Spring 2016

Law v. Safety: Balancing Domestic Surveillance's Legal Deficiencies Against The Necessity Of Counterterrorism

Jeremy Kommel-Bernstein

LAW V. SAFETY: BALANCING DOMESTIC SURVEILLANCE'S LEGAL DEFICIENCIES AGAINST THE NECESSITY OF COUNTERTERRORISM

A Masters Thesis

Presented to

The Graduate College of

Missouri State University

In Partial Fulfillment

Of the Requirements for the Degree

Master of Science, Defense and Strategic Studies

By

Jeremy Kommel-Bernstein

May 2016

LAW V. SAFETY: BALANCING DOMESTIC SURVEILLANCE'S LEGAL DEFICIENCIES AGAINST THE NECESSITY OF COUNTERTERRORISM

Defense and Strategic Studies

Missouri State University, May 2016

Master of Science

Jeremy Kommel-Bernstein

ABSTRACT

This thesis discusses whether the collection of metadata by the NSA, as revealed in 2013 by Edward Snowden, from domestic sources is legal and/or effective, and how to balance safety and liberty. The topic is both timely and important due to the potential for abuse that comes with domestic intelligence programs, as well as the risk of suffering a terrorist attack on U.S. soil. Research for this thesis included personal interviews with former NSA and CIA Director Michael Hayden, and reviewing numerous court cases, legal documents, and articles and books on the subject. There is significant evidence that the NSA's mass collection of metadata violates the 4th Amendment, while the FISA Court fails to meet the Case and Controversy and impartial magistrate requirements of the Constitution. Alternatively, it can be argued that the Necessary and Proper Clause, the 3rd Party Doctrine, and the governmental responsibility to protect and defend the people outweigh such concerns. Questions of efficacy are almost impossible to fully explore due to the need to access classified information to do so, but many experts have declared that there is significant evidence that the programs addressed herein are effective in the fight against terrorists. The result of this research is that these programs do violate the law, but with minor tweaks or concessions they can operate fully within constitutional boundaries, and while they may not have enormous effects on counterterrorism, enough good has come from them that it would be improper to shut them down.

KEYWORDS: intelligence, National Security Agency, metadata, domestic surveillance, 4th Amendment, FISA, War on Terror, Counterterrorism, USA PATRIOT Act

This abstract is approved as to form and content

_____

Dennis J. Bowden, M.A.
Chairperson, Advisory Committee
Missouri State University

LAW V. SAFETY: BALANCING DOMESTIC SURVEILLANCE'S LEGAL DEFICIENCIES AGAINST THE NECESSITY OF COUNTERTERRORISM

By

Jeremy Kommel-Bernstein

A Masters Thesis
Submitted to the Graduate College
Of Missouri State University
In Partial Fulfillment of the Requirements
For the Degree of Master of Science, Defense and Strategic Studies

May 2016

Approved:

_____
Dennis J. Bowden, MA

_____
Ilan Berman, JD

_____
Andrei Shoumikhin, PhD

_____
Julie Masterson, PhD: Dean, Graduate College

ACKNOWLEDGEMENTS

I would like to thank my mom Joanie, step-father Barry, and brother Jesse, who have always encouraged me and pushed me to be the best I can be, no matter what the circumstance. Mary, Dan, Kath, Steve, and Kelly, thanks for being family to me, even though you don't have to be.

Thank you to Dennis Bowden for being my advisor on this project and for first suggesting that I turn a paper for your class into something larger; without your help and guidance, this project would have been nearly impossible. Additionally, Ilan Berman and Dr. Andrei Shoumikhin deserve my thanks for agreeing to be involved in this project. Dr. John Rose also continually offered support and encouragement throughout my time in graduate school, and that has been greatly appreciated.

Thank you as well to General Michael Hayden for donating your time to lend me your invaluable opinions and expertise. We may not agree on everything, but your arguments were always well reasoned and thought-provoking, and I came out of each of our meetings feeling as if I had learned and benefitted from that time.

A special thank you to Dr. Matthew Light for having spent the last nine years pushing me to do more educationally, professionally, and personally; it has been invaluable.

Lastly, thank you Jess for all your support, encouragement, and love. The last two years would not have been the same without you.

"It is not the fact of liberty but the way in which liberty is exercised
that ultimately determines whether liberty itself survives"
--Dorothy Thompson

TABLE OF CONTENTS

Introduction.....1

History and Background.....9
- National Security Agency.....9
- Historical Violations of Americans' Privacy and Attempts to Limit Domestic Intelligence Collection.....13
- Edward Snowden Leaks.....21

Programs of Note.....24
- PRISM.....25
- MUSCULAR.....31
- BOUNDLESSINFORMANT.....35
- XKEYSCORE.....37
- Additional Thoughts.....40

Legal Arguments.....44
- New Procedures under USA FREEDOM Act.....47
- Fourth Amendment Questions.....52
- Due Process—Fifth and Fourteenth Amendments.....58
- Governmental Necessity.....62
- Miscellany.....65

How Effective is Domestic Surveillance?.....68
- Arguments for Effective Use.....71
- Arguments for Ineffectualness.....76

Conclusions.....80

Bibliography.....97

Appendices.....111
- Appendix A. Amendments to the Constitution of the United States of America (Excerpted).....111
- Appendix B. Constitution of the United States of America (Excerpted).....114
- Appendix C. Executive Order 12333 (Excerpted).....119

LIST OF FIGURES

Figure 1. Pew Research Center NSA Surveillance Poll 4

Figure 2. Overview of PRISM Capabilities 26

Figure 3. Private Company Involvement in PRISM by Date 28

Figure 4. Overview of MUSCULAR Capabilities 31

Figure 5. Overview of BOUNDLESSINFORMANT 36

Figure 6. XKEYSCORE Capabilities (1) 38

Figure 7. XKEYSCORE Capabilities (2) 39

Figure 8. USA FREEDOM Act Architecture 51

Figure 9. Pew Research Center Threats to U.S.A. Poll 64

Figure 10. Pew Research Center Trust in Government Poll 69

Figure 11. “Paul Revere” Metadata Chart 73

Figure 12. XKEYSCORE Successes 74

INTRODUCTION

The United States of America was founded upon the idea that government must be subordinate to the populace, a "government of the people, by the people, [and] for the people."[1] President Abraham Lincoln unintentionally expressed well the contradictory nature of the U.S. federal government, which by its very charter operates with the consent of the people and counts among its responsibilities the protection of the people, for their own sake and for that of the government.[2] In the 21st century, when the threats facing the United States, its allies, and most importantly its people, are unlike any imagined by the founding fathers, and technology has allowed war to progress from a battle of muskets to one of keystrokes, the legal and ethical waters are even more muddied than ever.

If government is responsible for protecting the people and the state, what should be the limits of its authority to do so? For that matter, if the threat is grave enough, or immediate enough, *are* there any limits? These are the questions that confront policy makers, congressional overseers, judges and, most importantly the American people in the wake of dramatic revelations in 2013 by a former National Security Agency (NSA) contractor of mass "surveillance" operations undertaken by the United States government.[3] In a government that is intended to be a protector of the people, from itself

---

[1] Abraham Lincoln, "The Gettysburg Address" (speech, dedication of the Soldiers' National Cemetery, Gettysburg, PA, November 19, 1863), reproduced at http://www.abrahamlincolnonline.org/lincoln/speeches/gettysburg.htm

[2] "Constitution of the United States," *U.S. Archives*, accessed September 6, 2015, http://www.archives.gov/exhibits/charters/constitution_transcript.html. The Preamble to the Constitution of the United States begins with the declaration that "the People" have established the government. The Preamble and several articles include references to the governmental responsibility for protecting the interests and safety of the citizenry.

[3] *See* Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," *Guardian* (London), June 6, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-

and from external threats, there is a line, one that is continually redrawn by quarrels between the government and its citizenry, which determines what is acceptable for the protector to undertake in order to accomplish that particular part of its charter. The Fourth Amendment to the Constitution of the United States provides a framework within which this line must remain, never varying too far from the specifics articulated in the search and seizure limitations of the amendment. (See Appendix A)

The question of what is permissible is only likely to grow more complicated as time goes on. As it is, many of the issues surrounding government surveillance that arose in 2013 appear to be a result of new capabilities rather than "malicious" intent on the part of the United States government. In the words of former National Security Agency and Central Intelligence Agency (CIA) Director General Michael Hayden (USAF, Ret.), the NSA is "getting far more incidental collection now than [it has] in the past, just because of the nature [of the] technology" available.[4] If Moore's Law, which postulates that computing power doubles every two years,[5] is accepted to be true, technology will continue to improve in the years ahead, and in doing so continue to risk further "incidental" collection by the government that could potentially affect the constitutionally protected files, communications, and data of American citizens. The intelligence community is built on the predilection that such collection is a positive. As former senior intelligence community official Mark Lowenthal wrote, "[t]he intelligence community

---

records-verizon-court-order; and Glenn Greenwald, et al, "Microsoft Handed the NSA Access to Encrypted Messages," *Guardian* (London), July 12, 2013, http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

[4] Michael Hayden (retired General, United States Air Force, former Director, Central Intelligence Agency and National Security Agency, former Principal Deputy Director of National Intelligence) in discussion with the author, September 21, 2015

[5] "Moore's Law," *www.mooreslaw.org*, accessed January 13, 2016, http://www.mooreslaw.org/

would rather collect more than less."[6] General Hayden addressed the issue even more simply, saying that in the days immediately following the 9/11 terrorist attacks, "when the decisions were made, all ties went to, 'bulk up the collection.'"[7] Thus, even with 2015's changes to the legal authorization for metadata collection,[8] the question of what is appropriate, legal, and acceptable remains salient; in fact, because of the risks that the future holds for potential abuse of authority, the question has even more importance than it did when journalists Glenn Greenwald and Laura Poitras exposed the leaked documents provided by Edward Snowden in 2013. What is collected, the amount that is collected, and even how it is accessed and stored, is up for debate at this time. With a population that is largely ambivalent about government intrusion into their lives, there is always the opportunity for the National Security Agency, Federal Bureau of Investigation (FBI), or any of the other intelligence and law enforcement agencies to push the boundaries of acceptable conduct in their ongoing quest to secure the United States and American citizens abroad from the threat of a terrorist attack. Following the publication of articles in 2006 regarding illegal NSA activities,[9] Americans split fairly evenly on the issue of whether the U.S. government should conduct domestic surveillance as part of its

[6] Mark Lowenthal, *Intelligence: From Secrets to Policy*, *Fifth Edition* (Los Angeles, CA: CQ Press, 2012), 208

[7] Hayden, in discussion with the author, September 21, 2015

[8] *See* "H.R. 2048: Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-Collection and Online Monitoring (USA FREEDOM) Act of 2015 (114th Congress, 2015-2016)," Library of Congress, https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf. This bill, which was signed into law in June 2015, will be addressed at later points in this thesis.

