2015

Government Secrets: The Public's Misconceptions of the Snowden Disclosures

Melanie M. Reid, *Lincoln Memorial University - Duncan School of Law*

Government Secrets:
The Public's Misconceptions of the Snowden Disclosures

by Melanie Reid*

"Secrets, silent, stony sit in the dark palaces of both our hearts: secrets weary of their tyranny: tyrants willing to be dethroned."

--James Joyce

I. Introduction

Human beings are curious by nature. We love to ask the "why" questions and would rather be privy to a secret than be kept in the dark. Not surprisingly, government conspiracy theories are quite popular.[1] It is much more interesting to think part of the government was somehow involved in the assassination of President John F. Kennedy rather than believe the lone gunman theory, or that the government is covering up an alien invasion by storing UFOs and alien bodies at Area 51 in Roswell rather than believe no such thing exists.[2]

Thus, when Edward Snowden revealed that one of the government's most secretive agencies, the National Security Agency ("NSA"), previously nicknamed "No Such Agency," was keeping a huge secret from the American people and monitoring American citizens' phone calls, instant messaging, emails, documents kept in the "cloud," contact lists, metadata[3], GPS data, etc., this became one of the greatest government conspiracy theories to contemplate since JFK and Roswell.

Is the NSA listening to my phone call right now? What if I say the word "president" or "al Qaeda," would they be definitely listening then? Or what if I "Google" one of these words? Would the NSA instantly watch what websites I am viewing?

Of course, it would be extremely difficult to keep such a large-scale government conspiracy under wraps. It seems surprising that any top-secret classified government operation is kept a secret. Ben Franklin's famous quote, "Three may keep a secret, if two of them are dead,"[4] might sound melodramatic but it rings true. Not much is kept secret anymore – in fact, there appears to

---

* Associate Professor of Law, Lincoln Memorial University-Duncan School of Law. I would like to thank Lauren Mullins for her invaluable research assistance, enthusiasm, thoughts and critiques on this topic.

[1] JFK (Warner Bros. 1991) (US Gross Box Office = $70,405,498) http://www.imdb.com/title/tt0102138/business?ref_=tt_dt_bus; CONSPIRACY THEORY (Warner Bros. 1997) (US Gross Box Office = $76,081,498) http://www.imdb.com/title/tt0118883/business?ref_=tt_dt_bus.

[2] Journalist Annie Jacobsen surmised that the UFOs and aliens found in Roswell, Nevada in 1947 were actually Russian children around 12-years-old with large heads and abnormally shaped, over-sized eyes that were the genetic experiments of Josef Mengele, a former German Nazi officer and physician in Auschwitz. ANNIE JACOBSEN, AREA 51: AN UNCENSORED HISTORY OF AMERICA'S TOP SECRET MILITARY BASE 2011. Soviet leader Joseph Stalin wanted to cause hysteria in America with the thought of "UFOs and an alien invasion." *Id.*

[3] Metadata, or transactional information, is collected as phone calls "are handed over, as is location data, call duration, unique identifiers, and the time and duration of all calls. The contents of the conversation itself are not covered." Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN, June 5, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. The courts interpret the "business records" provision of the PATRIOT Act (50 U.S.C. § 1861 (2014)) as legal justification for bulk collection of domestic telephone records. *Id.*

[4] Benjamin Franklin, *Poor Richard's Almanack* (1735), *available at* http://www.vlib.us/amdocs/texts/prichard35.html. A student of mine recently informed me this is also the theme to a show entitled, "Pretty Little Liars."

be more and more disclosures as spies, whistleblowers, journalists, and insiders begin to share their knowledge and spread it throughout the internet. The public clamors that it has a need-to-know in order to keep the government in check.

But what is it that we need to know? Do we need to know the specifics as to how individual NSA collection programs work? Should the public know which communication methods are being intercepted by the NSA and thus compromised, or what foreign embassies and consulates are being surveilled both inside and outside of the U.S., or how electronic beacons are implanted within targeted electronic devices, or how the NSA taps into the telecommunications of service providers, or know about U.S. collection priorities against foreign countries?

Once the initial reporting on the Snowden leak began in June 2013, the media and public wanted to know more – what was the NSA collecting, what were they listening to, what were they doing with this information, who are they sharing this information with? The actual legalities and illegalities of certain NSA programs and collection of data became more blurred as the media focused on the wide-scale public outrage at the idea that the government was spying on its own citizens regardless of the legalities. The media emphasized the public's ever-increasing distrust of government and the intelligence community's (IC)[5] classified programs.

Now that the initial deluge of classified information from Snowden's leaks has been disclosed, the questions are two-fold: (1) are these expansive collection programs by the IC legal or illegal and (2) if legal, are these "whistleblower" disclosures justified given the resultant damage these leaks have caused to our national security and law enforcement's ability to prevent the commission of future crimes?

II. Legality of IC's Actions

What is difficult to determine from the recent media disclosures is what exactly is being collected, how is the information collected, at what point can communications be accessed and analyzed, who receives the analysis, and what is the legal justification for each step along this process. There is a significant distinction between authorizations to collect telephone caller identification record information, or "to" and "from" information on a particular email address, versus authorization to listen in on the content of such communications. If this distinction is not made clear, then the public can draw erroneous conclusions about alleged breaches of privacy based upon misinformation.

