American University National Security Law Brief

Volume 5 | Issue 1 Article 3

2014

Dr. FISA or: How I Learned to Stop Worrying and Trust the NSA

Emmanuel Klint-Gassner

DR. FISA OR: HOW I LEARNED TO STOP WORRYING AND TRUST THE NSA

EMMANUEL KLINT-GASSNER

I. INTRODUCTION

In June 2013, Edward Snowden, a former contractor with the National Security Agency (NSA), leaked information about the NSA's information collection programs.[1] Edward Snowden worked with the *Guardian* newspaper to leak more classified documents and information over the next few months.[2] The first of these leaks involved the NSA's collection program on domestic telecommunications metadata. Then came leaks about Internet metadata being collected as well. Newspapers around the world inflated articles about how the United States was "spying" on its own citizens. More leaks followed, detailing U.S. spying activities on Chinese computers, and throughout Europe.[3] Edward Snowden claimed he was a whistle blower, and that he leaked the confidential documents because he felt that the United States' collection programs were morally wrong, and that they should not be kept from the general public.[4] Whether Edward Snowden is a whistle blower or a traitor is beyond the scope of this paper. However, Mr. Snowden's disclosures did more than just put smiles on our enemies' faces, it spurred a huge debate about surveillance, the Foreign Intelligence Surveillance Act (FISA), the NSA, technology, and how all these elements are combined and used by the government.

This paper will focus on scratching the itch. The annoying itch that Americans got when Edward Snowden told them that the Government was watching. The itch that makes one wonder if George Orwell's Big Brother[5] is in fact the United States Government — they might even be watching you right now. The fact that the government has the technology, ability, and authority to collect massive amounts of information on "everyday" private citizens makes Americans uncomfortable — like an itch that we just can't scratch.

This is not the first time that Americans have had to deal with uncomfortable news from our government. During the Cold War, Americans were dealing with the idea of nuclear bombs destroying the world. Popular culture, with everyone from novelists to Hollywood, came up with

1 Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN, June 6, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

2 Glenn Greenwald, *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, GUARDIAN, June 9, 2013, http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

3 Scott Shane & Ravi Somaiya, *New Leak Indicates Britain and US Tracked Diplomats*, N.Y. TIMES, June 16, 2013, http://www.nytimes.com/2013/06/17/world/europe/new-leak-indicates-us-and-britain-eavesdropped-at-09-world-conferences.html.

4 Laura Poitras & Glenn Greenwald, *NSA Whistleblower Edward Snowden: I Don't Want to Live in a Society that Does These Sort of Things*, GUARDIAN, June 9, 2013, http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video.

5 George Orwell, *1984* (1949).

fictional cures for the atomic dilemma.[6] This is exemplified by Stanley Kubrick's suggestion that we should "learn to live with (love) the bomb."[7] After 9/11 Americans are no longer (as) worried about superpowers and their nuclear weapons; the idea of terrorist groups, not states, rule the fears of everyday Americans. The fact that nineteen terrorists could cause the death of 3,000 Americans on American soil was a shock. Terrorists are different than America's previous enemies. They are not necessarily state actors, they are spread out across the world, they use technology just like we do, and their goal is non corporeal.[8] Terrorists have different motivations, different goals, and different means of attack, which is what makes them so frightening. After 9/11, President Bush announced that America would fight back with the War on Terror. Learning to live with the open-ended war on terror means learning to live with intelligence, technology, surveillance—the itch.[9]

This paper will focus on how Americans can learn to live with, though probably not love, the technology and procedures that were recently disclosed by Edward Snowden. In other words, to soothe the itch just a little bit, by learning about the details of bulk metadata collection and how the government uses it. It should be noted that the practices and policies that have been disclosed are not perfect, there is always room for improvement, and this paper is not positing that there are not issues of concern that should be addressed.

This paper will first discuss what metadata actually is, how the NSA uses the bulk metadata, how the information is retained, queried, and why it is used. Then this paper will go into a brief history of electronic surveillance and FISA. Finally, this paper will discuss the interaction between the Fourth Amendment and metadata collections and the arguments surrounding the constitutionality of bulk metadata collection.

II. "NSA Collecting Phone Records of Millions of Verizon Customers Daily"[10]

The 2013 *Guardian* article was not the first time allegations about the Government listening to Americans' phone calls had appeared in the media.[11] In 2005, the New York Times ran an article about how the Bush administration was listening to calls without judicial warrants.[12] However, the 2005 articles did not elicit any acknowledgement from the government. At the time few details about the programs were known and so the article simply referred to the NSA as "eavesdropping" on Americans' calls.[13]

---

6 Wesley Wark, *Introduction: Learning to Live with Intelligence*, 18 Intelligence and National Security, no. 4, 2008, at 1, 1-14.

7 Dr. Strangelove or: How I Learned to Stop Worrying and Love the Bomb (Colombia Pictures 1963).

8 *See* Wark, *supra* note 6, at 1-14.

9 *See id.*

10 *See* Greenwald, *supra* note 1.

11 David Kris, *On the Bulk Collection of Tangible Things*, Lawfare Research Paper Series, Sept. 29, 2013.

12 James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times, Dec. 16, 2005, http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&module=Search&mabReward=relbias%3As%2C%7B%222%22%3A%22RI%3A14%22%7D&_r=0.

13 *Id.*; *see* Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA Today, May 11, 2006, http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm (explaining that the 2005 disclosure was the also the subject of litigation); *see e.g.*, Hepting v. AT &T, 439 F. Supp. 974, 978 (2006) ("Plaintiffs allege that AT& T Corporation

The 2013 Snowden leaks disclosed details of programs where the NSA was not eavesdropping on calls but simply collecting metadata.[14] But what is metadata? Put simply metadata is "information about information."[15] The FISA Court order allowing the collection of metadata included "comprehensive routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile Station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call."[16] The order also stated that the metadata 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."[17] While the contents of messages are not being recorded, some scholars argue that the cumulative information of the metadata discloses substantive facts about a person and therefore is a violation of the Fourth Amendment.[18]

Because of the sensation around the Edward Snowden leaks, the government declassified documents and published legal reasoning behind the bulk metadata collection. These disclosures revealed many things about the NSA programs and the FISA court. These disclosures reveal that while there is the necessary element of secrecy surrounding the NSA collections procedures they are not without oversight, which should alleviate some of the public's fear about the bulk metadata collections.

I. The Foreign Intelligence Surveillance Court (FISC) Orders

First, some of the important documents released were FISC "Primary Order"[19] which was directed to the government, and the "Secondary Order" which was directed at a telecommunications

. . . are collaborating with the NSA in a massive warrantless surveillance program that illegally tracks the domestic and foreign communications and communication records of millions of Americans.").

14 *See* Risen & Lichtblau, *supra* note 12.

15 Bryce Clayton Newell, *The Massive Metadata Machine: Liberty, Power, and Secret Mass Surveillance in the US and Europe*, 10 ISJLP (forthcoming 2014).

16 *In Re* Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Bus. Network Servs., Inc., on Behalf of MCI Commc'n Servs., Inc. d/b/a/ Verizon Bus. Servs., No. BR 13-80 (FISA Ct. 2013) at 2 [hereinafter "215 Bulk Secondary Order"]; *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 (FISA Ct. 2013) at 2 n. 2 [hereinafter "August 2013 FISC Opinion"] (explaining that an IMSI number is usually a 15 digit number that identifies the telephone used in the mobile telephone network, and it is usually associated with the telephone's subscriber identity module (SIM) card that authenticates the telephone to the network. An IMEI number on the other hand is similar but it is identified with the telephone itself); *see* Newell, *supra* note 15, at 8.