[9] This will be discussed further in the following chapter

counterterrorism strategy. After the Snowden leaks, by contrast polls showed a significant majority said secret domestic surveillance was acceptable. (See Figure 1)[10]

Public's Views of NSA Surveillance Programs under Obama, Bush

NSA has been getting secret court orders to track calls of millions of Americans to investigate terrorism ...	**June 2013**
	%
Acceptable	56
Not acceptable	41
Don't know	2
	100
NSA has been investigating people suspected of terrorist involvement by secretly listening in on phone calls & reading emails without court approval...	**Jan 2006**
Acceptable	51
Not acceptable	47
Don't know	2
	100

PEW RESEARCH CENTER/WASHINGTON POST June 6-9, 2013. Figures may not add to 100% because of rounding. Jan. 2006 data from ABC NEWS/WASHINGTON POST.

F1: Pew Research Center polling data comparing and contrasting the public's reaction to the NSA's surveillance programs under both President George W. Bush and President Barack Obama

Much of the information needed to form a complete sense of the scope and methodology of the various programs exposed by Edward Snowden is still highly classified, and even those documents that have been leaked are difficult to interpret without the necessary context which remains classified and unobtainable.[11] Additionally, successes achieved by the various intelligence and law enforcement agencies, particularly

[10] "Majority Views NSA Phone Tracking as Acceptable Anti-terror Tactic: Public Says Investigate Terrorism, Even if it Intrudes on Privacy," *Pew Research Center*, June 10, 2013, http://www.people-press.org/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/

[11] All classified information contained within this thesis was obtained through open, public sources such as news media and published literature.

those that do not involve arrests on U.S. soil, are rarely publicized, and even when they are, the methods used to achieve these successes are almost never disclosed. Doing so would almost certainly diminish the effectiveness of these programs, however much or little that may be, by alerting the various potential targets that they are subject to surveillance, and the United States government has absolutely no incentive to make the lives and missions of terrorists easier.

Thus, if these programs are effective, as many past and present government officials, including President Barack Obama,[12] have insisted, then not only did Snowden categorically break the law, but he also may well have endangered American lives. However, that does not necessarily mean that the programs are legal, ethically sound, or in general keeping with the principles on which the United States was founded and intended to operate. In fact, on the face of it, much of what Snowden released seems to violate at least the Fourth Amendment to the Constitution of the United States, which states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[13]

The National Security Agency acknowledged that it has collected massive amounts of metadata from American citizens and other U.S. persons without a targeted methodology;

---

[12] Ellen Nakashima, "Congressional Act on NSA is a Milestone in the Post-9/11 World," *Washington Post*, June 2, 2015, http://www.washingtonpost.com/world/national-security/congressional-action-on-nsa-is-a-milestone-in-the-post-911-world/2015/06/02/f46330a2-0944-11e5-95fd-d580f1c5d44e_story.html

[13] "Bill of Rights." *U.S. Archives*. Accessed April 14, 2015. http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html

there are no descriptions of "the place to be searched, and the…things to be seized" that specifically apply to the investigation of a known criminal act.[14]

Edward Snowden's leaks were, according to him, intended to spark debate and external examination of the NSA's operations. He alleged that some of the activities the NSA was undertaking were illegal due to their intrusive nature, but that despite that invasiveness, programs were ineffective against terrorists, albeit highly effective at spying on American citizens. Snowden, through his own words and via the reporting of Greenwald, Poitras, *et al*, proclaimed that there should be investigations into the NSA's activities and punishment for those involved in what he proclaimed to be illegal, ineffective, and anti-American programs.[15] Despite Snowden's rhetoric and certainty, there are five possible scenarios when examining the future of these programs:

- The programs are entirely legal, and are an effective tool for counterterrorism, counterintelligence, and foreign affairs;
- The programs are entirely legal, but are an ineffective tool, or at least are not effective enough to justify their expense;
- The programs are illegal, but are an effective tool for counterterrorism, counterintelligence, and foreign affairs;
- The programs are illegal, and are either ineffective or overly costly for their effectiveness; and
- The legality of the programs is questionable, as is the effectiveness, but there is widespread debate and disagreement over each.

[14] John Darby, "SIGINT and the National Security Agency" (presentation, MSU DSS Intelligence, Counterintelligence, and Covert Action class, Vienna, VA, February 25, 2015); Hayden, in discussion with the author, September 21, 2015; Lee Ferran, "Ex-NSA Chief: 'We Kill People Based on Metadata,'" *ABC News*, May 12, 2014, http://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata/; and Barton Gellman and Matt Delong, "The NSA's Three Types of Cable Interception Programs," last accessed April 26, 2015, http://apps.washingtonpost.com/g/page/world/the-nsas-three-types-of-cable-interception-programs/553/#document/p7/a129998

[15] *Citizenfour.* HBO Films. 2014. Viewed via *HBOGO*

In four out of these five scenarios, policy makers would seem to have extremely easy decisions to make. If it is ineffective, why continue a program, regardless of legality? If it is legal *and* effective, why discontinue? And in general, if it is illegal, it is not worth doing, regardless of effectiveness, because the consequences of getting caught are too grave.[16] Additionally, people and organizations that operate in an ethical manner rarely commit willful violations of the law.

The issue with the programs revealed in 2013 by Edward Snowden is that they fall into the fifth and final scenario. Many, including Federal Judges Gerard E. Lynch[17] and Richard Leon,[18] as well as the legal counsel for Yahoo!, have stated that the untargeted collection of metadata by the United States government is illegal for a variety of reasons that will be addressed below.[19] Numerous others, including even Alan Dershowitz,[20] a noted Fourth Amendment protectionist and strict constructionist, and libertarian Federal Judge Richard Posner,[21] have said that the government is not

---

[16] James Bamford, *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (New York, NY: Doubleday, 2008), 108. General Hayden, speaking to the author, stated that, prior to 9/11, the NSA "played a bit back from the line so as not to get close to anything that got the agency's fingers burned in the Church-Pike era," referring to the Senate and House committees formed in the mid-1970s to investigate wrongdoing and malfeasance in the intelligence community.

[17] Ariane de Vogue, "Court Rules NSA Program Illegal," *CNN*, last updated May 7, 2015, http://www.cnn.com/2015/05/07/politics/nsa-telephone-metadata-illegal-court/; and David Fidler, "While Ruling NSA Program Illegal, Appeals Court Suggests Path Forward," *Defense One*, May 11, 2015, http://www.defenseone.com/politics/2015/05/while-ruling-nsa-program-illegal-appeals-court-suggests-path-forward/112435/

[18] Zach Warren, "Judge Rules NSA Collection 'Almost Certainly' Violates Constitution," *Inside Counsel*, December 17, 2013, http://www.insidecounsel.com/2013/12/17/judge-rules-nsa-collection-almost-certainly-violat

[19] Ron Bell, "Shedding Light on the Foreign Intelligence Surveillance Court (FISC): Court Findings from Our 2007-2008 Case," *Tumblr.com*, September 11, 2014, http://yahoopolicy.tumblr.com/post/97238899258/shedding-light-on-the-foreign-intelligence. Bell is General Counsel to Yahoo!

[20] Alan Dershowitz, interview by Piers Morgan, *Piers Morgan Live*, CNN, June 6, 2013. View at https://www.youtube.com/watch?v=0BhhB6vuhqg

[21] Grant Gross, "Judge: Give NSA Unlimited Access to Digital Data," *PC World*, December 4, 2014, http://www.pcworld.com/article/2855776/judge-give-nsa-unlimited-access-to-digital-data.html

overstepping its bounds. Examining the relevant statutory and constitutional issues involved will make up a significant portion of this thesis, as will the question of efficacy.

This thesis originated from a research project conducted by the author in a Missouri State University class entitled "Intelligence, Counterintelligence, and Covert Action;" portions of the original product are featured throughout. Extensive research has been undertaken, including interviewing General Michael Hayden, as well as examination of documents declassified by the United States government, news articles, court cases, and a variety of other media. Included within this thesis are reproductions of and references to classified information leaked by Edward Snowden in 2013.[22] Additionally, it is abundantly clear to any but the most zealous anti-government activist that the vast, overwhelming majority of people who work at the National Security Agency and its partners in the intelligence community (IC) are patriotic Americans who do their best every day to respect and uphold the rights of their fellow citizens.

That said, classified NSA documents have been released and the programs revealed; they cannot simply be ignored. Considering the legal framework and justification upon which the programs Edward Snowden revealed were based, it seems highly likely that they were conducted outside the boundaries of the law, in particular the United States Constitution. (See Appendix B) Furthermore, the use of these programs, in violation of legal norms, is thus likely to have a chilling effect on freedom of speech and expression for a number of different groups and potentially lead down a "slippery slope" wherein the intelligence community takes every excuse to "bulk up the collection" in the name of safety and security, while rights quietly but surely are stripped away.

[22] It should be noted that despite the use of these documents, the revelation of which was undoubtedly a violation of U.S. federal law, the author does not support Mr. Snowden's unilateral decision to release them, and in fact believes that Mr. Snowden should stand trial for having done so.

HISTORY AND BACKGROUND

Examining the origins of an issue provides more important context and helps one to understand its current status and relevance. This is particularly true in situations such as the NSA's domestic intelligence operations, as they have elements of the past repeating itself. Knowing about the NSA's origins, the legal strictures within which the intelligence community must operate when taking action within the borders of the United States, the manner in which the programs under discussion herein were revealed, and even why they those revelations were made make it far easier to judge the current situation and come to realistic, well-informed conclusions.

National Security Agency

While the Central Intelligence Agency has traditionally been the primary target of investigative journalists looking for the next big scoop on the intelligence community and its perceived foibles, the National Security Agency has toiled tirelessly in relative secrecy and anonymity. Those who paid attention to the intelligence community or national security were always aware of the NSA and may have even had some knowledge of its work, but the agency itself preferred to work in the high security confines of Fort Meade. Few people in the general public were aware of this massive, yet hidden, agency which employs more people and consumes more electrical power than any other single entity in the State of Maryland.[23] In fact, prior to the Church Committee's October 29th, 1975 hearing, "representatives of the NSA [had] never appeared before the Senate in a public

[23] Mark L. Barnett, "National Security Agency/Central Security Service" (unclassified presentation to the Greater Baltimore Committee, April 26, 2011)

hearing"[24] since the agency's inception in 1952. Now the NSA has its own website, Twitter feed, and *two* Facebook pages.[25]

Even the agency's scandals lacked the sexiness of the CIA's; contrary to the 1998 blockbuster film *Enemy of the State*, the NSA does not, in fact, take part in assassinations of congressmen and mob lawyers. However, at different points in its history, the NSA has come under fire from its oversight committees in Congress, which have alleged various improprieties and illegalities. These scandals included monitoring phone calls by American citizens who were opposed to the Vietnam War—a revelation that helped lead to the passage of the Foreign Intelligence Surveillance Act of 1978[26]—and the warrantless "eavesdrop[ping] on American phone calls and emails" ordered by President George W. Bush in the wake of the September 11th, 2001 terrorist attacks on New York City and the Pentagon, and later exposed in 2005 by the *New York Times*.[27] Overall, however, as often happens in cases involving the intelligence community, many in Congress have appeared to, at least publicly, offer unqualified support for the operations of the agencies, as Senator Dianne Feinstein (D-CA), at the time the Chairwoman of the Senate Select Committee on Intelligence,[28] did in the weeks and months following when

---

[24] "Intelligence Activities—National Security Agency and Fourth Amendment Rights" (testimony at U.S. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Washington, D.C., October 29, 1975). See the Chairman's opening remarks.