A. NSA's Bulk Collection of Metadata: Section 215

Snowden disclosed that the NSA is collecting the metadata from millions and even billions of phone calls and emails sent out every day, including Americans' emails and phone calls.[6] Metadata includes "much of the information that appears on a customer's telephone bill: the date

---

[5] "The Intelligence Community (IC) is a group of Executive Branch agencies and organizations that work separately and together to engage in intelligence activities that are necessary for the conduct of foreign relations and the protection of the national security of the United States." OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, U.S. NATIONAL INTELLIGENCE: AN OVERVIEW 7 (2011), *available at* http://www.dni.gov/files/documents/IC_Consumers_Guide_2011.pdf. Sixteen United States intelligence agencies comprise the IC and are under the Office of the Director of the National Intelligence: the Central Intelligence Agency, the National Security Agency, the Defense Intelligence Agency, the National Reconnaissance Office, the National Geospatial-Intelligence Agency, the Federal Bureau of Investigation (FBI) National Security Branch, the Drug Enforcement Administration (DEA) Office of National Security Intelligence, Department of Treasury Office of Intelligence and Analysis, Department of Energy Office of Intelligence and Counter-intelligence, State Bureau of Intelligence and Research, Department of Homeland Security Office of Intelligence and Analysis, and Army, Air Force, Coast Guard, Marine Corps, and Naval Intelligence. *See id*. at 9.

[6] GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE 30-32 (2014).

and time of a call, its duration, and the participating telephone numbers" and can include the nature of "how the call was routed from one participant to the other through the infrastructure of the telephone companies' networks."[7]

The NSA was given this power when the PATRIOT Act was passed post 9/11.[8] Section 215 of the Act allows the government to obtain a Foreign Intelligence Surveillance Court (FISC or FISA court) order every ninety days requiring third parties (including telecommunications providers) to hand over any records or other "tangible thing" if deemed "relevant" to "any investigation to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities."[9]

The NSA utilized this "Access to Certain Business Records for Foreign Intelligence and International Terrorism Investigations" power to justify their bulk telephone records collection program.[10] The NSA began to collect metadata from all sorts of third parties, including telecommunications carriers and internet providers, in order to have the information close at hand when it came time to conduct a targeted search.[11] The NSA stores these collected telephone records in a centralized database.[12] Before an analyst can access the database and search for a specific number or selection term, "one of twenty-two designated NSA officials must first determine that there is a reasonable, articulable suspicion that the number is associated with terrorism."[13] Once the analyst gains approval, he or she "may run queries that will return the calling records for that seed [number], and permit 'contact chaining' to develop a fuller picture of the seed's contacts. Contact chaining enables analysts to retrieve not only the numbers directly in contact with the seed number ("the first hop"), but also numbers in contact with all first hop numbers (the "second hop"), as well as all numbers in contact with all second hop numbers (the "third hop")."[14]

The government's argument is that one cannot investigate and prevent terrorist attacks without real-time access to metadata to determine who is contacting whom and when. "When the NSA identifies communications that may be associated with terrorism, it issues intelligence reports to other federal agencies, such as the FBI, that work to prevent terrorist attacks."[15] It is difficult to predict when attacks may occur, even more so if one hand is tied behind the IC's back when not given the ability to follow a target's phone number trail wherever that might lead.

---

[7] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 8, 21 (Jan. 23, 2014) [hereinafter PCLOB TELEPHONE RECORDS REPORT], *available at* http://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.

[8] *Id.*

[9] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, sec 208(1), Pub. L. No. 107-56, 115 Stat. 272 [hereinafter PATRIOT Act] (codified in scattered titles of U.S.C.), *available at* http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf., at sec. 215. *See also* BRENNAN CENTER FOR JUSTICE, ARE THEY ALLOWED TO DO THAT? A BREAKDOWN OF SELECTED GOVERNMENT SURVEILLANCE PROGRAMS 1 http://www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf.

[10] PCLOB TELEPHONE RECORDS REPORT, *supra* note 7, at 8.

[11] BRENNAN CENTER FOR JUSTICE, *supra* note 9, at 1-2.

[12] PCLOB TELEPHONE RECORDS REPORT, *supra* note 7, at 8.

[13] *Id*. at 8-9.

[14] *Id*. at 9.

[15] *Id*. at 8.

Critics of section 215 argue that by permitting intelligence agencies, specifically the NSA, to collect metadata from a variety of third parties, section 215 allows the government to get a whole picture of a person by searching one's "financial, library, travel, video rental, phone, medical, church, synagogue, and mosque records . . . providing the government says it's trying to protect against terrorism."[16] Metadata, "if properly exploited, could yield more valuable information than recordings of the phone calls or email messages themselves."[17]

Critics further argue that "[i]t is difficult to believe that the phone records of millions of Americans are actually 'relevant' to a specific terrorist or foreign intelligence investigation. Nor does Section 215 appear to allow the government to collect first and determine relevance later, which is what the government claims it is doing."[18]

In January 2014, the Privacy and Civil Liberties Oversight Board (PCLOB)[19] issued a report after reviewing the NSA's bulk collection of phone records. The PCLOB found that the bulk collection of phone records failed to comply with Section 215 and therefore should be terminated or significantly revised.[20] The PCLOB determined that (1) the bulk telephone records acquired had "no connection to any specific FBI investigation at the time of their collection;" (2) since the records are collected in bulk, they are not "relevant" to a particular investigation as required under section 215; (3) requiring telephone companies to furnish new call records on a daily basis is not permitted under section 215 nor FISA; and (4) section 215 only permits the FBI and not the NSA to obtain records relevant to a terrorism or foreign intelligence investigation.[21]