17 *See* 50 U.S.C.A. §1801(n) (stating that FISA defines "contents" as "any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication." This differs from §2510(8) because it includes information concerning the existence of a communication and the identity of the parties to it); *see* 215 Bulk Secondary Order, *supra* note 16, at 2; *see* August 2013 FISC Opinion, *supra* note 16, at 2 n. 2 (noting that Under 18 U.S.C. § 2510 (8) "content" is defined to include "any information concerning the substance, purport, or meaning of that communication"); *see also*, David S. Kris & J. Douglas Wilson, National Security Investigations and Prosecutions §§ 7:11, 18:2 (2013) [hereinafter "Kris &Wilson NSIP"].

18 *See infra* Part V.B (discussing on the Mosaic theory).

19 215 Bulk Secondary Order, *supra* note 16; August 2013 FISC Opinion, *supra* note 16.

provider.[20] The "Primary Order" set out various requirements and limitations on the government during its collection and for use of the telephony metadata.[21] The primary and secondary orders are issued by FISC for ninety days at a time, and they have been renewed consistently since they were first issued in 2006.[22] Only one secondary order directed at one company has been disclosed, although the government has confirmed that FISC has approved similar orders for around three[23] telecommunications companies to produce metadata.[24] As of July 2013, FISC had authorized the bulk metadata collection on thirty-four separate occasions by fourteen different judges.[25] Withstanding accusations of the FISC merely being a rubber stamp for the NSA, the fact that the bulk metadata program has to be reauthorized at regular intervals, and by varying judges ensures that legal reasoning, rather than bureaucratic pressure, is the driving force behind the orders.

II. What information the NSA gets from the Metadata

As previously discussed the metadata collected does not include contents of the communication, the identity, or any data about the physical location of the call other than the area code of the phone number.[26] When General Keith Alexander was asked if the NSA could tell the location of a call, or signal strength, or identify the specific tower of the call, he responded that the only locational information that is received in the database through the metadata is area code of the phone number.[27] Additionally, if the government wanted information about the cell site, or any locational information as part of a bulk production of call records, the government would have to provide

---

20 215 Bulk Secondary Order, *supra* note 16, at 1.

21 *How Disclosed NSA Programs Protect Americans and Why Disclosure Aids our Adversaries: Hearing before the House Permanent Select Committee on Intelligence* (June 18 2013), *available at* http://icontherecord.tumblr.com/post/57812486681/hearing-of-the-house-permanent-select-committee-on [hereinafter "June 18, 2013 HPSCI Hearing"] (statement of James Cole, discussing how the Primary Order " . . . . goes into great detail [about] what we can do with the metadata. How we can access it, how we can look through it, what we can do with it once we have looked through it. . . .").

22 *See generally* Press Release, ODNI, Foreign Intelligence Surveillance Court Renews Authority to Collect Telephony Metadata (July 19, 2013), at http://www.odni.gov/index.php/newsroom/press-releases/191=press -releases-2013/898-foreign-intelligence-surveilllence-court-renews-authority-to-collect-telephony-metadata; *see Section 215*, NSA Factsheet (June 18, 2013), *available at* http://www.wyeden.senate.gov/nes/blog/postwyden-and-udall-to-general-alexander-nsa-must-correct-inaccurate-statement-in-fact-sheet [hereinafter "NSA 215 Factsheet"]; Administration White Paper: *Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act* (Aug 9, 2013) at 1, *available at* http://publicintelilgnece.net/doj-bulk-telephony-collection [hereinafter "White Paper"]; *see also* August 2013 FISC Opinion, *supra* note 16.

23 Aspen Institute, *Counterterrorism, National Security and the Rule of Law*, (July 28, 2013) *available at* http://aspensecurityforum.org/2013-video (statement of Rajesh De).

24 Bob Litt, *Privacy, Technology and National Security: An Overview of Intelligence Collection*, (July 19, 2013) [hereinafter "2013 Litt Speech"] http://www.lawfareblog.com/2013/07/odni-gc-bob-litt-speaking-at-brookings/.

25 *See* White Paper, *supra* note 22, at 3.

26 August 2013 FISC Opinion, *supra* note 16, at 2 n. 2; see June 18, 2013 HPSCI Hearing, *supra* note 21 (statement of Chris Inglis: Question: "So there are no names and no addresses affiliated with these phone numbers?" Answer: "No, there are not, sir."); *see id.* (statement of General 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- is there a known database?" Answer: "NSA does not hold such a database.").

27 *See id.*

briefing, notice, and approval from FISC.[28]

III. Metadata Storage

The disclosures from the government also described how the metadata is stored. Once the metadata is collected it is stored within the secure networks of the NSA, and is uniquely identified. This data can then only be accessed by specifically cleared counterterrorism personnel that have been trained in the court procedures. Each area of data requires different trainings, so a certificate is required.[29] Without the specific certificate for the matching database, an employee is unable to access the metadata records.[30]

IV. Metadata Access

The procedures for accessing the database of metadata are clearly defined for the specific purpose of counterterrorism. This is especially important to note when discussing the line between the Fourth Amendment protections and the metadata collections.[31] Only a small amount of the metadata is ever actually accessed.[32] The stored metadata may only be accessed for intelligence purposes when there is a reasonable suspicion, based on specific facts that a particular identifier, like a phone number, is associated with a terrorist group.[33] The government must get approval from FISC for queries, specifying to which terrorists or targets a query relates. The government's applications to query the database are for specific terrorists that are the subject of a terrorism investigation.[34]

V. Finding of Reasonable Articulable Suspicion

For the element of reasonable suspicion to be fulfilled when presenting a request to query the database, the suspicion must not only be reasonable but must also have an articulated level of suspicion. One of twenty analysts at the NSA and two supervising managers must approve this

28 August 2013 FISC Opinion, *supra* note 16, at 4 n. 5.

29 *See* June 18, 2013 HPSCI Hearing, *supra* note 21 (statement of General Keith Alexander)(explaining that Snowden would have access to the information about how they procure the metadata, but because he didn't have the correct training or certificates he would not have been able to actually see the data that had been collected. In order to work with each set of data, a person must be trained and have a certificate to work with that data. In other words, the certificate is a key to the data.).

30 *See* NSA 215 Factsheet, *supra* note 22; *see* June 18, 2013 HPSCI Hearing, *supra* note 21 (statement of General Keith Alexander); *see also* August 2013 FISC Opinion, *supra* note 16, at 4-5 nn.2-3.

31 *See infra* Part V.

32 *See* 2013 Litt Speech, *supra* note 24.

33 Letter from Peter J. Kadzik, Principal Deputy Assistant Attorney to Representative Sensenbrenner (July 16, 2013) [hereinafter Sensenbrenner Letter], *available at* http://sensenbrenner.house.gov/uploadedfiles/ag_holder_response_to_congressman_sensenbrenner_on_fisa.pdf.

34 *See* 2013 Litt Speech, *supra* note 24.

reasonable suspicion.[35] Any authorized analyst who wants to query the database must have another authorized analyst also agree that there is a reasonable suspicion. Essentially there is always a two person control rule, with one of the analysts or managers providing oversight.[36] These twenty two NSA officials are specially designated and trained and are the only people that can make a finding that there is a reasonable articulable suspicion that a seed identifier[37] proposed for query is associated with a specific foreign terrorist organization.[38] If any of the numbers that are suspected involve the possibility of being connected to U.S. persons,[39] the NSA Office of General Counsel must review and approve such findings before the query is searched in the database.[40]

Findings of reasonable articulable suspicion must be made in writing in advance of the query being submitted and executed.[41] There are only seven officials in the NSA who can approve queries.[42] Individual queries are not reviewed by FISC,[43] but the Court sets out the criteria for the queries and receives regular reports every thirty days[44] on the number of identifiers used to query the metadata as well as the number of times a U.S. person's information is returned in the results.[45] A finding of a reasonable articulable suspicion is good for 180 days when involving U.S. persons and for one year for queries on non-U.S. persons.[46] There is an extra layer of protection for a finding of reasonable articulable suspicion for selectors believed to be for or of U.S. persons. NSA's General Counsel must determine that the reasonable articulable suspicion is not based solely on First

35 *See* June 18, 2013 HPSCI Hearing, *supra* note 21 (statement of Chris Inglis).