[25] www.nsa.gov, #NSAGov, and both an English and Spanish page on Facebook.

[26] Ed Pilkington, "Declassified NSA Files Show Agency Spied on Muhammad Ali and MLK," *The Guardian*, September 26, 2013, http://www.theguardian.com/world/2013/sep/26/nsa-surveillance-anti-vietnam-muhammad-ali-mlk. Ironically, the NSA was also tapping the phone of Senator Frank Church, who led the aforementioned probe into the intelligence community in the years immediately following the Nixon presidency.

[27] James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times,* December 16, 2005, http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&_r=2&

[28] "Members: 113th Congress (2013-2014)," *U.S. Senate*, accessed April 26, 2015, http://www.intelligence.senate.gov/members113thcongress.html

Edward Snowden's leaks began to appear in *The Guardian* and *Washington Post* newspapers, among others.[29]

Legally questionable activities by the NSA began before it even *was* the NSA. One of the agency's predecessors, the United States Navy's communications intelligence section, "began intercepting the international telephone calls and international cable traffic of Jewish agents in the United States" in 1946, a result of "Operation Gold."[30] Operation Gold was a U.S. Navy Intelligence operation to intercept cable transmissions crossing the Atlantic Ocean.[31]

Even the way in which the National Security Agency came into being is somewhat legally dubious.

> [O]n October 24th, 1952, [President Harry] Truman issued a highly secret order scrapping [the Armed Forces Security Agency] and creating in its place a new agency to be largely hidden from Congress, the public, and the world. Early on the morning of November 4, as Truman was leaving a voting booth in Independence, Missouri, the National Security Agency came to life.[32]

That high level of secrecy was par for the course for the NSA's predecessors, such as the tiny Signal Intelligence Service, the employees of which were warned that "[t]he State Department…was never to know of its existence."[33]

---

[29] Dianne Feinstein and Mike Rogers, interview by George Stephanopoulos, *This Week*, ABC, June 9, 2013. *See also* Chairwoman Feinstein's opening statement at a Senate Select Committee on Intelligence hearing on March 12, 2013, where she was most effusive in her praise for DNI Clapper, NSA Director Alexander, and FBI Director Mueller.

[30] Matthew M. Aid, *The Secret Sentry: The Untold History of the National Security Agency* (New York, NY: Bloomsbury Press, 2009), 10

[31] Calder Walton, "How Zionist Extremism Became British Spies' Biggest Enemy," *Foreign Policy*, January 1, 2014, http://foreignpolicy.com/2014/01/01/how-zionist-extremism-became-british-spies-biggest-enemy/

[32] James Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency* (New York, NY: First Anchor Books, 2001), 31

[33] Ibid, 1-3

Today, despite its website and Twitter feed, the NSA is still as secretive as any agency within the federal government can be in an age of instant news, immense computing power available at the public's fingertips, and leakers such as Snowden and Chelsea (Bradley) Manning. At one point, concerned that a new "eleven-story office building [located nearby] might be able to look into [Fort Meade], NSA leased the entire building before it was completed." In the early 1990s, a real estate photographer taking pictures near Fort Meade found himself "surrounded by NSA security vehicles" and questioned as to his intentions; he informed the officers that "he had never even heard of NSA."[34]

Despite being "the largest in terms of people and…in terms of budget" in the intelligence community,[35] the agency spent much of its history trying to deny it even existed. Even its internal nickname for the last seventy years has been a reference to the secrecy; in a play on its initialism, the NSA became "No Such Agency." The very number of employees is classified, and estimates of those working at Fort Meade range from 35,000 to 55,000.[36]

Much has changed for the National Security Agency since September 11th, 2001. As James Bamford, a former Naval Intelligence seaman during the Vietnam War who became one of the leading experts and authors on the NSA, noted in his book *The Shadow Factory*, prior to 9/11 "the NSA was a little-noticed agency attempting to

[34] Ibid, 5

[35] Ibid

[36] Anne Gearan, "'No Such Agency' Spies on the Communications of the World," *Washington Post*, June 6, 2013, https://www.washingtonpost.com/world/national-security/no-such-agency-spies-on-the-communications-of-the-world/2013/06/06/5bcd46a6-ceb9-11e2-8845-d970ccb04497_story.html

downsize by a third and searching for a mission."[37] After the events of that day, the agency not only had a mission, but its chief, General Hayden, while trying to respect how "sensitive the entire culture behind…[the NSA] is to the Fourth Amendment," was willing to do almost anything he considered necessary to prevent a repeat of that devastating terrorist attack.[38]

Historical Violations of Americans' Privacy Rights and Attempts to Limit Domestic Intelligence Collection

Statutory law and executive regulation, along with the Constitution, limit domestic intelligence collection. This includes the 1981 Executive Order (E.O.) 12333 and its successors and the National Security Act of 1947, signed into law by President Truman, which expressly prohibited the newly created Central Intelligence Agency from having "police, subpoena, law-enforcement powers, or internal-security functions."[39] E.O. 12333 established "lanes in the road" for the various intelligence agencies, demarcating exactly what functions each intelligence agency could undertake, and both conveying authority and explicitly denying it, particularly in the realm of domestic surveillance. It specifically assigned domestic intelligence duties, especially counter-espionage and counterterrorism efforts within the United States, to the Federal Bureau of Investigation (FBI). The CIA and the majority of the other intelligence agencies, such as those within the Department of Defense, were prohibited from engaging in domestic

[37] James Bamford, *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (New York, NY: Doubleday, 2008), 4

[38] Hayden, in discussion with the author, September 21, 2015

[39] "S. 758: The National Security Act of 1947 (80th Congress, 1947-1948)," *Oxford University Press*, last accessed January 27, 2016, http://global.oup.com/us/companion.websites/9780195385168/resources/chapter10/nsa/nsa.pdf

collection and surveillance, with limited exceptions for the purpose of "foreign intelligence" involving agents of "foreign powers."[40] (See Appendix C) Typically, even those cases have been under the purview of the FBI, with assistance from or cooperation with the foreign-focused intelligence agencies. The original limitations in the National Security Act were intended to prevent the American intelligence services from becoming domestic secret police like those in the Soviet Union or Nazi Germany, and the executive order was a reaction to past offenses by federal law enforcement and the intelligence community that came to light in the early 1970s.

E.O. 12333 and the Foreign Intelligence Surveillance Act of 1978 were specifically the result of the findings of the Church and Pike Committees in the Senate and House of Representatives, respectively, and the executive branch's Rockefeller Commission, named for the Vice-President who led it. Many of the issues that the commissions confronted were similar to those that are in the news today. These investigative groups discovered widespread violations of Americans' privacy, including investigations into civil rights leaders and protesters who had committed no crimes, and various other misdeeds by the FBI and other intelligence agencies, including the NSA.[41] Preventing further abuses was foremost in the minds of the members of the investigative committees.

The NSA is one of the agencies specifically proscribed from conducting intelligence collection on so-called "U.S. persons." E.O. 12333 defined the term as

[40] "Executive Order 12333 -- United States Intelligence Activities," *National Archives*, last accessed January 13, 2016, http://www.archives.gov/federal-register/codification/executive-order/12333.html

[41] "The Evolution of the U.S. Intelligence Community—An Historical Overview," *Federation of American Scientists*, February 23, 1996, http://fas.org/irp/offdocs/int022.html

> a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.[42]

22 U.S. Code §6010 states much the same: "'United States person' means any United States citizen or alien admitted for permanent residence in the United States, and any corporation, partnership, or other organization organized under the laws of the United States."[43] Exceptions are made for situations "when significant foreign intelligence is sought." Foreign intelligence is defined by E.O. 12333 as "information relating to the capabilities, intentions and activities of foreign powers, organizations or persons, but not including counterintelligence except for information on international terrorist activities."[44] Any other domestic surveillance (i.e. for law enforcement purposes) requires a warrant issued by a regular court.

After the Church and Pike hearings in the mid-1970s, Congress passed the Foreign Intelligence Surveillance Act (FISA) of 1978, becoming the main legislative barrier to unchecked IC actions within the United States. FISA established requirements for pursuing warrants against Americans for the purpose of intelligence collection. This includes the requirement that the targeted U.S. person be the subject of an investigation as an agent of a foreign power or of an international terrorism inquiry. These warrant applications are made to a special court, known as the Foreign Intelligence Surveillance Court, or FISC. It is also commonly known as the FISA Court. The eleven judges who

---

[42] Ibid

[43] "22 U.S. Code §6010: 'United States Person' Defined," *United States Government Printing Office*, last accessed January 27, 2016, https://www.gpo.gov/fdsys/pkg/USCODE-2010-title22/pdf/USCODE-2010-title22-chap69-sec6010.pdf

[44] "Executive Order 12333…"

sit on the FISC are Federal District Court jurists selected by the Chief Justice of the Supreme Court, and they serve for seven year staggered terms. FISA was also the first time that Congress had defined terrorists as being the subject of foreign intelligence, setting the stage for the post-9/11 increase in signals intelligence (SIGINT) collection related to terrorism.[45]

In 2005 *New York Times* reporters James Risen and Eric Lichtblau broke the news that the National Security Agency, under the auspices of a 2002 order by President George W. Bush, had begun a system of warrantless, targeted surveillance of "hundreds, perhaps thousands, of people inside the United States… in an effort to track possible 'dirty numbers' linked to Al Qaeda."[46] According to Matthew Aid, who has written extensively on the U.S. intelligence community, this program became known as the Terrorist Surveillance Program (TSP) and was running as part of an overarching counterterrorism SIGINT program codenamed STELLARWIND,[47] "which sifts through vast amounts of electronic data secretly provided by America's largest telecommunications companies and Internet service providers, looking for signs of terrorist activity at home and abroad."[48] STELLARWIND involved the collection of bulk metadata, similar to programs revealed by Edward Snowden, but in this case the targets eventually specifically included U.S. persons, despite the lack of a warrant from the FISA

[45] "S. 1566: Foreign Intelligence Surveillance Act of 1978 (95th Congress, 1977-78)," *United States Government Printing Office*, last accessed January 29, 2016, https://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf; *see also* "The Foreign Intelligence Surveillance Court," *Washington Post*, accessed April 19, 2015, http://www.washingtonpost.com/politics/the-foreign-intelligence-surveillance-court/2013/06/07/4700b382-cfec-11e2-8845-d970ccb04497_graphic.html for a simple explanation of the FISC.