That same month, President Obama made his own comments regarding the section 215 program, stating that he would continue to allow government use of bulk phone records while they attempt to come up with an alternative solution "without the government holding this metadata itself" and would require the agency to get court approval prior to accessing the metadata.[22] The NSA would also no longer be able to access records that go beyond two persons removed from the original query.[23]

In response to these findings, in May 2014, the House passed the USA Freedom Act[24] which focuses on the NSA's call-records program in which the agency retains billions of records for all phone calls made from or to the United States. Under the legislation, telecommunications companies would retain those records, and the NSA would only have access to specific information about targeted individuals under court orders.[25] A year later, due to inaction by the

---

[16] Emma Roller, *This Is What Section 215 of the Patriot Act Does*, SLATE (June 7, 2013, 1:17 PM), http://www.slate.com/blogs/weigel/2013/06/07/nsa_prism_scandal_what_patriot_act_section_215_does.html.

[17] SHANE HARRIS, THE WATCHERS: THE RISE OF AMERICA'S SURVEILLANCE STATE 204-05 (Penguin Books, 2011).

[18] BRENNAN CENTER FOR JUSTICE, *supra* note 9, at 3.

[19] The Privacy and Civil Liberties Oversight Board (PCLOB) was established in 2004 by the Intelligence Reform and Terrorism Prevention Act of 2004. In 2007, the 9/11 Commission Act restructured the Board requiring that all five members be appointed by the President. *See* 42 U.S.C.A. § 2000ee (2012 & Supp. 2014). As a result, the Board did not fully exist until June 2013, after the Senate confirmed members to resume operations. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, http://www.pclob.gov/about-us (last visited Aug. 23, 2014).

[20] PCLOB TELEPHONE RECORDS REPORT, *supra* note 7, at 10.

[21] *Id*.

[22] Transcript of President Obama's Jan. 17 Speech on NSA Reforms, WASHINGTON POST, Jan. 17, 2014, http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html.

[23] *Id*.

[24] USA Freedom Act, H.R. 3361, 113th Cong. (2013-2014), *available at* https://beta.congress.gov/bill/113th-congress/house-bill/3361.

[25] *Id*. The bill "[r]equires the FBI to include in such tangible thing applications a specific selection term to be used as the basis for such production." *Id*. A "specific selection term" is "a term specifically identifying a person, entity,

Senate, the bulk collection program under section 215 was allowed to expire on June 1, 2015.[26] The Senate then approved the USA Freedom Act on June 2nd, and the revised Section 215 program which effectively eliminates bulk collection will continue until December 15, 2019.[27]The USA Freedom Act allows the bulk collection of telephone metadata for only a 180 day transition period (until November 29, 2015) during which such collection could continue.[28]

B. NSA's Monitoring of Conversations: FISA and Section 702

Section 215 of the PATRIOT Act addresses the bulk collection of telephone records, and the FISA Amendments of 2008 (FAA) address the collection and subsequent analysis of the content of telephone and internet communications.[29] The FAA (also known as section 702) has been utilized to allow the NSA to work with electronic communication service providers "to copy, scan, and filter internet and phone traffic coming through their physical infrastructure" and compel the disclosure of the content of such communications so long as it targets foreign persons reasonably believed to be located outside the United States.[30] No particular warrant is required in that instance. The targeting of the non-U.S. person on foreign soil must be conducted in order to acquire foreign intelligence information as defined in FISA, and the NSA must obtain approval from the FISA court as to their targeting and minimization procedures prior to collection to make sure U.S. persons are not inadvertently intercepted.[31]

---

account, address, or device" that is "used by the government to limit the scope of the information or tangible things sought pursuant to the statute." *Id*. In each application requesting call detail records (i.e., telephone numbers and time or duration of a call), the FBI must show "(1) reasonable grounds to believe that the call detail records sought to be produced based on the specific selection term are relevant to such investigation; and (2) facts giving rise to a reasonable, articulable suspicion that such specific selection term is associated with a foreign power or an agent of a foreign power." *Id*.

[26] Opinion and Order *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, Docket No. BR 15-75, Foreign Intelligence Surveillance Court, June 29, 2015 at 2. *See also* Erin Kelly, *Here's what happens now that the Patriot Act Provisions Expired*, USA Today, June 1, 2015, http://www.usatoday.com/story/news/nation/2015/05/31/patriot-act-expires-senate-stalemate/28260905/.

[27] Opinion and Order *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, Docket No. BR 15-75, Foreign Intelligence Surveillance Court, June 29, 2015 at 2-3 (citing to USA FREEDOM Act § 705(a)).

[28] Opinion and Order *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, Docket No. BR 15-75, Foreign Intelligence Surveillance Court, June 29, 2015 at 10-11 (citing to section 109(a) of the USA FREEDOM Act).

[29] H.R. 6304, 110th Cong. (2007-2008), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-110hr6304enr/pdf/BILLS-110hr6304enr.pdf.