36 *Id.*

37 *See* June 18, 2013 HPSCI Hearing, *supra* note 21 (statement of Chris Inglis); *see also* Sensenbrenner Letter, *supra* note 33, at 2 (explaining that a seed identifier is a telephone number that is used as a query).

38 White Paper, *supra* note 22, at 5.

39 *See* James R. Clapper, *DNI statement of Activities Authorized under 702 of FISA*, Office of the Director of National Intelligence (June 6, 2013), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/869-dni-statement-on-activities-authorized-under-section-702-of-fisa (responding to articles in the *Guardian* and the *Washington Post*, DNI Clapper issued a statement that the activities cannot be used to intentionally target any US citizen or any other American or anyone located in the United States.); *see also* 50 U.S.C. §1801(i) ("United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101 (a) (20) of title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section."); Eric Holder Jr., Attorney General, Exhibit B: *Minimization Procedures Used by the National Security Agency Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended July 28, 2009*, *available at* http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB436/docs/EBB-026.pdf (defining guidelines determining what a US person is in regards to metadata collection).

40 *See* August 2013 FISC Opinion, *supra* note 16, at 7.

41 *See* June 18, 2013 HPSCI Hearing, *supra* note 21 (statement of James Cole); *see* Sensenbrenner Letter, *supra* note 33, at 3.

42 *See* August 2013 FISC Opinion, *supra* note 16, at 7 n. 6.

43 *See* June 18, 2013 HPSCI Hearing, *supra* note 21 (statement of James Cole); *see* 215 Bulk Secondary Order, *supra* note 16, at 16.

44 *See* NSA 215 Factsheet, *supra* note 22 (stating that the NSA has other reporting duties as well concerning the queries into the metadata database. There are the 30 day reports to the FISC, 90 day meetings of NSA, DOJ and ODNI and 90 day meetings between the NSA and its inspector general.).

45 215 Bulk Secondary Order, *supra* note 16, at 16.

46 215 Bulk Secondary Order, *supra* note 16, at 10; August 2013 FISC Opinion, *supra* note 16, Order at 10.

Amendment activities.[47]

VI. HOPS

In 2012, around 300 identifiers met the reasonable articulable suspicion standard and were queried in the database.[48] While there were only 300 identifiers, the NSA is allowed to query them multiple times.[49] Each initial query may produce two additional "hops"[50] or numbers that are related to the initial query. Under the FISC order, the NSA may obtain information concerning the second and third tier contacts of the original seed identifier. The first hop relates to a set of numbers that are in direct contact with the seed identifier. The second hop numbers related to the numbers found from the first hop and the third hop represents numbers that are connected to the second hop.[51]

NSA agency officials have stated that even though they are allowed up to a three-hop analysis, analysts are careful to not overuse this, and rarely get to the third tier hop.[52] For example, in 2012 the NSA provided twelve reports to the FBI, which included less than 500 numbers that had been generated by the queries and their related hops.[53] The hops are mainly used to determine patterns and to understand the manners and methods by which targets network and communicate with each other.[54]

VII. DATA-MINING OR CONTACT CHAINING

Prior to 2006, the NSA developed an "alert list" process to assist in the review of the telephony metadata it received. The alert list contained the telephone identifiers that NSA was targeting for collection, including some that had not met the reasonable articulable suspicion standard. The NSA automated system then ran the targeted numbers against the telephony metadata set.[55] Since 2006, the NSA has not been authorized to use this type of data mining technique. The government has not disclosed any documents indicating data mining, contact

47 August 2013 FISC Opinion, *supra* note 16, at 7-9.

48 *See Senate Judiciary Committee Strengthening Privacy Rights and National Security; Oversight of FISA Surveillance Programs*, (July 31, 2013) [hereinafter "July SJC Hearing"] (statement of Senator Feinstein), *available at* http://icontherecord.tumblr.com/post/57811913209/hearing-of-the-senate-judiciary-committee-on; *see* NSA 215 Factsheet, *supra* note 22; *see* Sensenbrenner Letter, *supra* note 33.

49 *See* June 18, 2013 HPSCI Hearing, *supra* note 21 (statement of Chris Inglis).

50 *House Judiciary Committee: Oversight of the Administration's use of FISA Authorities* (July 17, 2013) [hereinafter "July 2013 HJC Hearing"] (statement of Chris Inglis).

51 White Paper, *supra* note 22, at 4.

52 July 2013 HJC Hearing, (statement of Chris Inglis).

53 215 Bulk Secondary Order, *supra* note 16, at 11.

54 *Id.*

55 Memorandum of the United States in Response to the Court's Order Dated January 28, 2009 No. BR-08-13 (Feb. 17, 2009), https://www.fas.org/irp/agency/doj/fisa/fisc-021209.pdf.

chaining[56] or other automated programs related to the bulk metadata production.[57]

However, the NSA can receive data under other legal authority that may not be subject to the FISA and FISC rulings.[58] Alternative methods of metadata collection would include bulk metadata collection that is under Executive Order 12333.[59] NSA technicians under the FISA orders may access the metadata to manage the data to make it more useable and identify high volume numbers that are for non-terrorist activities such as telemarketing.[60]

VIII. Disseminating Metadata information of Interest relating to a U.S. person

Only seven senior officials at the NSA may authorize the dissemination of any information that might be attributable to a U.S. person.[61] The information can only be made available to the FBI, and only if the information is related to and or necessary to understand a counterterrorism initiative.[62]

The NSA has a strict policy for when a U.S. person's information is received. If the U.S. person's information received was unintentional, inadvertent, or as reverse targeting (someone targeted a foreign entity who is known to communicated with a U.S. person) collection, an analyst must stop collection immediately, cancel all reports based on that collection, notify their superior or auditor, write up an incident report immediately, and submit the incident write up for inclusion in the Inspector General Quarterly review.[63] If an analyst targets a legitimate foreign entity and information and or communications are acquired from or about a U.S. person, minimization procedures must be put in place, and the focus must be on the foreign end of the report.[64] Since it is found incidental to a search it does not have to be included in the Inspector General's Quarterly review.[65]

---

56 *See* Memorandum from Kenneth L. Wainstein, Assistant Attorney General, Subject: Proposed Amendment to Department of Defense Procedures to Permit the National Security Agency to Conduct Analysis of Communications Metadata Associated with Persons in the United States, to the Attorney General, November 20, 2007 at 2 *available at* http://www.guardian.co.uk/world.interactive/2013/jun/27/nsa-data-collection-justice -department (explaining that contact chaining involves the use of computer algorithms to create a chain of contacts linking telephone numbers, IP addresses, addresses, and email addresses of target. This is a document that was disclosed by Snowden via the Guardian and has not been officially recognized by the government. For the purposes of this paper it will only provide background information and definitions.).

57 215 Bulk Secondary Order, *supra* note 16, at 6.

58 *See* August 2013 FISC Opinion, *supra* note 16, at 10 n. 10.

59 18 U.S.C. § 2511(2)(f).

60 *See* 215 Bulk Secondary Order, *supra* note 16, at 5-6; *see also* August 2013 FISC Opinion, *supra* note 16, 5-6.a

61 *See* June 18, 2013 HPSCI Hearing, *supra* note 21 (statement of Chris Inglis).

62 *See id.*

63 (U) Lesson 4: So you got U.S. Person Information?, *available at* https://www.eff.org/files/2013/11/15/20130816-wapo-so_you_got_a_us_person.pdf.