[46] Risen and Lichtblau

[47] This program was also known as the President's Surveillance Program, or PSP

[48] Aid, 288

Court or any other federal magistrate.[49] From its origins, President Bush granted approval for the NSA, through STELLARWIND and TSP, to surveil Americans, letting this foreign-focused agency wiretap U.S. persons' international phone calls and collecting bulk telephone and email metadata without a warrant.[50] This was in direct violation of the Fourth Amendment and the Foreign Intelligence Surveillance Act, which at the time did not include the provisions authorizing similar warrantless collection now found in Section 702 of that law, which were added in the 2008 amendments to that law and will be discussed in later chapters of this thesis. This was also in spite of NSA having previously "stated that FISA has in no way hampered its other SIGINT collection operations."[51]

President Bush's originally authorized the NSA to surveil only calls that included at least one party to the call that was foreign, or calls specifically about terrorism, but according to the *New York Times* a report by several Inspectors General shows that the NSA went beyond that mandate and began gathering metadata on purely domestic calls. After being confronted by senior members of the Justice Department, including Attorney General John Ashcroft, about inconsistencies between what was authorized on paper and what types of surveillance was actually being conducted, the president "retroactively" authorized the full scope of what NSA was doing.[52]

---

[49] Mike Masnick, "Latest Leak: NSA Collects Bulk Email Metadata on Americans," *techdirt*, June 27, 2013, https://www.techdirt.com/articles/20130627/09455923637/latest-leak-nsa-collected-bulk-email-metadata-americans.shtml

[50] Charlie Savage, "Declassified Report Shows Doubts about Value of N.S.A.'s Warrantless Spying," *New York Times,* April 24, 2015, http://www.nytimes.com/2015/04/25/us/politics/value-of-nsa-warrantless-spying-is-doubted-in-declassified-reports.html

[51] Aid, 296

[52] Charlie Savage, "George W. Bush Made Retroactive N.S.A. 'Fix' After Hospital Room Showdown," *New York Times*, September 20, 2015,

Just a year before TSP began in 2002, then NSA Director Hayden, serving at the time as NSA director, and his CIA counterpart, George Tenet, had testified before the House Permanent Select Committee on Intelligence (HPSCI) that neither of their agencies monitored the communications of Americans, with General Hayden going so far as to call it an "urban myth," and "assured the committee that NSA would assiduously abide by the legal strictures on such activities as contained in [the Foreign Intelligence Surveillance Act of 1978]."[53]

Even though these programs may have been legally questionable, a Justice Department lawyer, John Yoo, and White House counsel Alberto Gonzales—who later became Attorney General of the United States—wrote legal briefs justifying at least TSP. However, the access to information on these classified briefs was tightly controlled, and "[a]t the top of the list of people who were *not* permitted to see the Gonzales and Yoo legal briefs were the lawyers in NSA's Office of General Counsel responsible for ensuring that the eavesdropping programs conformed with the law."[54] Excluded from the process were attorneys from the Justice Department's Civil and Criminal Divisions, the Inspector General for the National Security Agency, or the Deputy Attorney General, any or all of whom would ordinarily be involved in vetting programs that were in any way legally questionable to make sure they complied with and conformed to the law. As Matthew Aid pointed out, the only people who were allowed access were those who "were deemed to be 'loyal' by [Vice President Dick] Cheney's office, and as such,

---

http://www.nytimes.com/2015/09/21/us/politics/george-w-bush-made-retroactive-nsa-fix-after-hospital-room-showdown.html?_r=1

[53] Aid, 287

[54] Ibid, 288-89

unlikely to question the programs' legality."[55] This severe control over the legal briefs meant that there was virtually no one "in the know" who could, or at least would, take a critical look and attempt to determine whether the powers of the Presidency had been exceeded, much less whether there was a fundamental violation of the Constitution.

Eventually, the central arguments of the Yoo and Gonzales briefs were made public; they posited that, during a time of war, there was in fact *no limit* to the President's power.[56] The George W. Bush Administration ignored two centuries of legal precedent, not to mention the fact that the country was not in fact at war; that requires a declaration by Congress, as laid out in Article II, Section 8 of the Constitution, which states this is the exclusive power of the Congress.[57] Legality aside, General Hayden maintains that the program was valuable and important intelligence was gained that was used to help prevent terrorist attacks.[58]

In 2004, then-Deputy Attorney General James Comey, who was acting in place of a hospitalized and extremely ill John Ashcroft, refused to recertify the STELLARWIND programs as lawful. An attempt by Gonzales to go around Comey by visiting Ashcroft in the hospital had the same result, and both Comey and Ashcroft cited work by Assistant Attorney General for the Office of Legal Counsel Jack Goldsmith in their refusals. Goldsmith argued that Yoo's legal rationale for the warrantless collection program was far too broad and noticed the disparity between what was authorized and what was taking place.[59]

---

[55] Ibid

[56] Ibid, 295

[57] "Constitution of the United States"

[58] Hayden, in conversation with the author, September 21, 2015

[59] Savage, "George W. Bush Made…"

Further reservations about the program were eventually voiced by Senator John D. Rockefeller IV (D-WV), a Foreign Intelligence Surveillance Court judge, and several members of the IC itself.[60] According to Charlie Savage of the *New York Times*, "a threat of mass resignation by top [Justice] department officials" was what eventually prompted President Bush "to accept curbs on the program."[61]

All of this took place in a world where the attitude of the NSA, expressed to James Bamford by an intercept operator from the agency, was that "[b]asically all rules were thrown out the window, and they would use any excuse to justify a waiver to spy on Americans." This included American journalists, Red Cross workers, and businesspeople working in the Middle East, people who should have been protected by FISA, E.O. 12333, and most importantly the United States Constitution.[62] Although the executive order grants authority to the Attorney General to issue waivers to conduct electronic surveillance of U.S. persons if the investigation is for non-law enforcement purposes, it does require that there be "probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power."[63] Because the NSA was spying on American citizens who could only be tried in civilian courts—with the exception of members of the uniformed military—any such investigation would have to be for law enforcement purposes.

The same general controversy is still active at the time of the writing of this thesis as the public, courts, the executive branch and Congress argue over the rights of citizens

---

[60] Risen and Lichtblau

[61] Savage, "George W. Bush Made…"

[62] Bamford, *The Shadow Factory*, 1

[63] "Executive Order 12333." *See* Part 2, section 2.5, "Attorney General Approval."

and the responsibilities of government. Many of the programs revealed by Edward Snowden are direct successors to STELLARWIND, and PRISM was originally a part of the President's Surveillance Program.[64]

Edward Snowden Leaks

On June 5th, 2013, London's *The Guardian* published an article that declared that the "National Security Agency is currently collecting the telephone records of millions of US customers of Verizon, one of America's largest telecoms providers."[65] Over the next several months, led by Glenn Greenwald, Ewen MacAskill, Barton Gellman, and numerous other journalists, *The Guardian*, the *Washington Post*, the *New York Times*, and several European news organizations such as *Der Spiegel* released hundreds of articles detailing NSA programs that collected, analyzed, and searched internet, phone, and text data from all over the world. Edward Snowden passed documents and information to reporters either via encrypted e-mails or USB detachable hard drives in Hong Kong.[66]

Much of what NSA collected is known as "metadata," which is defined as "information wireless carriers collect about where, when and to whom customers make phone calls… [M]etadata can contain phone numbers, the time and duration of calls and the location of the caller and the recipient… It can include which cellular towers were

[64] Lindsey Boerma, "NSA Secretly Mining User Data from U.S. Internet Giants," last updated June 7, 2013, http://www.cbsnews.com/news/nsa-secretly-mining-user-data-from-us-internet-giants/

[65] Greenwald, "NSA Collecting Phone Records…"

[66] *Citizenfour*

used to transmit the call and what kind of phone was being used."[67] As one journalist put it, metadata is "data about data."[68] Additionally, as will be seen in the following chapter, some of the these programs were picking up more than just the bare metadata and were, in fact, collecting entire internet-based phone calls, Skype sessions, and emails.

Snowden approached first Greenwald in December 2012, then eventually Laura Poitras, due to their noted opposition to American intelligence efforts in the internet era.[69] Snowden had written to Poitras after Greenwald failed to respond to him in a timely manner, telling her that he had access to, and intended to leak, "some extremely secret and incriminating documents about the US government spying on its own citizens and on the rest of the world…and specifically requested that she work with [Greenwald] on releasing and reporting on them."[70] He went on to explain his reasoning for the leaks:

> We [referring to Poitras and himself] can guarantee for all people equal protection against unreasonable search through universal laws… [W]e must enforce a principle whereby the only way the powerful may enjoy privacy is when it is the same kind shared by the ordinary: one enforced by the laws of nature, rather than the policies of man.[71]

This showed clearly what Snowden's motives and intentions were: he wanted first to "out" the intelligence community for doing something he considered to be wrong, although not necessarily illegal, and he wanted to enforce his own set of moral ideals on the IC's collection methods and programs. In Greenwald and Poitras, Snowden found

---

[67] David Goldman, "Obama and NSA: So What is Metadata Anyway?" *CNN*, January 17, 2014, http://money.cnn.com/2014/01/17/technology/security/obama-metadata-nsa/

[68] Jeff Stone, "What is 'Metadata?' NSA Loses Surveillance Power on American Phone Calls, but 'Data About Data' Remains Hazy," *International Business Times*, June 2, 2015, http://www.ibtimes.com/what-metadata-nsa-loses-surveillance-power-american-phone-calls-data-about-data-1947196

[69] *Citizenfour*; and Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (New York: Metropolitan Books, 2014), 7-8, 11-13

[70] Ibid, 12

[71] Ibid, 13

two people who felt much the same as he, with strong anti-government feelings, particularly as they applied to intelligence.