[30] ELECTRONIC FRONTIER FOUNDATION, COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION REGARDING SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE AMENDMENTS ACT TO THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD 8 (Apr. 22, 2014), *available at* https://www.eff.org/files/2014/04/22/eff_pclob_comments_11_april_2014.pdf; *See also* H.R. 6304, 110th Cong. (2007-2008), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-110hr6304enr/pdf/BILLS-110hr6304enr.pdf.

[31] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 6 (July 2, 2014) [hereinafter PCLOB SECTION 702 REPORT], *available at* https://www.nsa.gov/civil_liberties/_files/pclob_section_702_report.pdf. "The targeting procedures govern how the executive branch determines that a particular person is reasonably believed to be a non-U.S. person located outside the United States, and that targeting this person will lead to the acquisition of foreign intelligence information. The minimization procedures cover the acquisition, retention, use, and dissemination of any non-publicly available U.S. person information acquired through the Section 702 program." *Id*. at 6-7. "For example, the NSA's minimization procedures require that queries of Section 702-acquired information be designed so that they are 'reasonably likely to return foreign intelligence information.'" *Id*. at 8.

Unfortunately, it is virtually impossible to separate the collection of phone and internet communications of strictly foreign persons from U.S. persons if the foreign person is communicating with a U.S. person.[32] These communications are also potentially being copied and stored in a searchable database.[33] Information on U.S. persons may incidentally be collected if that U.S. person communicates with a non-U.S. person that is being targeted or two non-U.S. persons discuss the U.S. person.[34] Or, a U.S. person's conversation may inadvertently be collected by mistake if erroneously targeted by the NSA and thought to be a non-U.S. person.[35] In the case of inadvertent collection, the communications must be destroyed.[36]

The Privacy and Civil Liberties Oversight Board (PCLOB) approved of the Section 702 program in its report dated July 2, 2014, stating:

> [t]he Section 702 program has enabled the government to acquire a greater range of foreign intelligence than it otherwise would have been able to obtain – and to do so quickly and effectively. Compared with the "traditional" FISA process under Title I of the statute, Section 702 imposes significantly fewer limits on the government . . . [t]he program has proven valuable in the government's efforts to combat terrorism as well as in other areas of foreign intelligence. . . . [m]onitoring terrorist networks under Section 702 has enabled the government to learn how they operate, and to understand their priorities, strategies, and tactics.[37]

While the core of the section 702 program was deemed to be "reasonable" under Fourth Amendment law, the PCLOB set forth additional proposals to address their concerns about

> the unknown and potentially large scope of the incidental collection of U.S. persons' communications, the use of "about" collection to acquire Internet communications that are neither to nor from the target of surveillance, and the use of queries to search for the communications of specific U.S. persons within the information that has been collected.[38]

On June 19, 2014, the House passed a bill that includes an amendment which bars the NSA, the CIA, and others in the IC from actually examining the communications of Americans that were collected into databases created to target foreigners.[39] Critics have called this

---

[32] JAMES BAMFORD, THE SHADOW FACTORY: THE ULTRA-SECRET NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA 304 (Anchor Books, 2009).
[33] *Id.*
[34] PCLOB SECTION 702 REPORT, *supra* note 28, at 6.
[35] *Id.*
[36] *Id.*
[37] *Id.* at 9-10.
[38] PCLOB TELEPHONE RECORDS REPORT, *supra* note 7, at 9.
[39] H.R. 5016, 113th Cong. (2013-2014), *available at* https://beta.congress.gov/bill/113th-congress/house-bill/5016/amendments.

technique the "backdoor search loophole."[40] "The bill also prohibits the government from requiring a private company to alter its software to allow clandestine surveillance."[41]

C. Legal Conclusions as to IC Actions

In summary, upon review of FISA, the FAA, and the PATRIOT Act, it would be lawful for the NSA to monitor electronic communications of foreign persons reasonably believed[42] to be located overseas without any type of warrant. However, if that person is a "U.S. person" or that foreign person was to communicate with a person located in the United States, the NSA would need to apply for a FISA warrant. The difficulty is in determining where the particular person is located at the time of the call. While the law does not allow the intentional monitoring of U.S. persons, the FISC approves minimization procedures to limit the amount of information about U.S. persons that is intercepted, retained, and disseminated. Hence, the IC's monitoring of content in communications is legal.

On the other hand, the legality of the NSA's collection of metadata is uncertain. While the NSA has previously used section 215 of the PATRIOT Act to justify its bulk records collection program,[43] it is clear that the NSA has been collecting more than foreign persons' metadata and metadata not necessarily relevant to a terrorism or foreign intelligence investigation.[44] Regardless, the bulk data collection of business records and other tangible things, as we know it, will terminate after November 29, 2015.[45]. After such date, the IC will have to furnish "specific selection term[s]" to the FISC before being granted access to such metadata from third party communications providers.[46] However, at the time of the Snowden leak, both the monitoring of content and the bulk records collection program were legally justified.

III. Snowden's Reasons for Disclosure versus Damage Done to National Security

A. Bulk Collection and Keeping the Internet "Free"

Snowden's real complaint seems to boil down to the NSA's collection of metadata – not the subsequent analysis of this data because targeting and minimization procedures have been put in place to avoid bulk *analysis* of the data collected. Therefore, Snowden is concerned about

---

[40] Charlie Savage, *House Votes to Curb N.S.A. Scrutiny of Americans' Communications*, NY TIMES (June 20, 2014), http://www.nytimes.com/2014/06/21/us/politics/house-votes-to-curb-nsa-scrutiny-of-americans-communications.html.