64 *Id.*

65 *Id.*

IX. Minimization procedures

Metadata that has not been reviewed, which is the majority of metadata received, is retained for about five years,[66] and is then automatically deleted from the NSA's system on a rolling basis.[67] Data that has been collected improperly is also purged.[68] For the acquisition, retention, use, or dissemination of non-publically available information concerning non-consenting U.S. persons, strict procedures are in place to minimize the data.[69] The most important part of the minimization procedures is having analysts review the data and make a reasonable judgment if the data is from or about a U.S. person. This can be very difficult especially in Internet and phone metadata because the data does not have any locational identifiers, except area codes and ISP addresses which are not dispositive of locational confirmation. Once an analyst determines that the data belongs to a U.S. person, minimization procedures take precedent and unless an exception is applicable, the data is destroyed immediately.[70]

Domestic information or information that is by or about a U.S. person will not be destroyed if the communication is reasonably believed to contain significant foreign intelligence information, or reasonably believed to contain evidence of a serious crime that has been, is being, or is about to be committed,[71] or in situations where the technical data is needed to understand a foreign intelligence operational concern, or lastly if there is evidence of a national security threat or threat to human life.[72] If the communication intercepted happens to contain attorney client privilege communication about a person who is known to be under criminal indictment in the United States, the communication monitoring will cease immediately, and procedures are put in place to protect the data and it cannot be used in the criminal case.[73]

X. Compliance Issues

There have been several reported compliance issues, the vast majority of which were self-identified from the NSA, because of the in house procedures in place.[74] Once a compliance

66 *See* June 18, 2013 HPSCI Hearing, *supra* note 21 (statement of Chris Inglis); *see* 215 Bulk Secondary Order, *supra* note 16, at 4.

67 National Security Agency Central Security Service, *USSID-18*, 27 July 1993, http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB24/nsa11a.pdf.

68 *See* June 18, 2013 HPSCI Hearing, *supra* note 21 (statement of Chris Inglis).

69 *Minimization Procedures used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978*, as amended, Oct. 21, 2011, [hereinafter "NSA Minimization Procedures"] http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB436/docs/EBB-038.pdf.

70 *Id.*

71 *See id.* (explaining that if the communication is about a crime, the information may be disseminated, including the US person identities to appropriate Federal law enforcing authorities in accordance with 50 U.S.C. §1806(b) and §1825(c). After dissemination the NSA can only keep the data for up to six months, unless authorized by the Attorney General to allow reasonable access for the law enforcement agencies if needed.).

72 *See* NSA Minimization Procedures, *supra* note 69.

73 *See id.*

74 June 18, 2013 HPSCI Hearing, *supra* note 21 (statement of Bob Litt and General Keith Alexander).

issue is identified, the NSA works with the FISC judges to correct what has gone awry.[75] Often the mistake is human error, such as transposing numbers or letters which, for querying purposes, make a big difference. However, there has never been a finding of an intentional violation of the court orders.[76] Once a mistake is submitted to the FISC, the FISC demands an in-depth analysis of what went wrong, why, what has been done to remedy the situation, and if the NSA has gotten rid of the information wrongly procured.[77] In addition to individual compliance reports, the FISC receives quarterly reports about compliance issues.[78] Several good examples of FISC oversight and compliance with the NSA have been released.[79] The NSA is also audited by the Department of Justice, the Office of the Director of National Intelligence and the Attorney General.[80] It is important to note, that throughout these years of audits, none of the compliance incidents have involved the application of the reasonable articulable suspicion standard, which is at the foundation of the metadata program.[81]

XI. The Purpose of it All

One of the biggest problems the United States faces in preventing terrorists' attacks is the identification of terrorists and their networks.[82] Whilst identifying specific spies and or plots by enemies was important in previous years, the government usually had an idea of who the enemy was. With the advent of increased terrorist activity, the government is not fighting against one group, but multiple small groups scattered throughout the world.[83] Terrorists groups come in all sizes, from all nations, and with differing goals, hence identification is particularly difficult and important. Communication between countries and therefore terrorists groups has never been easier than now considering the near-global ubiquity of the Internet and cell phones.[84]

The United States uses the metadata it collects to identify present and future terrorist plots,

75 *See id.*

76 *See id.* (statement of James Cole).

77 *Id.*

78 White Paper, *supra* note 22, at 5.

79 *See* Memorandum Opinion, (October 3, 2011 FISC Ct.); *see also* Memorandum Opinion, (Nov. 2011 FISC Ct.); *see also* August 2013 FISC Opinion, *supra* note 16, at 5 ("The court is aware that in prior years there have been incidents of non-compliance with respect to NSA's handling of produced information. Through oversight by the court over a period of months, those issues were resolved.").

80 *See* Department of Justice and Office of the Director of National Intelligence, *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: December 1, 2008- May 31, 2009, (December 2009); *see also* Department of Justice and Office of the Director of National Intelligence, *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence*, Reporting Period: June 1, 2009-November 30, 2009, (May 2010).

81 June 18, 2013 HPSCI Hearing, *supra* note 21 (statement of General Keith Alexander).

82 White Paper, *supra* note 22, at 2.

83 Robert J. Hanyok, *The First Round: NSA's Effort against International Terrorism in the 1970s*, Cryptologic Almanac, November- December 2002.

84 A. Denis Clift, *Intelligence in the Internet Era*, Studies in Intelligence 73 (Fall 2003), http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB436/docs/EBB-008.pdf.

using crime mapping and network analysis.[85] The metadata collection program was specifically designed to assist the U.S. Government in detecting communications between known or suspected terrorists who are operating outside of the United States and who are communicating with others inside the United States, as well as communication between operatives within the United States.[86] By doing so, the program helps to close the critical intelligence gaps that were highlighted by the September 11, 2001 attacks.[87]

III. This Ain't our First Rodeo

In order to understand wiretapping, telephony metadata, and surveillance it is important to look at the history of surveillance, with a special emphasis on electronic surveillance. The history of electronic surveillance leads right into the creation of FISA, and how Congress came to the current understanding of FISA, and electronic surveillance for national security purposes.

I. In the Beginning

Surveillance and spying is not a new concept. Nor is domestic surveillance, and its ensuing controversy. In 1797, Secretary of State Timothy Pickering hired a private agent to investigate a conspiracy between the British navy and Senator William Blount.[88] In 1862, Secretary of War Edwin M. Stanton asked President Lincoln for complete control over the telegraph lines.[89] The President granted this authority and soon the telegraph lines running through Stanton's office made his department the nexus of war information. He used power over the telegraphs to influence what the journalists did or did not publish, and arrested dozens of journalists on questionable charges.[90] After the war ended, Congress addressed this use of telegraph censorship and reprimanded the administration.

In World War I the government took over operation of the phones as a wartime measure.[91] In 1924, Attorney General Harlan Stone, seeking to recover credibility from recent scandals

85 North Atlantic Treaty Organization, *Intelligence Exploitation of the Internet*, (October 2002), available at http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB436/docs/EBB-005.pdf (discussing the early implications for electronic privacy); *see* Marcia S. Smith, Jeffrey W. Seiffer, Glenn J. McLoughlin & John Moteff, *The Internet and the USA Patriot Act: Potential Implications for Electronic Privacy, Security, Commerce and Government*, Cong. Research Serv., March 4, 2002, http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB436/docs/EBB-004.pdf.

86 White Paper, *supra* note 22, at 3.

87 *Id*; *see also* Nat'l Comm'n: On Terrorist Attacks Upon the U.S., The 9/11 Commission Report 339-60 (2004), http://www.gpoaccess.gov/911/pdf/full reportf.pdf; *see also* Office of the Inspector General, A Review of the FBI's Handling of Inteligence Information Related to the September 11 Attacks 21-42, http://www.justice.gov/oig/special/s0606/final.pdf.