Within weeks of the leaks becoming public, the U.S. Department of Justice (DoJ) leveled criminal charges against Snowden. The charging document, filed in the United States District Court for the Eastern District of Virginia on June 14th, 2013, alleges that Snowden, by copying classified files and releasing them to Poitras, Greenwald, and others, violated 18 U.S.C. §641 (Theft of Government Property), §793(d) (Unauthorized Communication of National Defense Information), and §798(a)(3) (Willful Unauthorized Communication of Classified Communications Intelligence Information to an Unauthorized Person).[72] Despite his repeated assertions to Poitras and Greenwald that he was prepared to face trial, and indeed wanted to have his day in court,[73] as of this writing Edward Snowden had not returned to the United States and is residing in Russia. Snowden claims that he originally intended to flee to Latin America, and never intended to go to Russia.[74]

[72] "U.S. vs. Edward J. Snowden Criminal Complaint," *Washington Post*, last accessed February 2, 2016, http://apps.washingtonpost.com/g/documents/world/us-vs-edward-j-snowden-criminal-complaint/496/

[73] *Citizenfour*

[74] Katrina vanden Heuvel and Stephen F. Cohen, "Edward Snowden: A 'Nation' Interview," *The Nation*, November 17, 2014, http://www.thenation.com/article/snowden-exile-exclusive-interview/

PROGRAMS OF NOTE

Rather than focusing on known targets with articulable terrorist connections, the National Security Agency has adopted several programs that mine data from a wide range of non-specific targets. Because of the top secret nature of the programs, it is not possible for this thesis to determine whether they are truly successful, but it is worth noting the absence of any major terrorist activities on United States soil or against major American targets in the nearly fifteen years since the World Trade Center attacks. This is not necessarily proof of triumph, as proving a negative is impossible, but considering what is known about how capable some terrorist organizations are, and their destructive goals, it is hard to imagine that they have not made numerous attempts to strike at the American homeland. The fact that many of the publicized attempts made have been simple[75] or "amateurish" and easily foiled[76] seems to speak to a more anxious, or even desperate, opponent whose attempts to strike at the United States have been thwarted at every turn.

Even assuming the programs are successful, that does not mean they are legal, moral, or ethical. However, it would also be foolish to accept on faith that reporters like Greenwald and filmmakers like Poitras, not to mention leakers of classified documents like Edward Snowden, are right in saying that these untargeted, mass-data programs are

[75] David Ariosto and Deborah Feyerick, "Christmas Day bomber sentenced to life in prison," *CNN*, February 17, 2012, http://www.cnn.com/2012/02/16/justice/michigan-underwear-bomber-sentencing/. The "Underwear Bomber" was poorly trained at best, and was easily stopped by his fellow passengers as he attempted to detonate.

[76] Al Baker and William K. Rashbaum, "Police Find Car Bomb in Times Square," *New York Times*, May 1, 2010, http://www.nytimes.com/2010/05/02/nyregion/02timessquare.html?pagewanted=all&_r=0. A crude bomb, which failed to properly detonate, was noticed when the SUV that contained it began to emit significant amounts of smoke, alerting a nearby merchant who flagged down police.

illegal. Each program is unique, has its own constitutional questions, and must be evaluated individually before broader conclusions are possible.

Examining classified programs while only having access to limited information and documents is a significant challenge, and presenting a full and impartial summary of them when the documents that are available were selectively released by individuals with an agenda is even more difficult. Because of this, great care has been exercised in attempting to locate as accurate and unbiased information as possible, through personal examination of the documents that were leaked by Edward Snowden, learned opinions from experts and journalists who have spent their entire careers covering the national security and intelligence fields, and, of course, the statutes that led to these programs. While the rest of this thesis includes inferences and assumptions by necessity, this section contains as few as possible.

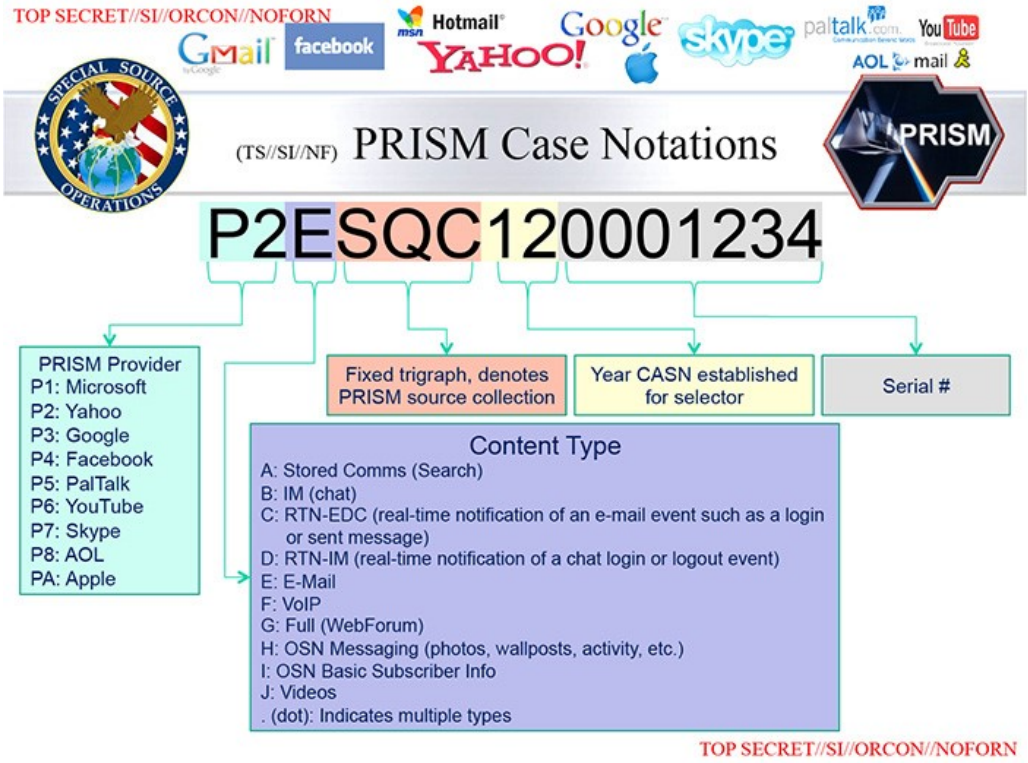
PRISM

The computer program called PRISM, disclosed early in the leaked articles by both *Washington Post* and *The Guardian* journalists, is far and away the best known and most debated of the programs revealed by Edward Snowden in 2013.[77] PRISM has become synonymous with all programs conducted under the auspices of section 702 of the FISA Amendments Act of 2008, and will be used in that manner hereafter.[78] Warrants were issued under the auspices of this program to compel telecommunications companies to provide access to, among others: stored communications (searches); instant

[77] Google News searches for PRISM NSA, MUSCULAR NSA, and BOUNDLESS INFORMANT NSA result in returns of "about" 31900, 5960, and 701, respectively

[78] Benjamin Dreyfuss and Emily Dreyfuss, "What is the NSA's PRISM Program? (FAQ)," *CNET*, last updated June 7, 2013, http://www.cnet.com/news/what-is-the-nsas-prism-program-faq/

messaging/chat services; and even real-time information on chat and email log-ins or Voice over Internet Protocol (VoIP) usage.[79] The DoJ sent PRISM program subpoenas to some of the most widely used and largest companies,[80] not just in the telecommunications industry, but in the world.[81] These companies were clearly labeled as "providers" for the program in NSA slides. (See Figure 2)[82] Unlike programs such as MUSCULAR, detailed below, PRISM court orders gave companies the opportunity to fight the U.S. government,



F2: Slide from NSA presentation on PRISM capabilities. Shows providers and types of contact that can be collected, in the context of establishing a PRISM case number

[79] "NSA Slides Explain the PRISM Data-Collection Program," *Washington Post*, last updated July 10, 2013, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

[80] Ibid

[81] "Global Top 100 Companies by Market Capitalization," *PwC IPO Centre* (London, England: March 31, 2014), 39. Since the publication of this report, Google and Microsoft have moved ahead of Exxon Mobile, to join Apple in the top three.

[82] "NSA Slides Explain the…"

including most notably Yahoo!, which "viewed [PRISM] as unconstitutional and overbroad surveillance," resulting in the company having "challenged the U.S. Government's authority"[83] for several years. Yahoo! only began complying with the order when the federal government threatened to impose fines of $250,000 *per day* on the company,[84] an existential threat even to a corporation with a market capitalization of over $40 billion.[85] Microsoft, the only company to precede Yahoo! in the program, complied fully with the government, including providing backdoor access to many applications.[86] (See Figure 3)[87]

According to the *Washington Post*, PRISM allowed the NSA and FBI to tap "directly into the central servers of nine leading U.S. internet companies, extracting audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets."[88] PRISM retrieved mass amounts of data directly from these nine companies, rather than the small, specifically targeted amounts a warrant typically allows. The court agreed to issue "four new orders…[which] defined massive data sets as 'facilities," provided that the government allowed the FISC to "certify periodically that the government had reasonable" minimization procedures in place.[89]

---

[83] Bell

[84] Ibid

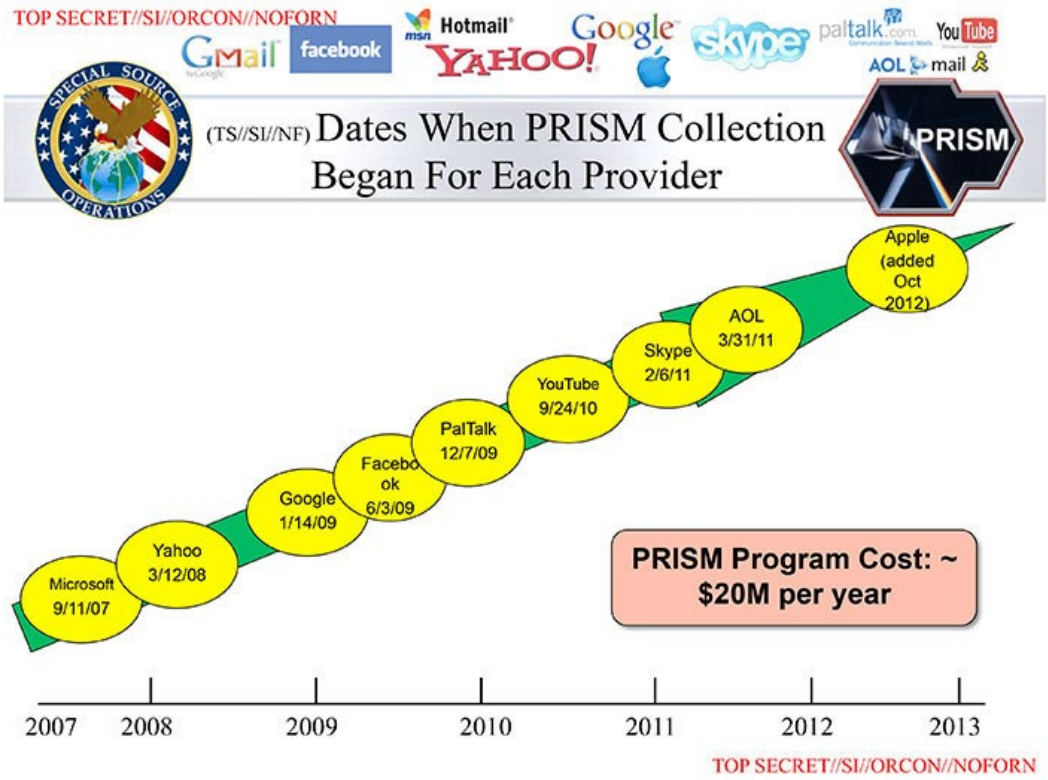
[85] "Yahoo! Inc. (YHOO)," *Yahoo! Finance*, accessed April 26, 2015, http://finance.yahoo.com/q?s=YHOO. Accurate as of April 24, 2015.