[41] Andrew Rosenthal, *The House Actually Did Something About Warrantless Surveillance*, TAKING NOTE: THE EDITORIAL PAGE EDITOR'S BLOG (June 20, 2014, 1:30 PM), http://takingnote.blogs.nytimes.com/2014/06/20/the-house-actually-did-something-about-warrantless-surveillance/.

[42] "[T]he NSA has reportedly interpreted that to mean that it need only ensure '51 percent confidence of the target's 'foreignness.'" BRENNAN CENTER FOR JUSTICE, *supra* note 9, at 3; *See also* Barton Gellman & Laura Poitras, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, WASHINGTON POST (June 6, 2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

[43] 50 U.S.C.A. § 1861(a)(1) (2003 & Supp. 2014).

[44] Barton Gellman et al., *In NSA-intercepted data, those not targeted far outnumber the foreigners who are*, WASHINGTON POST (July 5, 2014), http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html?hpid=z1.

[45] Opinion and Order *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, Docket No. BR 15-75, Foreign Intelligence Surveillance Court, June 29, 2015 at 18.

[46] Opinion and Order *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, Docket No. BR 15-75, Foreign Intelligence Surveillance Court, June 29, 2015 at 10 (citing to USA FREEDOM Act § 103(b), amending FISA § 501(c)).

the *potential* for abuse in the collection of metadata not necessarily current abuse of power now that this data is in the hands of the NSA.

Snowden has given several interviews and written manifestos explaining why the public needs to know the specifics as to what the NSA is collecting and how they are collecting it. In Snowden's eyes, only with the public's input can true regulation and accountability take place.[47] Apparently, congressional oversight committees, the FISC, the Department of Justice, internal agency auditing and monitoring, and oversight from the Executive branch is not enough. It bears reminding that the previously described collection and surveillance programs are regulated – by Congress, by the FISC, by the Department of Justice and by oversight lawyers within intelligence agencies themselves.[48]

Snowden wants to keep the internet free from NSA collection – so that those who grow up on the internet feel free to explore, make mistakes, and express themselves without fear that anyone is watching.[49] Unfortunately, regardless of whether the NSA is watching, others are and will always be watching. Private companies make it their mission to collect as much information as possible on individual consumers and sell it to the highest commercial bidder. Criminals both overseas and in our own back yard who want to steal our information are monitoring and exploiting the Internet as well. Director of the FBI, James Comey, recently stated,

> I think there's something about sitting in front of your own computer working on your own banking, your own health care, your own social life that makes it hard to understand the danger (of third party surveillance, cybercrime, and cyber-attacks on companies and individuals on the internet). I mean, the Internet is the most dangerous parking lot imaginable. But if you were crossing a mall parking lot late at night, your entire sense of danger would be heightened. You would stand straight. You'd walk quickly. You'd know where you were going. You would look for light. Folks are wandering around that proverbial parking lot of the Internet all day long, without giving it a thought to whose attachments they're opening, what sites they're visiting. And that makes it easy for the bad guys.[50]

The Internet, unfortunately, will never be free from surveillance. Even if our government is not monitoring the Internet, there will always be a myriad of bad actors that do. Foreign Intelligence Services target the Internet to collect positive intelligence and steal trade secrets, cyber criminals hack into our private e-mails and steal personal identification information, terrorist organizations promote jihad and the destruction of our cyber infrastructure.

---

[47] GREENWALD, *supra* note 6, at 13, 30-31.

[48] At a recent debate, former CIA director James Woolsey stated,

> I have seen, either from in the Executive Branch, or as a private citizen interested in these issues and following them, the oversight personnel capabilities, numbers of offices, numbers of people involved in overseeing the American system of intelligence is truly awesome. There is no country anywhere in the world that has the massive oversight from legislative, judicial, and executive sides and functions over their intelligence systems. Nobody is even close to the United States.

Transcript of INTELLIGENCE SQUARED U.S. debate, *Snowden was justified*, (Feb. 12, 2014), *available at* http://intelligencesquaredus.org/images/debates/past/transcripts/021214%20Snowden.pdf.

[49] GREENWALD, *supra* note 6, at 46-47.

[50] Transcript of Interview by Scott Pelley with James Comey, Oct. 5, 2014, *available at* http://www.cbsnews.com/news/fbi-director-james-comey-on-threat-of-isis-cybercrime/

More importantly, do we want our government to be proactive and attempt to prevent or disrupt terrorist attacks before they take place? If the answer is yes, then we need to provide federal law enforcement with a requisite amount of surveillance tools to be able to accomplish this mission.