88 *See* Samuel Edwards, Barbary General: *The Life of William H. Eaton*, 54-55 (Prentice-Hall 1968) (describing investigation into plot); Buckner F. Melton, Jr., *The First Impeachment*, 93 (Mercer Univ. Press 1998) (describing plot).

89 David T.Z. Mindich, *Lincoln's Surveillance State*, N.Y. Times, July 5, 2013, http://www.nytimes.com/2013/07/06/opinion/lincolns-surveillance-state.html?_r=0.

90 *Id.*

91 Brief of Defendant- Appellant at 7, Nardone v. United States, 302 U.S. 379 (1937) (No.190).

involving the Justice Department Bureau of Investigation spying on Congress[92] and the Palmer Raids, announced that the FBI was concerned only with investigating conduct forbidden by law and not opinions, political or otherwise.[93] He restricted the use of wiretaps and referred to the practice as unethical.[94]

Four years later, the first electronic surveillance case reached the United States' Supreme Court.[95] In the *Olmstead* case, evidence had been obtained through wiretaps that were inserted along the ordinary telephone wires.[96] The Court held that because no entry of the houses or offices of the defendants took place, or in other words, no trespass, there was no Fourth Amendment violation.[97] Despite the dissenting voices,[98] the trespass doctrine of the Fourth Amendment was put in place.

The Court stated in *Olmstead* that although wiretapping was legal via Fourth Amendment standards, Congress could choose to bar wiretapping as admissible evidence through legislation.[99] With the Federal Communications Act of 1934, Congress protected wire communications.[100] However, the Federal Communications Act said nothing about the use of mechanical devices used to record in person conversations.[101] Without this prohibition, Fourth Amendment cases continued to go through the courts and started eroding the trespass doctrine of *Olmstead*.[102]

II. *Katz*, *Keith*, and Church: On the Way to FISA

Four decades after *Olmstead* the Supreme Court finally overruled the trespass doctrine.[103]

---

92 *See* Athan Theoharis, *From the Secret Files of J. Edgar Hoover* 2 (1991).

93 *See* Neal Katyal & Richard Caplan, *The Surprisingly Stronger Case for the Legality of the NSA Surveillance Program: The FDR Precedent*, 60 Stan. L. Rev. 1023 (Feb. 2008).

94 *See* Richard E. Morgan, *Domestic Intelligence: Monitoring Dissent in America*, 89 (1980).

95 *See* Mark D. Young, *Electronic Surveillance in an Era of Modern Technology and Evolving Threats to National Security*, 22 Stan. L. & Pol'y Rev. 11, 15 (2011).

96 Olmstead v. United States, 277 U.S. 438 (1928).

97 *Id* at 457.

98 *Id* at 479.

99 *Id* at 465-466.

100 Pub. L. No. 416 § 605, 48 Stat. 1064 (noting that despite the Federal Communications Act, FDR and the FBI continued to use wiretapping, even though the court disallowed wiretapping as evidence in *Nardone I* and *Nardone II*.); *see also* Neal Katyal and Richard Caplan, *The Surprisingly Stronger Case for the Legality of the NSA Surveillance Program: The FDR Precedent*, 60 Stan. L. Rev. 1023 (Feb. 2008) (discussing surveillance during FDR's administration).

101 *See* Nardone v. United States, 302 U.S. 379, 380-82 (1937); *see also* Nardone v. United States 308 US 338, 340 (1939) (*Nardone II*) (holding that evidence obtained through wiretapping was not admissible in court).

102 Gina Marie Stevens & Charles Doyle, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, Cong. Research Serv., Oct. 9, 2012; *see also* Goldman v. United States, 316 U.S. 129 (1942) (saying that the use of a Dictaphone to secretly overhear a private conversation in an adjacent office offended no Fourth Amendment protection because no physical trespass into the office in which the conversation took place had occurred); *see also* Lee v. United States 343 U.S. 747 (1952) (noting that the absence of a physical trespass precluded the Fourth Amendment coverage of where a federal agent secretly recorded his conversation with the defendant held in a commercial laundry in a public area); Silverman v. United States, 364, U.S. 505 (1961) (ruling that the Fourth Amendment was violated when the government drove a spike mike into the common wall of a row house until it made contact with a heating duct for the home in which the conversation occurred.).

103 Rebecca A. Copeland, *War on Terrorism or War on Constitutional Rights? Blurring the Lines of Intelligence Gathering in Post-*

In *Katz*, the Court was confronted with communications obtained by the FBI through electronic listening and recording devices that were attached to the outside of a public telephone booth known to be used often by the defendant.[104] In its analysis the Court described a new test to be used with the Fourth Amendment involving a reasonable expectation of privacy.[105] Even though the phone booth was made of glass and in a public place, the idea that the door shuts provides a reasonable person the belief that their conversations will remain private.[106] However, the Court specifically stated that this decision did not apply to surveillance under the auspices of national security.[107]

In response to *Katz*, Congress enacted the Omnibus Control and Safe Streets Act in 1968.[108] The original version of the Omnibus Act protected unauthorized aural interceptions defined as interceptions made by a wire or oral means, understandable by the human ear, and communicated via a common carrier.[109] This was not a restriction on electronic surveillance, although the Omnibus Act was later amended to include electronic communications.[110] However the Omnibus Act was still not a protection against the President's power to wiretap without warrants outside of the United States and it did not provide protections for interceptions related to any kind of foreign surveillance or national security protection by the government.[111] `

The *Keith* decision involved the warrantless electronic surveillance of a defendant in a federal prosecution of radicals for destruction of government property.[112] The government acknowledged the electronic surveillance of the defendant but argued that since Title III and the Omnibus Crime Control Act[113] did not mention the limitation of the presidential power to wiretap domestically to protect national security, it had in effect given the power to conduct electronic surveillance directed against domestic groups that advanced violence against the government.[114] The Justices decided that the specific facts of the case did not justify warrantless surveillance, and therefore the surveillance was a violation of the Fourth Amendment. However *Keith* left gaps in the constitutional law of intelligence gathering.[115] First, the warrant requirement it imposed did not extend to cases involving foreign intelligence. The opinion ended by reiterating that the warrant requirement applied only

---

September 11 America, 35 TEX. TECH. L. REV. 1 (2004).

104 Katz v. United States, 389 U.S. 347 (1967).

105 *See id.* at 351.

106 *See id.*

107 *Id* at 358-64.

108 Wire and Electronic Communications Interception and Interception of Oral Communications, 18 U.S.C. §§ 2510-22 (2000).

109 *See* Rebecca A. Copeland, *War on Terrorism or War on Constitutional Rights? Blurring the Lines of Intelligence Gathering in Post-September 11 America*, 35 TEX. TECH. L. REV. 1, 8 (2004).

110 *See* S. Rep. No 99-541 at 1 (1986) (noting that in 1986, the Omnibus Act was amended by the Electronic Communications Privacy Act (ECPA) to account for the changes in new computer and telecommunications technologies).

111 *See* Copeland, *supra* note 109, at 8.

112 United States v. United States Dist. Court (*Keith*) 407 U.S. 297 (1972).

113 18 U.S.C. §§ 2510-22 (2006).

114 Robert C. Power, *"Intelligence" Search's and Purpose: A Significant Mismatch Between Constitutional Criminal Procedure and the Law of Intelligence- Gathering*, 30 PACE L. R. 620 (2010).