[86] Glenn Greenwald, et al, "Microsoft Handed the NSA Access to Encrypted Messages," *The Guardian*, July 12, 2013, http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

[87] "NSA Slides Explain…"

[88] Barton Gellman and Laura Poitras, "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program," *Washington Post*, June 7, 2013, https://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

[89] Ibid



F3: Slide from NSA presentation showing dates various companies were added to the PRISM program. Yahoo! is the only company to publicly state that they fought the program, while others such as Facebook and Apple deny having any knowledge of the government's access

In order to initiate this access, the government would send a "directive" to an internet service provider (ISP) or content provider, approved by the Attorney General and Director of National Intelligence "compelling the providers assistance."[90] The Privacy and Civil Liberties Oversight Board (PCLOB), which studied the legality and effectiveness of the 702 programs, explained how PRISM collection worked in an invented scenario.

> The NSA learns that John Target, a non-U.S. person located outside the United States, uses the email address johntarget@usa-ISP.com to communicate with associates about his efforts to engage in international terrorism. The NSA applies

[90] "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," *Privacy and Civil Liberties Oversight Board*, July 2, 2014, available at https://www.pclob.gov/library/702-Report.pdf, 32

> its targeting procedures…and "tasks" johntarget@usa-ISP.com to Section 702 acquisition for the purpose of acquiring information about John Target's involvement in international terrorism. The FBI would then contact USA-ISP Company (a company that has previously been sent a Section 702 directive) and instruct USA-ISP Company to provide to the government all communications *to or from* email address johntarget@usa-ISP.com. The acquisition continues until the government "detasks" johntarget@usa-ISP.com.[91] (Emphasis added)

In addition to direct access to systems controlled by ISPs and content producers, the same authority from which PRISM was derived led to a program referred to as "upstream collection." This allowed the NSA to access the systems of the so-called "backbone" of the internet,[92] the routers that actually move data throughout the interconnected virtual world.[93] Rather than simply acquiring the "to or from" emails (or whichever other tasked selector was being used) of a particular target, it also allowed the NSA to collect communications *about* the target. The PCLOB explained this type of collection as "one in which the tasked selector is referenced within the acquired Internet transaction, but the target is not necessarily a participant in the communication."[94]

Presumably, the NSA used these orders and direct access to the various companies in order to spy only on the internet activity of foreign terrorism suspects. However, with a direct line into a company's system, and with access to "about" communications, it would be easy for the NSA to, either intentionally or accidentally, collect significant amounts of data from U.S. persons. In a case where this is accidental, there are procedures in place to "minimize" the collected data. Minimization is the

---

[91] Ibid, 34

[92] Ibid, 36-39

[93] A simple explanation of how the infrastructure of the internet works is available at http://computer.howstuffworks.com/internet/basics/internet-infrastructure.htm

[94] "Report on the Surveillance…," 37

process by which intelligence or law enforcement agencies erase or censor information related to U.S. persons to protect their privacy.[95]

Ordinarily if a U.S. intelligence agency captured an American's emails or other communication, minimization procedures would require them to delete the data immediately upon discovery, and in fact the NSA has computer systems designed to catch this and erase the data before a human being even has access. However, "wholly domestic communications could be acquired as much as 0.197% of the time" when NSA is picking up "about" communications due to flaws in IP filter programs.[96] While this number seems to be quite small, the enormous amount of communications data collected means that "upstream collection could result in the government acquiring as many as tens of thousands of wholly domestic communications per year."[97] This data should be manually deleted, but if a captured email or "instant message" from a U.S. person, protected by the Fourth Amendment, contains clear evidence of a major felony or terrorist act, that information will be passed on to the FBI.[98] Rather than being the "fruit of the poisonous tree" that would make not only that evidence but anything further derived from it or the knowledge of it inadmissible in court,[99] this evidence would allow the FBI to open a full investigation.[100] The U.S. government's approach to incidental

[95] *See* 50 U.S. Code §1806(A) for the U.S. government's definition and basic requirements for minimization

[96] Report on the Surveillance…," 38

[97] Ibid, 39

[98] Marc Ambinder, "Solving the Mystery of PRISM," *The Week*, June 7, 2013, http://theweek.com/articles/463418/solving-mystery-prism

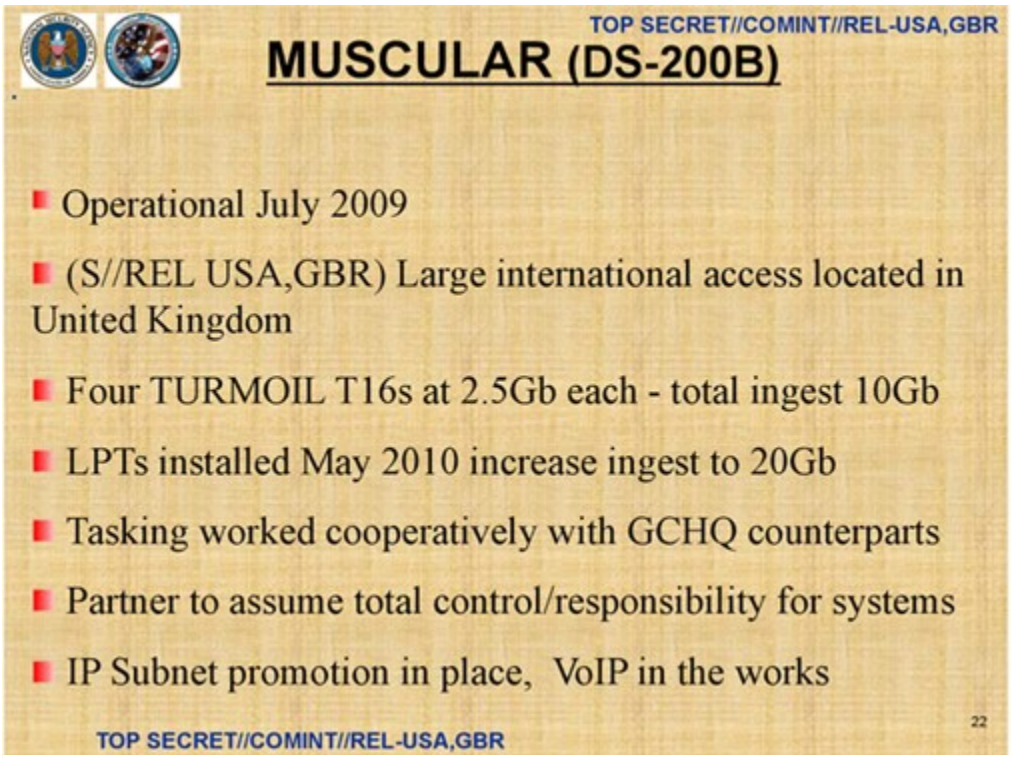
[99] *See* "Fruit of the Poisonous Tree," *Cornell University Law School Legal Information Institute*, last accessed March 5, 2016, https://www.law.cornell.edu/wex/fruit_of_the_poisonous_tree

[100] Ambinder

collection does bear strong similarities to its policies on collateral damage in war; attempting to avoid it, and minimizing where avoidance is impossible.

MUSCULAR

The program known as "MUSCULAR" was identified in the *Washington Post* as "collect[ing] the internet 'cloud' traffic of Yahoo! and Google from an interception point on British territory," with the ability to "store 10 gigabytes a day of processed traffic [in 2009];" capacity may have as much as quadrupled at the present time.[101] (See Figure 4)[102] According to published reports, this program was undertaken without the



F4: NSA slide from presentation on Special Source Operations leaked by Edward Snowden. It shows the storage capacity of the program and its cooperative nature with Britain's Government Communications Headquarters, the United Kingdom's version of NSA

[101] Gellman and Delong

[102] Ibid

knowledge of the targeted companies, and Google claimed to be "'outraged' by the revelation."[103]

The cloud is an internet storage and software medium that allows a person to access data across multiple devices in non-static locations. Companies like Yahoo! and Google store billions of images, emails, instant messages, and other communications items on the cloud at any given moment; every major internet company uses it in some manner, often without customers truly knowing or understanding what it is or how it works. The cloud is now so ubiquitous that the server "farms" that support it were, as of 2014, "responsible for more than 2% of the United States' electricity usage."[104] Because of this widespread usage, the NSA directly accessing Yahoo!'s and Google's cloud traffic gave it the opportunity to retrieve records numbering in the hundreds of millions. According to one document dated June 9th, 2013 that was leaked by Edward Snowden, in the preceding month MUSCULAR collected upwards of 180 million new records.[105] Like with PRISM, the law of large numbers applies: if even a tiny percentage of the more than two billion records—assuming a relatively similar number of captured items each month—are from protected U.S. persons, there will be tens of thousands, if not millions of pieces of data that were captured in violation of the Fourth Amendment. This is especially likely considering that "[m]any cloud providers engage in 'georedundancy'

---

[103] Chloe Albanesius, "Report: NSA Secretly Spied on Yahoo, Google Data Centers," *PC Magazine*, October 30, 2013, http://www.pcmag.com/article2/0,2817,2426590,00.asp

[104] David Goldman, "What is the Cloud?" *CNN*, September 4, 2014, http://money.cnn.com/2014/09/03/technology/enterprise/what-is-the-cloud/

[105] Considering the total amount of email traffic on a daily basis worldwide, this is actually a relatively miniscule number. A report by a private marketing firm estimated that over 205 billion emails were sent and received every day in 2015, and that number is likely to grow significantly. *See* "Email Statistics Report, 2015-2019," *Radicati Group, Inc.*, March 2015, available at http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf

efforts, which result in vast amounts of customer data sent to and from other datacenters to ensure that the data is always available."[106] Thus, data that is stored in the British Isles is not necessarily from outside the United States, even though both Yahoo! and Google have datacenters in America.

Considering the amount of data that was mined in this operation, and the ubiquity of use of each of these companies' products and services in the United States, Americans' data was sure to have been captured. This program was also undertaken without warrants and provided the NSA access, even if it does not intentionally take advantage, to a variety of information on United States citizens or other protected U.S. persons.

The program itself is primarily operated by the United Kingdom's Government Communications Headquarters (GCHQ), that country's signals intelligence agency and the British equivalent of the NSA. That distinction could be why General Keith Alexander, who was director of the NSA at the time of the Snowden leaks, said that NSA did not break into the two companies' databases, saying "[i]t would be illegal for [NSA] to do that." However, E.O. 12333 bans the intelligence community from requesting or demanding any actions from any person or organization that, if conducted by a member of the IC, would be illegal. Therefore, if NSA cannot legally gain access to Yahoo! or Google servers in this manner, it is also illegal to request that GCHQ provide assistance in doing so, or to request information derived from those servers.