B. Bulk Collection and the *Potential* for Abuse of Power

Snowden's argument for public disclosure would be much stronger if he could point to specific abuses of power that would liken current NSA activities to those abuses disclosed in the 1970's during the Church Committee hearings. The Church Committee discovered that the IC had illegally gathered information and compiled files on communists in the 1950s and civil rights groups and Vietnam War protesters in the 1960s.[51] These findings resulted in a significant overhaul in IC oversight and accountability and the passage of the Foreign Intelligence Surveillance Act (FISA) of 1978 in order to prevent future abuse of power by the IC.[52]

In addition to his concerns about NSA spying on Americans through its bulk collection programs, Snowden also disclosed examples of individual government employees who abused the power and responsibility placed in their hands. This abuse of power was illegal, and the offenders should have faced criminal or severe administrative penalties, but their behavior in many instances was either condoned or overlooked. In one article, Snowden is quoted as saying,

> Many of the people searching through the haystacks were young, enlisted guys, 18 to 22 years old. They've suddenly been thrust into a position of extraordinary responsibility, where they now have access to all your private records. In the course of their daily work, they stumble across something that is completely unrelated in any sort of necessary sense – for example, an intimate nude photo of someone in a sexually compromising situation. But they're extremely attractive. So what do they do? They turn around in their chair and they show a co-worker. And their co-worker says, "Oh, hey, that's great. Send that to Bill down the way," and then Bill sends it to George, George sends it to Tom, and sooner or later this person's whole life has been seen by all of these other people. The analysts don't discuss such things in the NSA cafeterias, but back in the office anything goes, more or less. You're in a vaulted space. Everybody has sort of similar clearances, everybody knows everybody. It's a small world. It's never reported, because the auditing of these systems is incredibly weak. The fact that records of your intimate moments have been taken from your private communication stream, from the intended recipient, and given to the government, without any specific authorisation, without any specific need, is itself a violation of your rights. [When asked how often do such things happen?] . . . I'd say probably every two

[51] UNITED STATES SENATE, *Senate History: January 27, 1975 Church Committee Created*, http://www.senate.gov/artandhistory/history/minute/Church_Committee_Created.htm.

[52] Foreign Intelligence Surveillance Act of 1978, Pub.L. 95-511, 92 Stat. 1793 (codified at 50 U.S.C. §§ 1801 to 1811 (2014)).

> months. It's routine enough. These are seen as sort of the fringe benefits of surveillance positions.[53]

Everyone would agree that NSA analysts should not be opening private email attachments that contain naked photos (or any non-foreign intelligence related material for that matter) and sending them to their colleagues. This is illegal and there should be repercussions. But was this sort of childish behavior on the part of some immature analysts worth the damage done to our nation's security due to Snowden's disclosures?

Other reasons as to why Snowden made such disclosures include: (1) disgust over CIA operatives who would get targets drunk enough to land in jail and then bail them out in order to recruit an asset,[54] (2) Clapper lying in a congressional hearing about whether the NSA collects data on Americans,[55] (3) military and CIA drones and targeted killings,[56] (4) outrage over the NSA's "ability to map the movement of everyone in a city by monitoring their MAC address, a unique identifier emitted by every cell phone, computer, and other electronic device,"[57] (5) NSA's access to email and other Internet traffic from Syria during the civil war,[58] (6) the NSA's building of a Massive Data Repository where "billions of phone calls, faxes, emails, computer-to-computer data transfers, and text messages from around the world [would] flow through the MDR every hour,"[59] and (7) the NSA's access to virtually all private communications coming in from overseas to people in the US in order to "identify these malicious traffic flows and respond to them."[60]

Again, the resounding concern is collection, and the fact that the public is not told about the mass collection. As mentioned, some of Snowden's complaints had nothing to do with bulk collection. Snowden did have a list of individual government employees whose actions merited administrative action and reprimand, but their specific activity did not undermine the legality or wisdom of the programs which Snowden was actually railing against. Snowden has certainly been successful at opening the dialogue as to bulk collection – as everyone is now discussing collection, how to reform or eliminate section 215, and how to move collection from government's hands to a third party.[61]

Transparency is important to a certain degree. It keeps the government honest and it ensures the public can keep tabs on the checks and balances that are put in place to ensure abuse does not occur. But too much transparency defeats the very purpose of clandestine intelligence operations in the first place, i.e., to protect the American public and keep the bad guys in the dark

---

[53] Alan Rusbridger & Ewan Macaskill, *I, spy: Edward Snowden in exile*, THE GUARDIAN, July 19, 2014, http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-interview-rusbridger-macaskill.

[54] James Bamford, *The most wanted man in the world*, WIRED, June 13, 2014, http://www.wired.com/2014/08/edward-snowden/.

[55] At a congressional hearing on March 12, 2014, Senator Ron Wyden asked Director of National Intelligence James Clapper, "Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?" Clapper responded, "No sir . . . not wittingly." Fred Kaplan, *Fire James Clapper*, SLATE, June 11, 2013, http://www.slate.com/articles/news_and_politics/war_stories/2013/06/fire_dni_james_clapper_he_lied_to_congress_about_nsa_surveillance.html.

[56] Bamford, *supra* note 49.

[57] *Id.*

[58] *Id.*

[59] *Id.*

[60] *Id.*

[61] Would a third party's (telecommunications company) employees perform better than government employees and abuse their power much less than government employees that undergo background checks and significant vetting before being granted top secret clearances?

as to our intentions and capabilities. The general public has already been informed as to the purpose and mission of the NSA, plus a vague description of NSA collection platforms and capabilities is readily available. Once you delve into the details such as specific methods and sources, and the identities of certain targets, then this information becomes sensitive and classified, and as such, should be available to only those who are trusted and have a legitimate need to know. It may be advisable to have an open discussion on collection but there is no need to go into details that are classified, since such disclosures could cause harm to national security. Whistleblowers certainly need to step forward to discuss abuse within the system, especially when these failures are not being addressed by oversight committees within or outside the IC agencies. Certainly, on an individual level, when government analysts are caught monitoring calls and opening attachments that are not relevant to an authorized investigation, these people need to be brought to the attention of that agency's internal security team. However, there are multiple administrative layers of authority, policy review officials and security personnel available to anyone concerned who earnestly wants to report wrong doing or illegal activity.