115 *Id* at 629.

to domestic aspects of national security without fully defining the category.[116] Second, the opinion emphasized that electronic surveillance for domestic intelligence might be appropriate under different standards than those that apply to the criminal law enforcement, noting its own use of Constitutional interest balancing for non law enforcement purposes.[117] The Court again urged Congress to create laws that would regulate surveillance to protect domestic national security.[118] The Court also recognized that "unless the Government safeguards its own capacity to function and to preserve the security of its people, society itself could become so disordered that all rights and liberties would be endangered."[119]

Keith was followed by several lower court cases involving surveillance where foreign powers were involved, but where the communications of American citizens were overheard. The majority of the lower courts upheld warrantless searches, even involves U.S. citizens,[120] however the D.C. Circuit differed and held that warrantless searches were unconstitutional.[121]

In the following years, a series of news stories broke detailing the existence of covert domestic surveillance programs directed at U.S. citizens.[122] The publicity surrounding the various abuses by intelligence agencies, including NSA surveillance of Americans and drug traffickers, U.S. Army military intelligence surveillance of domestic groups, FBI covert operations against alleged subversive groups, CIA opening of domestic mail sent to or received from abroad, and electronic surveillance of political enemies, fanned by investigations and reports by the Senate, the House, and the Executive branch, had significant effects.[123] Congress put together a special committee, spearheaded by Senator Frank Church, to investigate the many accusations surrounding the abuse of power by the Intelligence community.[124] Their investigation found that the Intelligence community was not the "rogue elephant" they thought, and that almost every activity which had previously caused disrepute were ordered by a senior official or the President.[125] After the Watergate scandal

116 *Id*

117 *Id*

118 United States v. United States Dist. Court (*Keith*), 407 U.S. 297 (1972)(stating, "Given those potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III.").

119 *Id* at 312.

120 *See* United State v. Brown, 484 F.2d 418 (5th Cir. 1973) (upholding warrantless searches wiretap against US citizen); *see* United States v. Butenko, 494 F. 2d 593 (3rd Cir. 1974) (saying that a wiretap is valid if primary purpose to gather foreign intelligence information); United States v. Buck, 548 F.2d 871,875 (9th Cir. 1977) (ruling that warrantless surveillance is "lawful for the purpose of gathering foreign intelligence").

121 *See* Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975) (finding surveillance of the Jewish Defense League unconstitutional because although the JDL was involved in international terrorist activities there was no showing that the JDL was itself a foreign power or an agent of a foreign power, and therefore did not fit under the *Keith* exception).

122 *See* Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 Harv. J.L. & Pub. Pol'y 757 (2014) (forthcoming).

123 *See* William Funk, *Electronic Surveillance of Terrorism: the Intelligence/ Law Enforcement Dilemma- A History*, 11 Lewis & Clark L. Rev. 1099 (2007).

124 *See* Robert F. Turner, *First Principles: Are Judicial and Legislative Oversight of NSA Constitutional?*, The Federalist Society for Law & Public Policy Studies, October 21, 2013.

125 *See id.* (explaining that Representative Otis Pike who chaired the House Committee investigation on the CIA said that after the investigation he had a higher regard for the CIA than when he started. He went on to state that the Committee found a multitude of evidence where the CIA said "don't do it" and the White House had said "we are

came to light, Congress decided that new legislation was needed to legislate the powers around the President's surveillance power.[126]

III. FISA

Senator Kennedy introduced the first draft of what would later become the Foreign Intelligence Surveillance Act in 1976.[127] After multiple hearings and revisions, President Carter signed the Foreign Intelligence Surveillance Act (FISA) into law on October 25, 1978.[128] FISA established the Foreign Intelligence Surveillance Court (FISC) in order to hear applications for electronic surveillance.[129]

As passed, FISA authorized electronic surveillance[130] of a foreign power[131] or agent of a foreign power[132] to obtain foreign intelligence information via two separate means. The first path to authorization for surveillance would be for the Attorney General to certify under oath that the surveillance was solely directed at the communications transmitted exclusively between certain foreign powers, and that the surveillance was not intended to and was unlikely to taint the communications of a U.S. person.[133] This type of surveillance could be authorized for up to one year.[134] For all other circumstances, FISA requires the FISC to authorize surveillances.[135] In order to obtain an order from the FISC, the Attorney General must submit an application that includes information about the identity or a description of the target of the surveillance, the facts and circumstances justifying the belief that the target is a foreign power or agent of a power, the means by which the surveillance will be implemented and minimization procedures, as well as a description of the type of information sought and the type of communication or activities that are subject to

---

going to anyway." The CIA was much more professional and had a far deeper reading on the down the road implications of some immediately popular act than the executive branch or administrative officials. The CIA never did anything the White House didn't want. Sometimes they didn't want to do what they did); *see also* Frank J. Smith, Jr., *Congress Oversees the United States Intelligence Community* 197 (1990).

126 *See* Robert A. Dawson, *Shifting the Balance: The DC Circuit and the Foreign Intelligence Surveillance Act of 1978*, 61 GEO. WASH. L. REV. 1380, 1382-87 (1993).

127 50 U.S.C. §§ 1801 (1982).

128 *See* Funk, *supra* note 123, at 1112.

129 *See* § 1803(a).

130 *See* § 1801(f) (defining electronic surveillance to include four different forms of surveillance. The first would include ordinary wiretaps. The second and third would include various radio communications, and the last would be include the ordinary "bugging." Together this was intended to cover all electronic surveillance in the United Sates directed at persons in the United States. It was not intended to cover surveillances abroad or even surveillance of communications to the United States if conducted abroad); H.R. Rep. No. 95-1283, pt. 1, at 50-51 (1978).

131 *See* § 1801(a) (defining foreign power as two separate sets of entities. The first set included foreign government or factions of foreign nations, and the second set included groups involved in international terrorism.).

132 *See* § 1801(b); *see* Clapper, *supra* note 39 (defining an agent of power differently depending upon whether the person was a US citizen. If the person was not a US person, any officer or employee or member of a foreign power would qualify as an agent of a foreign power, and additionally if any person acted on behalf of, or assisted a foreign power in sabotage or international terrorism would qualify as an agent to a foreign power).

133 50 U.S.C.§ 1802(a)(1) (1982).

134 *See id.*

135 § 1802(b).

surveillance.[136]

Three certificates are required to accompany the application to the FISC stating that the purpose of the surveillance is to obtain foreign intelligence information, that the information sought is foreign intelligence information, and that the information cannot be reasonably obtained through normal means.[137] One of the FISC judges then reviews the application making sure that all of the minimization procedures are met, and that there is sufficient probable cause to believe that the target is a foreign power.[138] The original authorizations from the FISC are for ninety-day periods of surveillance, although they can be renewed as needed.[139]

It is clear from the brief legislative history detailed above that FISA was meant as a protection for U.S. citizens against warrantless searches. However, the legislature still knew that the protection of national security remained paramount and because of that, surveillance would be allowed, but it would now have the oversight of its own court with judges specially acquainted with the laws and needs of national security. FISC provides the vehicle for foreign surveillance warrants to be obtained, with a differing standard from the warrant procedures of criminal law. Hence, FISA can be seen as an extra protection for those worried about Nixon Era wiretapping resurfacing.

IV. FISA Post 9/11

After the attacks on the World Trade Center and the Pentagon on September 11, legislators quickly expressed frustration with the failure of intelligence agencies and law enforcement to prevent such a large-scale attack.[140] The Attorney General asked that Congress grant the Justice Department greater power to prevent future terrorists acts.[141] Within six weeks of the attacks, Congress passed the USA PATRIOT Act, a warp speed for the legislature.[142] The USA PATRIOT Act made numerous changes and amendments to existing law, including several distinct changes in FISA.[143] The USA PATRIOT Act changed the test used for issuance of a FISA surveillance order from "the purpose of the surveillance is to obtain foreign intelligence information"[144] to "a significant purpose of the surveillance must be for obtaining foreign intelligence."[145] This small phrasing change signaled a significant change in the standard for issuance of FISA Surveillance.[146]

---

136 § 1804(a)(3)-(6), (8).

137 § 1804(a)(7).

138 § 18095(a)(3).

139 50 U.S.C. § 1805(d)(1) (1982).

