CRS (Jan. 10, 2006).

[223] 50 U.S.C. § 413b(e)(2).

[224] 50 U.S.C. § 413b(a)(5).

[225] 50 U.S.C. § 413b(f).

interpretive questions, some of which might affect many Americans.[226] Yet it might be impossible, in many cases, to explain those interpretations without revealing the most sensitive classified information.[227]

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."[228] 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 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

---

[226] 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.

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

[228] Senators Wyden and Udall, along with Senators Feinstein and Merkley, sent a letter to the FISA Court in February 2013 (available at http://www.fas.org/irp/agency/doj/fisa/fisc-021313.pdf), 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." In a letter dated March 27, 2013 (available at http://www.fas.org/irp/agency/doj/fisa/fisc-032713.pdf), 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."

think the law allows and what the government secretly claims the law allows."[229] 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."[230] 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.

2. 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,[231] 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 details of intelligence activity.

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.[232] Those reports, which were very well done and extremely

---

[229] Wyden-Udall Letter of March 15, 2012 at 2.

[230] 157 Cong. Rec. S3372 (May 26, 2011).

[231] See David Kris, Thoughts on a Blue Sky Overhaul of Surveillance Laws, Lawfare, May 18-21, 2013, available at http://www.lawfareblog.com/author/dkris/.

[232] See 50 U.S.C. § 1808(b).

informative, are cited throughout National Security Investigations and Prosecutions. 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.

Third and finally, we could significantly re-calibrate the balance between secrecy and transparency, revealing significantly more information publicly. In June 2013, President Obama stated through a spokesperson that he "welcomes the discussion of the trade-off between security and civil liberties,"[233] and that he "look[s] forward to continuing to discuss these critical issues with the American people" as well as with Congress.[234] At a press conference held on August 9, 2013, the President stated:

> [W]e 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

---

[233] 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.

[234] 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.

> 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.[235]

In keeping with the President's direction, the Intelligence Community has released many new details about the bulk telephony metadata collection program, as described above. In addition, as also noted above, the FISC itself has released significant new information.

The key remaining question is whether there will be additional, authorized releases concerning intelligence activity that has not been subject to prior, unauthorized releases.[236] A program of increased disclosure, designed only to correct misimpressions based on prior leaks, differs from a broad embrace of transparency even in the absence of such leaks.[237] On the other hand, if the leaks themselves are (or will be) very broad, the difference between the two approaches may shrink.

As of this writing, it is not clear whether the Obama Administration intends to pursue a narrow or broad re-calibration. In public, at least, it has not clearly described the philosophical approach underlying the 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.[238] To some observers, however, we seem to be on course for an

---

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

[236] 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 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 isclosures." July 2013 Litt Speech 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."

[237] 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." 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 "[o]nce 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." August 2013 Remarks by the President.

[238] 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/.

environment in which the basic existence of all (or most) signals intelligence programs is publicly disclosed, with information about particular participants in those programs (e.g., providers and targets) still secret. That would be a very significant re-calibration. Whether and to what extent the transparency would extend still further, to other intelligence programs—e.g., those involving Humint or covert action—also remains to be seen.

The effects of a broad re-calibration could be felt in at least two ways. 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.[239] 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 between increased transparency and the scope of intelligence activity. Intelligence activity that helps the U.S. government when done covertly may harm it when done overtly. For example, clandestine surveillance of foreign government officials may aid U.S. foreign policy—e.g., by giving U.S. treaty negotiators insight into their foreign counterparts' instructions. As such, foreign policy makers may support and even require such surveillance from the Intelligence Community. On the other hand, however, transparent surveillance of foreign government officials may have precisely the opposite effect, creating challenges that cause policy makers to require less surveillance. If less surveillance leads to a perceived intelligence failure, of course, resulting demands to expand surveillance may cause the pendulum to swing back.[240]

---

[239] See 5 U.S.C. § 552; U.S. v. Reynolds, 345 U.S. 1 (1953).

[240] 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. Imagine that journalists construed every fact they learned in light of the need to keep feeding at the trough of a source who had

These are probably the most significant long-term questions resulting from the June 2013 disclosures: how will the United States re-calibrate the tension between secrecy and transparency, and what will follow from that re-calibration?[241] As Justice Stewart explained in his concurring opinion in the Pentagon Papers case, the resolution of that tension requires "judgment and

---

> 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.

Ben 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/.

[241] The other most significant long-term question is how the government will deal with the challenge and opportunity of "big data," as discussed in the text with respect to minimization.

wisdom of a high order." His observations more than 40 years ago seem relevant today:[242]

> 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.[243]

As a democracy that runs on informed public debate but also engages in classified intelligence activity, America has struggled with the proper balance between secrecy and transparency. Recent disclosures have brought that struggle into much sharper relief, and have called into question the balance struck and maintained since the 1970s. It remains to be seen whether those disclosures will yield substantial, enduring change.

---

[242] 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.").

[243] New York Times v. U.S., 403 U.S. 713, 729 (1971) (Stewart, J., concurring). The June 2013 disclosures raise several other issues. Within the Executive Branch, they may call into question the balance between the principles of "need to know" and "need to share" information, because one person apparently was able to access and exfiltrate a vast number of highly classified documents. Moreover, the disclosures seem to have affected relationships between the government and the electronic communications providers. As discussed in Kris & Wilson, NSIP § 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." http://apps.americanbar.org/abanet/media/release/newsrelease.cfm?releaseid=264 (last viewed June 12, 2011).