Former NSA General Counsel Rajesh De, in response to a query about MUSCULAR at a PCLOB public hearing in November of 2013, refused to confirm or deny the program's existence, but did say the following: "[A]s a general matter…any

[106] Zack Whittaker, "Meet 'Muscular': NSA Accused of Tapping Links Between Yahoo, Google Datacenters," *ZDNet*, October 30, 2013, http://www.zdnet.com/article/meet-muscular-nsa-accused-of-tapping-links-between-yahoo-google-datacenters/

collection NSA does would involve minimization procedures that are approved by the Attorney General, or if coverage were under FISA, by the FISC, that has rules in place to minimize the collection, retention and use of any incidentally collected U.S. person information."[107] In essence, De said that even if this program were exactly what journalists alleged it was, procedures were in place that would minimize the impact on U.S. persons.

The NSA refuted the claim that Americans were subjected to any violation of their rights, and released a statement saying: "NSA applies Attorney General-approved processes to protect the privacy of U.S. persons—minimizing the likelihood of their information in our targeting, collection, processing, exploitation, retention and dissemination. NSA is a foreign intelligence agency…[only] focused on discovering and developing intelligence about valid foreign intelligence targets."[108] In all likelihood, this is a very factual statement; it is hard to imagine that the NSA—which employs tens of thousands of patriotic Americans, including military personnel who have often given up opportunities to earn greater pay to work to help secure the safety of the United States—are going to work plotting how to violate peoples' rights. Searches of the information collected by MUSCULAR and the programs like it are limited by policy and regulation, and only a small number of people have access.[109]

---

[107] *Privacy and Civil Liberties Oversight Board*, "Public Hearing: Consideration of Recommendations for Change: The Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act" (transcript, Washington, D.C., 2013), 11

[108] Quoted in: Albanesius, "Report: NSA Secretly…"

[109] Darby

BOUNDLESSINFORMANT

All the information pulled into NSA databases by PRISM, MUSCULAR, and a myriad of other programs just results in massive banks of computer servers being filled; BOUNDLESSINFORMANT[110] is the computer program that allows analysts to access, search, and pull specific files and information from the NSA's server banks where collected data are stored. Without BOUNDLESSINFORMANT, some of the other programs would be essentially worthless, like mining ore without having a smelter to extract the valuable portions. *The Guardian* reported that Snowden-leaked documents show "it is designed to give NSA officials answers to questions like, 'What type of coverage do we have on country X' in 'near real-time by asking the SIGINT infrastructure.'"[111] For this reason BOUNDLESSINFORMANT may be the most valuable of the three programs examined herein as it allows the NSA to do actual analysis, not merely collection of intelligence.

It is also the least known of the four programs examined herein, but it has the potential to be the most controversial. Slides showing statistics like the acquisition of, as Greenwald and MacAskill wrote, "almost 3 *billion* pieces of intelligence from US computer networks over a 30-day period"[112] [emphasis added] are sure to make excellent fodder for those looking to bash the National Security Agency, the administrations of

---

[110] General Hayden, in a Munk Debate in Toronto, joked that "if I were actually thinking of names that would eventually become public, that's probably not one I would pick." The entire debate is available at https://www.youtube.com/watch?v=_d1tw3mEOoE

[111] Glenn Greenwald and Ewen MacAskill, "Boundless Informant: the NSA's Secret Tool to Track Global Surveillance Data," *The Guardian*, June 11, 2013, http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining. The ability to search for information on a particular country is not the least bit concerning from a legal standpoint, but the impressive capabilities of BOUNDLESSINFORMANT could easily be turned to search for information on protected U.S. persons.

[112] Ibid

Presidents Bush and Obama, or the intelligence community as a whole. (See Figure 5)[113] Despite Greenwald and MacAskill's inflammatory arguments in *The Guardian*, this is probably the most easily defended program as it simply a tool to search records, not capture them. Therefore, while it could easily be used by a rogue employee illegally,

F5: NSA slide BOUNDLESSINFORMANT overview leaked by Edward Snowden program showing the amount of data that are collected (and thus searchable by this program) from various countries around the world, including the United States

there is no way to point to it as being inherently unlawful itself, whereas that argument can be (and has been) applied to the others. It is only in concert with programs like PRISM and MUSCULAR that BOUNDLESSINFORMANT becomes suspect by association; taken alone, or with other NSA programs determined to be legal and ethical, it poses no great issue.

However, when programs collect data that BOUNDLESSINFORMANT can search, and that data was obtained in a legally questionable manner, the search program contributes to the illegality by extension. Using illegally collected data is also inherently

[113] Ibid

a violation of the law, and BOUNDLESSINFORMANT makes it significantly easier to do exactly that. While the program is a spectacular tool, it is also the most easily abused program discussed in this thesis. Like all other NSA programs, there are limitations on the program including minimization and tasking requirements, but in rare cases NSA employees have abused surveillance authority according to a report by the agency's inspector general.[114] This tool simply makes it easier to do so.

XKEYSCORE

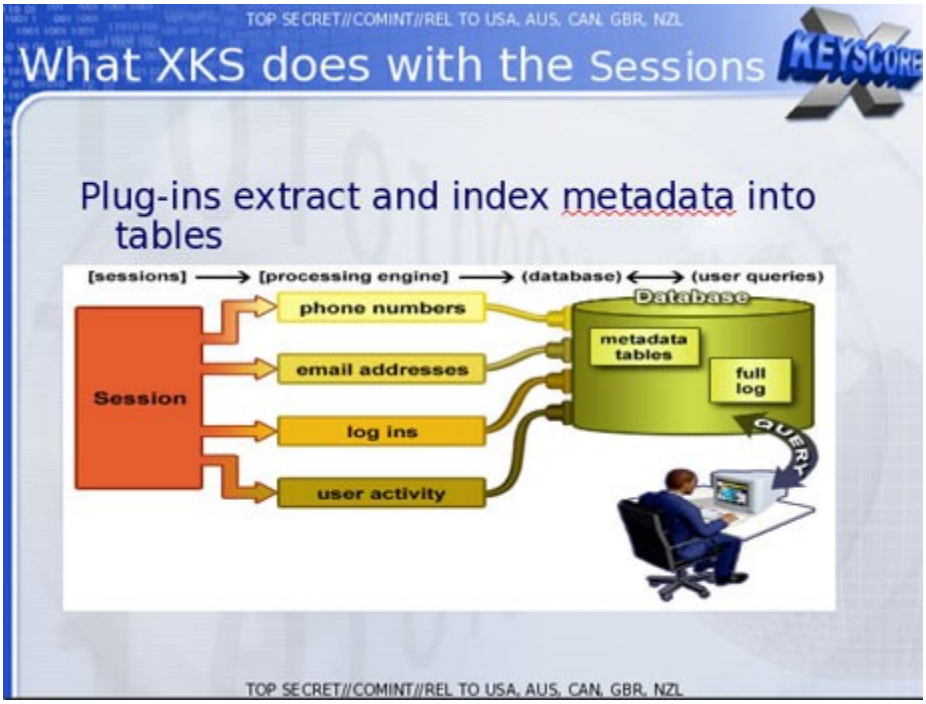
XKEYSCORE is a computer application designed for one thing: data mining, and lots of it. As part of what the NSA refers to as "Digital Network Intelligence" (DNI), it has the capability to track, as one NSA presentation on the program stated, "nearly everything a typical user does on the internet." This includes email, website visits, and metadata. (See Figures 6 and 7)[115] Searches via the program's interface could easily target Americans or other U.S. persons without the need for a court order, simply because XKEYSCORE automatically scooped up internet data irrespective of the nationality or protected status of the originating user.[116] According to reports, this data is collected from more than one hundred field sites in countries all over the world via fiber optic cables similar to the upstream collection of the aforementioned PRISM programs. It is then stored for three to five days in the case of "full-take data" and four to six weeks for

[114] Chris Strohm, "Lawmakers Probe Willful Abuses of Power by NSA Analysts," *Bloomberg*, August 24, 2013, http://www.bloomberg.com/news/articles/2013-08-23/nsa-analysts-intentionally-abused-spying-powers-multiple-times

[115] "XKeyscore Presentation From 2008 – Read in Full," *Guardian* (London), Wednesday, July 31, 2013, http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation

[116] Glenn Greenwald, "XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet," *Guardian* (London), July 31, 2013, http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

metadata.[117] Full-take data is everything that passes through the fiber optic cables, including emails, VoIP and Skype calls, internet searches, and much more. HBO's John Oliver, in a comic segment with Edward Snowden in an April 2015 episode of his show *Last Week Tonight*, discussed how this meant that very private, intimate images that a man may send someone would be picked up by this kind of program, stored for a period of time, and be searchable by, according to Snowden, anyone within NSA.[118] Despite its wide reaching nature, according to *The Intercept*, XKEYSCORE is actually an extremely basic software program, running on linked Linux servers and accessible by standard web



F6: Training slide "What XKS does with the Sessions" showing XKEYSCORE (referred to as "XKS") capabilities, including collecting user activity, metadata, and other internet activity

[117] Morgan Marquis-Boire, Glenn Greenwald, and Micah Lee, "XKEYSCORE: NSA's Google for the World's Private Communications," *The Intercept*, July 1, 2015, https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/

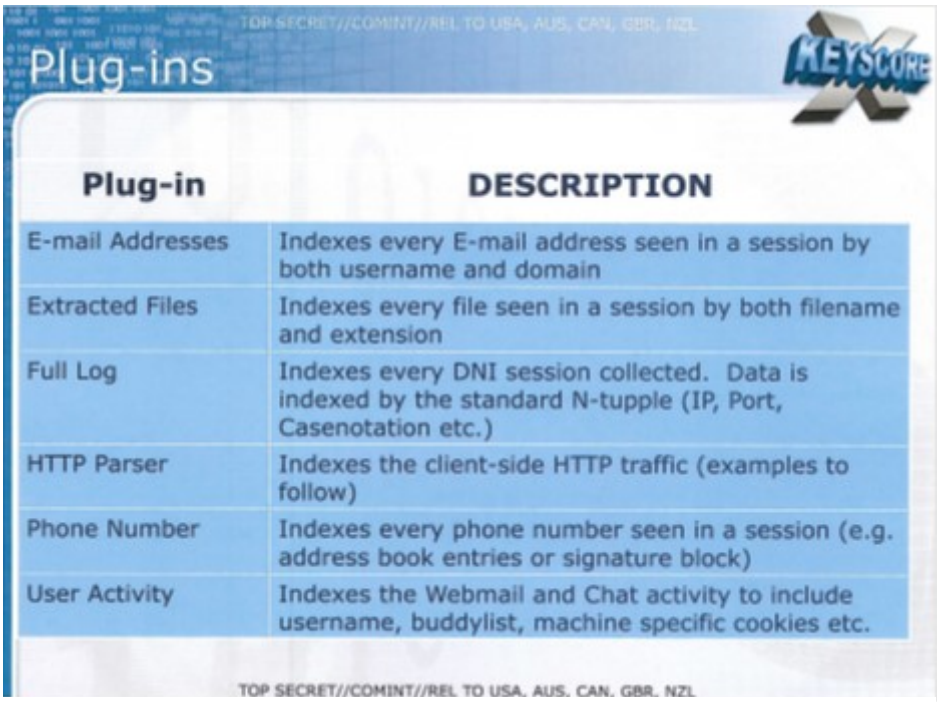
[118] Edward Snowden, interview by John Oliver, *Last Week Tonight with John Oliver*, HBO, April 5, 2015. The full episode is viewable at https://www.youtube.com/watch?v=XEVlyP4_11M

browsers such as Mozilla's Firefox.[119]