140 *See* Michael T. McCarthy, *U.S.A. Patriot Act*, 39 Harv. J. on Legis. 435, 438-39 (2002) (saying that prior to September 11, the CIA had intelligence on two of the hijackers identifying them as suspected terrorist, but the agency failed to share that information with FBI in time for them to prevent the hijackers from entering the country).

141 *See id.* at 437-38.

142 *Id.*

143 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act of 2001), Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered titles of the U.S.C).

144 50 U.S.C. § 1804(a)(7)(B) (1991).

145 50 U.S.C. § 1801(A)(7)(B) (2003).

146 Jennifer L. Sullivan, *From "The Purpose" to "a Significant Purpose": Assessing the constitutionality of the Foreign Intelligence Surveillance Act Under the Fourth Amendment*, 19 Notre Dame J. L. Ethics & Pub. Pol'y 379 (2005).

Other issues besides foreign intelligence could be investigated, as long as the foreign intelligence element was still prominent. Other changes included the addition of roving wiretaps, the ability to secretly survey email communications, and an expanded duration for which a FISA warrant is valid.[147]

FISA has continued to change since the USA PATRIOT Act. The 2008 FISA Amendments preserved the changes to FISA made by the USA PATRIOT Act. Besides proving that the gathering of foreign intelligence is a significant purpose of the wiretap, the government must, in addition, establish a reason for the belief that the target is an agent or employee of a foreign power.[148] The 2008 Amendments also changed the original FISA standard for non-U.S. persons, who are located abroad. As per the original statute, no warrant is required if the wiretap does not require access to facilities located in the United States, for a non-U.S. person.[149] However when the wiretap requires access to facilities in the United States, a FISA warrant is required, although the government must only prove that a significant purpose of the tap is to procure foreign intelligence information. The 2008 Amendments also relives the government of the need to disclose to a FISA judge the identity of each individual to be targeted. The amendments only require that the government describe and employ procedures reasonably designed to ensure that its proposed surveillance activity will only target foreigners abroad.[150]

The USA PATRIOT Act and the 2008 FISA Amendments definitely broadened the scope of the government's authority to wiretap. However, it is still more limited than pre-FISA surveillance authority. One important thing to notice is that FISA was originally enacted to monitor the domestic surveillance of foreign powers, which has now morphed into protections guaranteed against non-U.S. persons abroad. Most of the overreaching amendments of current day FISA are applicable only to non-U.S. persons abroad; these people are not, nor ever were, protected by the Constitution. In effect, FISA extends protections out to members of the world community that historically have no Constitutional protections, in order to placate the fears of an overreaching government by U.S. citizens.

Taking into consideration the overwhelming globalization[151] of the American economy and culture, it is inevitable that some U.S. person's information will be collected. FISA provides an extra layer of protection via the FISC, and via mandated minimization procedures. In light of the recent NSA disclosures, focus should be shifted from the Constitutionality of FISA to the congratulations of the Intelligence Community on the relatively small number of violations for such an overarching program in the new globalized world.

147 *See* Copeland, *supra* note 103; *see also* Sullivan, *supra* note 147.

148 *See* FISA Amendments ACT of 2008, Pub. L. No. 110-261, codified at 50 U.S.C. § 1881 (2012).

149 *Id.*

150 § 1881(a)-(g); *see also* William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEX. L. REV. 1633 (2010).

151 *See generally* Elizabeth B. Bazan, *The Foreign Intelligence Surveillance Act: An Overview of Selected Issues*, CONG. RESEARCH SERV., July 7, 2008, at 7.

IV. Walking the line of the Fourth Amendment: Privacy versus National Security

One of the main issues with the Snowden revelations was the confrontation of where the line between civil liberties, primarily privacy, and national security lies.[152] The Fourth Amendment protects against unreasonable searches and seizures—basically the right of privacy from the government for individuals. This paper has already touched upon some Fourth Amendment issues in Part Three, but mainly in relation to FISA. Even though there is statutory law backing up the national security surveillances that have been released, this next section will talk about how the Fourth Amendment interacts with the activities of the NSA.

I. The Third Party Doctrine

The Third Party doctrine of the Fourth Amendment provides that any information willingly exposed to a third party loses all Fourth Amendment protection. The theory reasons that once a person shares information willingly with a third party, one assumes the risk that the third party may divulge that information to others, including the government.[153] Under longstanding Supreme Court precedent, the Third Party doctrine holds that even if there is an understanding that the third party will treat the information as conditional, the information is no longer protected under the Fourth Amendment.[154] These facts alone would be enough to justify the application of the third party doctrine to the telephony metadata collection program conducted by the NSA. However, the Supreme Court has directly addressed the issue of telephone data, and Fourth Amendment implications via the Fourth Amendment with *Smith v. Maryland*.[155]

In *Smith*, the Court held that the installation of a pen register was not a search within the meaning of the Fourth Amendment and thus that no warrant was required to collect such information.[156] The pen register collected the dialed phone numbers from the telephone company.[157] It did not constitute a search because persons making phone calls lack a reasonable expectation of privacy in the numbers they dial.[158] The Court explained that even if someone did intend to keep the numbers they dialed secret, the person has "voluntarily conveyed numerical information to the telephone company and exposed that information to its equipment in the ordinary scope of business and therefore has assumed the risk the company would reveal to the police the numbers which were dialed."[159]

---

152 *See* Robert N. Davis, *Striking the Balance: National Security vs. Civil Liberties*, 29 Brook. J. Int'l L. 175 (2003).

153 *See generally* United States v. Miller, 425 U.S. 435 (1976); *see* Smith v. Maryland, 442 U.S. 735 (1979).

154 *See* White Paper, *supra* note 22, at 20; *see also* Miller, 425 U.S. at 443 ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to the Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."); *see also* SEC v. Jerry T. O'Brian, Inc., 467 U.S. 735, 743 (1984).

155 *See* Smith, 442 U.S. at 735.

156 *See id.* at 745-46.

157 *Id.*

158 *Id.*

159 Smith v. Maryland, 442 U.S. 735, 744 (1879).

Under *Smith* the telephony metadata program conducted by the NSA is clearly within Constitutional bounds. As previously discussed, the metadata only reveals the basics of the call information such as the numbers dialed and the length and time of dialing.[160] Some scholars might argue that it is not the individual's rights that are being infringed upon, but the telecommunications providers. However, the Court has also stated that Fourth Amendment rights "are personal in nature, and cannot bestow vicarious protection on those who do not have a reasonable expectation of privacy in the place to be searched."[161] Therefore, the telecommunications providers may not assert the Fourth Amendment rights of their customers. Under this same principle, there is no Fourth Amendment expectation of privacy by virtue of the fact that the telephony metadata records of many individuals are collected rather than those of a single individual.[162]

Additionally, the courts have extended the *Smith* reasoning to issues in matter of electronic communications.[163] The overwhelming trend among courts has been to find that individuals have no reasonable expectation of privacy when it comes to information voluntarily disclosed to an Internet Service Provider.[164]

For Fourth Amendment purposes, courts have considered email metadata to be analogous to telephone calls and to letters sent through the postal system.[165] The metadata the government collects through phone records and Internet communications is like the information that appears on mail covers, including the name and address of the addressee and of the sender, the postmark, and the class of mail, all of which is considered unprotected in Fourth Amendment terms.[166] This issue between what can be counted as protected information versus unprotected information is clarified in the content/envelope distinction.[167] Courts recognize that while a third party may have physical control over an individual's information, such control does not make all expectations of privacy unreasonable.[168] Rather only the information that the third party sees, like the address, is

160 *See* Newell, *supra* note 16.

161 Steagald v. United States, 451 U.S. 204, 219 (1981); *accord, e.g.*, Rakas v. Illinois, 439 U.S. 128, 133-34 (1978) ("Fourth Amendment rights are personal rights which . . . may not be vicariously asserted.").