One concern raised by Snowden is the allegation that the NSA "has been gathering records of online sexual activity and evidence of visits to pornographic websites as part of a proposed plan to harm the reputations of those whom the agency believes are radicalizing others [to become devoted to the jihadist cause] through incendiary speeches."[62] The six "radicalizers" known to be targeted by the NSA were Muslim and all are believed to be currently residing outside the United States though one has been described as a U.S. person.[63] Snowden argued in a recent interview that that type of surveillance and individual targeting may easily find its way into U.S. politics, and these tactics could be used to spy on the pornography-viewing habits of political opponents.[64] However, there is no evidence to suggest that giant leap has been made, and this type of slippery slope is exactly what oversight committees, supervisors, and government lawyers, need to monitor, and prevent any subsequent abuse of power.[65]

The United States Intelligence Community including the NSA collects foreign political, economic and military intelligence in order to provide U.S. policy makers with the necessary information to make the proper decisions in order to protect our national security and promote America's best interests both at home and abroad. To accomplish this goal, the IC, within certain legal limits needs to have access to every conceivable intelligence collection technique. The moral and ethical use of these tools, the potential benefits and possibility for abuse, the advisability and public acceptance for these techniques, are questions and discussions best left to the three branches of our government, and the public, to a more limited extent, to iron out.

IV. The Damage Done

Chairman of the Foundation for Defense of Democracies and former Director of the CIA, James Woolsey, during a recent debate on whether Snowden was justified, described four

---

[62] Glenn Greenwald, Ryan Grim, & Ryan Gallagher, *Top Secret Document Reveals NSA Spied on Porn Habits as Part of Plan to Discredit 'Radicalizers'*, HUFFINGTON POST, Nov. 26, 2013, http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html.

[63] *Id.*

[64] Bamford, *supra* note 49.

[65] For example, it was reported that CIA officers searched the computers of congressional staff while they prepared a Senate Intelligence Committee report on the CIA's detention and interrogation program. The CIA's inspector general investigated the matter and sent a criminal referral to the DOJ for further investigation. Mark Mazetti & Carl Hulse, *Inquiry by C.I.A. Affirms It Spied on Senate Panel*, N.Y. TIMES, July 31, 2014, http://www.nytimes.com/2014/08/01/world/senate-intelligence-commitee-cia-interrogation-report.html?_r=0. This is exactly what needs to be done when abuse of power is suspected.

programs which have been compromised due to the disclosures: (1) pre-Snowden, the IC had learned how to counter Chinese cyber-attacks by sending their malware back to the hackers after making some adjustments and creating problems for them; Snowden's disclosures explained how the U.S. was able to do this; (2) pre-Snowden, the IC was able to read emails and early stage drafts of emails of the Islamic State of Iraq; Snowden's disclosures allowed the terrorist group to learn of this; (3) pre-Snowden, the Defense Department had technology that allowed soldiers and CIA operatives to know whether they were being followed; post-Snowden, this technology has been shared with our adversaries; and (4) pre-Snowden, the U.S. learned how to penetrate the communication networks in some Latin American countries of some of the worst organizations and groups that are selling women, principally women into sexual slavery; post-Snowden those sex trafficking organizations now know which communication networks are compromised.[66]

Any time a government employee or unauthorized person reveals sources and methods used by law enforcement or the IC, this disclosure allows criminals, spies, and terrorists alike to minimize their risk of getting caught by taking countermeasures. When FBI Director Comey reveals that "the emergence of default encryption settings and encrypted devices and networks" will "leave law enforcement in the dark" and then names the specific companies building these devices, the concern is that criminals will use these loopholes to avoid detection.[67] The protection of sources and methods is critical to curtail illegal activity.

Perhaps the exposure of specific programs, sources, and methods is not the only problem, since there is now the dilemma or revelation of what was not disclosed, what does not exist, which indirectly underscores NSA limitations. In other words, if all of NSA's programs are disclosed, theoretically everything that was not revealed does not exist. NSA surveillance capabilities would be limited to the techniques exposed by Snowden and others. Criminals and terrorists alike have typically displayed signs of paranoia believing that IC capabilities approach the levels of those depicted in science fiction, and some adversaries are concerned that their every move is being watched by law enforcement. And more than likely, our sophisticated adversaries assume the government has greater surveillance powers than they actually do. The mystique of "big brother" can be a more effective weapon and deterrent than if our adversaries actually knew our true capabilities. What these disclosures have revealed is that the government has limits to what they can target, who they can target, and what they can access. As Snowden argues in his own words, "[t]he fact that people know communications can be monitored does not stop people from communicating [digitally]. Because the only choices are to accept the risk, or to not communicate at all."[68] But at least now, our adversaries know which communication service providers cooperate with the government, the specific collection techniques being used, and where the IC has focused the majority of its efforts. Our adversaries can now develop countermeasures, alternative methods of communicating with one another, and avoid or eliminate operations with identified vulnerabilities. NSA's mystique of know-all, see-all has been seriously tarnished.

---

[66] Transcript of INTELLIGENCE SQUARED U.S. debate, *supra* note 43.