162 White Paper, *supra* note 22, at 21.

163 *See* Memorandum from Kenneth L. Wainstein, Assistant Attorney General, Subject: Proposed Amendment to Department of Defense Procedures to Permit the National Security Agency to Conduct Analysis of Communications Metadata Associated with Persons in the United States, to the Attorney General, November 20, 2007 at 5, *available at* http://www.guardian.co.uk/world.interactive/2013/jun/27/nsa-data-collection-justice-department.

164 United States v. Skinner, 690 F.3d 772 (6th Cir. 2012); United States v. Lifschitz, 369 F.3d 173 (2d Cir. 2004) (reasonable expectation of privacy exists on home computers, but it is gone when it is transmitted over the internet or email and received by a third person); *see also* Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, 11 UCLA J. L. & TECH., no. 1, 2007.

165 *See* United States v. Charbonneau, 979 F. Supp. 1177 (S.D. Ohio 1997); United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996).

166 *See* United States v. Choate, 576 F. 2d 165 (9th Cir. 1978); United States v. DePoli, 628 F.2d 779 (2d. Cir. 1980); United States v. Huie, 593 F. 2d 14 (5th Cir. 1979); Vreeken v. Davis, 718 F. 2d 343 (10th Cir. 1983) (a mail cover which records information about the sender and recipient of a letter, is indistinguishable in any important respect from the pen register at issue in *Smith*).

167 *See* Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 611 L. 648, 676-678 (2002).

168 Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV., 1264, 1286 (2004) (explaining

unprotected, while the contents of the communication still remain hidden, are protected.

The content/envelope distinction further verifies the government's telephone and electronic metadata collection. The government is not looking at any of the contents of the email[169] or listening to the conversations of the phone call, or the content; rather, the government is in effect only collecting the unprotected "envelope" data from the surveillance—metadata.

II. The Mosaic Theory

There are two different, but similar ideas that are relevant to the mosaic theory concerning the NSA metadata collection program. First, there is the theory of intelligence gathering that is known as the "mosaic theory."[170] The "mosaic" is the overall picture that is put together by drawing inferences from seemingly disparate pieces of information.[171] An example of some of the pieces of information that would be used in intelligence gathering is the NSA's collection of metadata. It is studied and analyzed to extrapolate information about terrorists, and terrorist threats to national security.

The second "mosaic theory" that needs to be discussed is the mosaic theory of the Fourth Amendment. The mosaic theory was introduced in *United States v. Maynard*,[172] and although it has never explicitly been endorsed by the Supreme Court, the recent decision in the case of *United States v. Jones*[173] endorsed some form of the mosaic theory, although not per se. The mosaic theory of the Fourth Amendment comes from the same idea of the intelligence gathering theory of the mosaic theory. Put simply, the mosaic theory states that searches can be analyzed as a collective sequence of steps rather than as individual steps. Many non-searches packaged together as a collective entity become a search because the individual pieces of the puzzle that seem small in isolation could be assembled together like a mosaic to reveal the full picture of a person's life.[174]

The Supreme Court specifically limited its analysis in *Jones* to the trespass nature of a GPS on a car, and did not address the national security exception to the Fourth Amendment.[175] However, it is obvious that these two theories are essentially after the same thing, with drastically divergent implications for the metadata collection program. The whole idea behind the metadata program is to look for patterns, and deduce information that would be useful in preventing terrorism, producing a mosaic of the terrorists' activities. But court precedent has said that searches that reveal

---

"ECPA largely tracks the distinction made by the Court in *Smith v. Maryland*, between what Kerr calls 'envelope' and 'content' information. Analogizing to postal mail, Kerr states that 'the content information is the letter itself, stored safely inside its envelope. The envelope information is the information derived from the outside of the envelope, including the mailing and return addresses, the stamp and postmark, and the size and weight of the envelope when sealed.') (quoting Kerr, *supra* note 168, at 611-16).

169 *See* Lawless, *supra* note 165.

170 Michael P. Goodwin, *A National Security Puzzle: Mosaic Theory and the First Amendment Right of Access in the Federal Courts*, 32 Hastings Comm. & Ent. L. J. 179, 185 (2010).

171 *Id.*

172 United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).

173 United States v. Jones, 132 S. Ct. 945 (2012).

174 Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311, 325 (2012).

175 Jones, 132 S. Ct. at 945.

the mosaic of a person's life are in violation of the Fourth Amendment. Many scholars[176] dislike the mosaic approach to the Fourth Amendment and state that it is unworkable for future cases, since all detective work could be extrapolated to fit the mosaic theory if the right facts arose.

Clearly, the mosaic theory of the Fourth Amendment needs to be clarified in terms of national security and the overall theory of intelligence gathering. However, supposing that the mosaic theory were to apply, inferring that the metadata collection being done by the NSA was a search under the Fourth Amendment, it would be overcome by one of two things.

First, the FISA court issues orders allowing the surveillance and reviewing the evidence just like in a warrant application. While the standards are different for FISA issues and for regular criminal issues, the FISC order essentially has the protection of a warrant because of the nature of the FISC oversight.

Secondly, even if the NSA collection program were to fall under the meaning of a search under the mosaic theory, and the FISC order was not considered a sufficient national security warrant, the court would then have to go through the standard balancing act of the Fourth Amendment. That standard requires a balancing of "the promotion of legitimate Governmental interest against the degree the search intrudes upon an individual's privacy."[177] If any Fourth Amendment privacy interest were implicated in the collection of telephony metadata it would be limited, and is severely outweighed by the public interest of the prevention of terrorist attacks. The telephony metadata is a forward-looking prevention of the loss of life, including potentially on a catastrophic scale, as opposed to "ordinary crime solving"[178] which is a regressive attempt to solve or prevent future crimes. Given the important objective and the minimal, if any, Fourth Amendment intrusions that the telephony metadata collection program entails, the program would be constitutional even if the Fourth Amendment's reasonableness standard applied.[179]

III. Conclusion

> "Let me start by saying that I would much rather be here today debating this point than trying to explain how we failed to prevent another 9/11. It is a testament to the ongoing teamwork of the Central Intelligence Agency, The Federal Bureau of Investigation and the National Security Agency, working with our allies and then industry partner, that we have been able to connect the dots and prevent more terrorist attacks." [180]

General Alexander's statement to the House Committee On Intelligence resonates deeply. The Snowden leaks exposed many of the secret activities of our government, the activities that

176 *See generally* Kerr, *supra* note 175; Goodwin, *supra* note 171; *see also*, Benjamin M. Ostrander, *The Mosaic Theory and Fourth Amendment Law*, 86 Notre Dame L. Rev. 1733 (2011).

177 Maryland v. King, 133 S. Ct. 1958, 1970 (2013).

178 *Id.* at 1982 (Scalia, J., dissenting).

179 White Paper, *supra* note 22, at 21.

180 June 18, 2013 HPSCI Hearing, *supra* note 21 (statement of General Keith Alexander).

are put in place to keep us safe and protect our civil liberties, not take them away. The media has run rampant with claims of the Government listening to Americans' phone calls, reading emails, and tracking the Internet history of thousands upon thousands of innocent Americans, without warrants, violating the very freedom that the Government should be protecting. But upon deep examination of the documents leaked, the media's messages flounder.

The documents show extensive procedures and policies put in place by the Intelligence Community to protect American's information. They show the oversight and checks and balances of our government. The documents show that while the idea of the Government having access to the telephony metadata of Americans is uncomfortable, it is necessary for the protection of America against the evolving world of international terrorism.

While the continued disclosures from the *Guardian* and Snowden continue to make Americans feel uncomfortable or 'itchy' it is important to remember that technology and FISA surveillance is something that we will have to learn to live with, just like the bomb. It may not be easy, but it has not killed us yet.