[67] *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? A Conversation with FBI Director James Comey*, BROOKINGS INSTITUTE, Oct. 16, 2014, transcript available at http://www.brookings.edu/~/media/events/2014/10/16%20going%20dark%20technology%20privacy%20comey%20fbi/20141016_fbi_comey_transcript.pdf. .

[68] Bamford, *supra* note 49. "And when we're talking about things like terrorist cells, nuclear proliferators – these are organised cells. These are things an individual cannot do on their own. So if they abstain from communicating, we've already won. If we've basically talked the terrorists out of using our modern communications networks, we have benefited in terms of security – we haven't lost." *Id.*

Extensive damage has been done to U.S. credibility and trust issues with its foreign allies who no longer blindly trust the United States with their intelligence secrets. Our allies have reassessed the level of their cooperation on intelligence sharing since the United States has been shown incapable of keeping secrets and even occasionally spies on its closest foreign partners. Foreign allies may be hesitant to cooperate on the next terrorism investigation. Communications service providers that were willing to cooperate with the government previously on issues dealing with national security and efforts to combat terrorism are now exposed, and may refuse to cooperate with the government in the future without being forced to do so by a court order.

V. Conclusion

It is not surprising that Snowden revealed top secret information on NSA surveillance programs twelve years after 9/11. When the PATRIOT Act, which provided the IC and law enforcement with expansive surveillance and investigative powers, passed in 2001, the law had strong popular support. Americans feared for their safety. The government took significant legal steps to ensure they would be better able to attempt to predict and prevent another terrorist attack before it occurred, and they have been, for the most part, extremely successful in thwarting other 9/11-type attacks. Therefore, it is ironic that the IC's own success has paved the way for whistleblowers such as Snowden to gain sufficient popularity in order to reveal NSA programs under the guise of being concerned about our right to privacy. The pendulum has swung the other way, and Americans are more concerned about potentially being monitored by the government than they were immediately after 9/11. If the government had been unsuccessful in preventing attacks, the concern would be entirely different. The question would be what more can the IC do to prevent such attacks from occurring rather than the current question as to why the government is collecting so much personal data. The risk of terrorist attacks seems to be, at the very least, stabilized, and the bigger concern is our civil liberties. Due to its success, the IC is now on the defensive (as it was for the opposite reason the day after 9/11).

In short, all the media hype and "24/7 surveillance state" diatribes should be taken with a grain of salt. The moniker "big, bad government" is a misnomer although our system remains imperfect. Our leadership and government employees are for the most part decent, honest, reliable folks who are doing their jobs to the best of their ability. Some government employees are abusing their power and should be punished. When discussing government surveillance practices, there must be adequate oversight to avoid widespread, abusive practices that gradually become so pervasive that they are deemed acceptable. However, full and specific disclosure when it comes to the sensitive nature of intelligence collection and its analysis is unnecessary. There are legal remedies, anonymous tip lines, and multiple avenues to report wrong doing when a whistleblower becomes concerned about "perceived" illegal activity by government. Snowden did not pursue most of these legal remedies before disclosing classified information to the media. It is true that certain aspects of NSA's bulk collection and interception efforts may require further review and legal clarifications, but such discussions need not take place on the front page of newspapers. The recent disclosures of NSA abuse as "perceived" by Snowden do not come close to the pervasive abuses described by the Church Committee in the seventies.

Despite Snowden's pleas for an open-source community free from monitoring, the Internet is not and will not be free from surveillance regardless if the NSA participates or not. It is naive to think otherwise. The government needs to collect and analyze intelligence information in order to arrive at the best domestic, foreign, economic, military, law enforcement, or political decisions possible, and that includes policy decisions on the fight against terrorism.

In one interview, Snowden makes reference to the German Stasi that conducted "mass, indiscriminate spying campaigns"[69] in communist-dominated East Germany where the secret police collected information on roughly one quarter of the population.[70] The NSA is not the Stasi of East Germany – the NSA is not conducting mass, indiscriminate spying campaigns hoping to catch anti-government protestors in incriminating positions in order to lock them away and eliminate any and all dissent. Stasi-like dossiers are not being created on individuals who vote a certain way or oppose government policies. NSA does not monitor U.S. citizens to identify their daily activities, what errands they run, what websites they are viewing, and how their children are doing in school. What NSA does do is collect positive intelligence information, foreign intelligence information which is collected and analysed under legal parameters. These collection efforts are meant to protect U.S. citizens from future terrorist attacks and future cyber-attacks. Under section 702, targeting and minimization procedures are in place, and FISA warrants are required when the NSA wants to target U.S. citizens suspected of being agents of a foreign power.

It is not the government surveillance programs we should be overly concerned about. Public discussion and congressional and internal oversight committees keep those necessary but controversial programs under control and within legal parameters. It is the few isolated cases of individuals within the government who abuse their power and betray the American people who are of major concern, e.g., those who abuse their power and violate sections 215, 702 and FISA laws. Those are the illegalities that should be brought to light, not our government's specific sources, methods, capabilities, and successes that our enemies desperately want revealed.

[69] Rusbridger & Macaskill, *supra* note 48.
[70] Julia Angwin, *You Know Who Else Collected Metadata? The Stasi.*, PROPUBLICA, Feb. 11, 2014, http://www.propublica.org/article/how-the-stasi-spied-on-social-networks.