Similarly, *The Intercept* writers Morgan Marquis-Borie, Glenn Greenwald, and Micah Lee claim that

> XKEYSCORE also collects and processes Internet traffic from Americans, though NSA analysts are taught to avoid querying the system in ways that might result in spying on U.S. data… [However], [o]ne document *The Intercept*…[published] suggests that FISA warrants have authorized "full-take" collection of traffic from at least some U.S. web forums.[120]

They also allege that a leaked 2013 NSA document entitled "VoIP Configuration and Forwarding Read Me" proves that the NSA is collecting voice calls, videos, and faxes numbering in the hundreds of thousands per day, although they do not specifically



F7: NSA training slide "Plug Ins" addressing XKEYSCORE capabilities, including extracting chat activity, entries in an "address book" online, and the filename and extension of every file seen during an internet session

[119] Micah Lee, Glenn Greenwald, and Morgan Marquis-Boire, "Behind the Curtain: A Look at the Inner Workings of NSA's XKEYSCORE," *The Intercept*, July 2, 2015, https://theintercept.com/2015/07/02/look-under-hood-xkeyscore/

[120] Marquis-Boire, Greenwald, and Lee, "KXEYSCORE: NSA's Google for…"

contend that any of these are from protected U.S. persons.[121] Greenwald claimed in a July 2013 article that exposed XKEYSCORE that much of this collection can be done in "real-time," meaning that it takes place as the actual incident is occurring.[122]

These assertions run contrary to the contentions by many, including Director of National Intelligence James Clapper, that foreign-oriented U.S. intelligence agencies do not routinely surveil "millions of Americans,"[123] and those of former NSA Director General Keith Alexander that his agency neither surveils nor collects the emails, Google searches, phone calls or text messages of Americans,[124] both in 2013. In fact, when viewed with the knowledge of the PRISM and MUSCULAR programs, it is virtually impossible to conclude anything other than the fact that the National Security Agency has routinely conducted operations and used programs that allow for the capture of data, beyond simple metadata, transmitted and received by American citizens and other U.S. persons. What DNI Clapper and General Alexander may have meant is that the NSA does not intentionally surveil or collect on Americans, or that this collection is minimized upon its discovery in the agency's servers.

Additional Thoughts

As Glenn Greenwald wrote in his book describing the process of meeting and revealing Edward Snowden, *No Place to Hide*, "it can be hard to generate serious concern about secret state surveillance: invasion of privacy and abuse of power can be viewed as

---

[121] Ibid

[122] Greenwald, "XKeyscore: NSA Tool Collects…"

[123] James Clapper (testimony before Senate Select Committee on Intelligence, Washington, D.C., March 12, 2013)

[124] *Citizenfour*

abstractions, ones that are difficult to get people to care about viscerally…[t]he issue of surveillance is invariably complex."[125] This is clearly evident in the slides shown above; even the simplest of them requires some context to interpret their meaning as they pertain to the rights and privileges of U.S. persons versus those of the rest of the world.

With the proper context, details, and background, and with all of them put together, these four programs give a far clearer indication of what it is that the National Security Agency has been doing for the last decade in terms of domestic collection of signals intelligence. This includes the use of sophisticated technology, direct lines into the infrastructure of some of the leading telecommunications companies in the United States and abroad, and storage of potentially trillions of records. Considering the size of a new NSA data storage facility in Utah, with approximately 100,000 square feet—more than two acres, or about the size of a regulation soccer field, and about two-thirds the size of Facebook's newest server center, which will "have servers installed in line with demand"[126]—of server rooms, and the fact that this facility is certainly not unique, it is impossible to come to any conclusion other than that NSA believes it will, and indeed intends to, retain the need to store immense amounts of raw data.[127] In the "olden days" of the 1980s and 1990s, that much data would have been an overabundance, far too much raw information for the NSA to have much ability to sort and analyze due to the technological limitations of the time.

---

[125] Greenwald, *No Place to Hide,* 19

[126] "Press Release: Facebook Opens First Data Center in Prineville, Oregon," *Facebook*, April 15, 2011, https://www.facebook.com/notes/prineville-data-center/press-release-facebook-opens-first-data-center-in-prineville-oregon/10150150581753133/. Facebook has over 1.4 billion monthly active users, according to financial reporting for first quarter 2015. *See* "Facebook Reports First Quarter 2015 Results," *Facebook*, April 22, 2015, http://investor.fb.com/releasedetail.cfm?ReleaseID=908022

[127] James Bamford, "The NSA is Building the Country's Biggest Spy Center (Watch What You Say)," *Wired*, March 15, 2012, http://www.wired.com/2012/03/ff_nsadatacenter/

Now, with BOUNDLESSINFORMANT and XKEYSCORE, the NSA has the ability to rapidly sort and search much of that data. Some observers, including television news personality Lawrence O'Donnell, have said that this massive collection makes them feel less worried about surveillance. O'Donnell was quoted as saying "the fact that the government is collecting at such a gigantic, massive level means that it's even harder for the government to find me."[128] There is still an element of truth in this, not least of which is that there are also so many potential targets that it is highly unlikely that the government is going to *want* to find you. As *Washington Post* writer Ruth Marcus said, "my metadata almost certainly hasn't been scrutinized,"[129] but this attitude ignores the fact that the NSA has developed programs that allow it to find your metadata, and more, if someone in the agency decides that it is relevant.

Edward Snowden claimed that he "could wiretap anyone, from you or your accountant, to a federal judge or even the president, if I had a personal email." This was vehemently denied by NSA Director Admiral Michael Rogers, saying that that was "impossible."[130] While it may well be accurate that Snowden himself did not have this capability, an examination of the various XKEYSCORE slides makes it abundantly clear that *someone* had this option. Of course, it is also possible that Snowden did have this capability due to his position within the agency's information technology support unit, but should not have. More importantly, there does not appear to be any mechanism to prevent an analyst or other official who does, and should, have access to this program

[128] Quoted in: Greenwald, *No Place to Hide*, 195

[129] Quoted in: Ibid, 196

[130] Ibid, 157

from using it for unofficial reasons or without the expressed permission of a federal judge.

Regardless of the legality of these programs, which will be addressed at length in the following chapter, the safeguards in place would not prevent a rogue analyst from violating peoples' rights. The small number of people with access to these special programs has been presented as a reason not to worry about abuses,[131] but it seems that an alternative way of examining this issue would be that the fewer people who know about something, the more likely they are to abuse it. This was certainly the case in the early 2000s when the Office of the Vice President severely limited the number of people who had access to the illegal wiretapping program that was being run out of the NSA. Special access programs limit the number of people involved, but they also limit the number of people watching. Obviously some programs need to be closely guarded, and anything involving SIGINT methods is likely to be included in that category, but simply having a small number of people with access is not a safeguard against abuse.

The best safeguard is likely the one that General Hayden mentioned: the "sensitivity" to any issues involving the Fourth Amendment.[132] No one wants to be "that guy" who screwed up, and, as mentioned, NSA workers are not likely to be people with an inherent desire or intent to harm other Americans.

[131] Darby

[132] Hayden, in discussion with the author, September 21, 2015

LEGAL ARGUMENTS

If nothing else is clear about the situation in which Edward Snowden has ensnarled himself, it is that he violated the law, his legally binding agreement upon being hired by Booz Allen Hamilton, and the confidentiality agreement he signed upon being assigned to work as a contractor with the National Security Agency.[133] Unfortunately, Snowden's apparent guilt or innocence do not make the legal questions surrounding the collection of metadata and other methods of surveilling domestic communications any simpler. Rather, it may be the only thing about the NSA's surveillance programs that provides more clarity than opacity. Law is inherently a matter of interpretation, hence why the findings of a court are referred to as opinions; Constitutional law is even more so. Facts are hard to ascertain; one person's version of fact is another's opinion, made all the more difficult by the apparent intransigence of most legal scholars who rarely change their minds on an issue regardless of what evidence is presented to them. Interpretations do change, but it is often over the course of decades or generations, not in days or months or even years. The law is, as the former Chief Justice of the Ohio Supreme Court put it, a "product of the ages—wrapped in the opinion of the moment."[134]

The question of the legality of the collection of domestic metadata and other communications and signals intelligence is primarily one of Constitutional law, but the programs themselves derive their authorities from ordinary statutes. The most important of these statutes are the aforementioned Foreign Intelligence Surveillance Act of 1978

[133] *Citizenfour*

[134] Thomas J. Moyer, "State of the Judiciary" (speech before the judges and justices of the Ohio court system, Columbus, OH, September 11, 2008)

(and its various amendments), specifically Section 702 of the 2008 FISA Amendments Act, and Section 215 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001: the USA PATRIOT Act.

Section 702 authorized the PRISM program, which the government argues is entirely aimed outside the United States.[135] It authorizes, "for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[136] This portion of the FISA Amendments Act of 2008 includes a subsection on limitations, which states:

> An acquisition authorized under subsection (a) — (1) may not intentionally target any person known at the time of the acquisition to be located in the United States; (2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States; (3) may not intentionally target a United States person reasonably believed to be located outside the United States; (4) may not intentionally acquire any communications as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and (5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.[137]

The clear intention of this part of the Act was to ensure that American citizens and other U.S. persons were not targeted by the intelligence community during its counterterrorism and counterintelligence searches. Due to the specific prohibitions on targeting U.S.

---

[135] "Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," *Office of the Director of National Intelligence*, June 8, 2013, http://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf

[136] "H.R. 6304: Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (110th Congress, 2007-2008)," *Library of Congress*, last accessed December 17, 2015, https://www.congress.gov/bill/110th-congress/house-bill/6304/text?overview=closed&resultIndex=1

[137] Ibid

persons, for actions under §702 "the government is *not* required to go before the court to obtain individual surveillance orders."[138]

Section 215 provided the Director of the Federal Bureau of Investigation or a designee the ability to:

> make an application [to the Foreign Intelligence Surveillance Court] for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.[139]

The government interpreted this to include electronic records as "tangible things,"[140] and thus the FISC authorized the wholesale gathering of all available metadata from companies such as Verizon.[141] It would stand to reason that the government also requested orders for the production of similar "tangible things" from other service providers such as AT&T, Sprint, and the other major carriers, but none have been made public as of the writing of this thesis.

Metadata is collected by each phone company for the purpose of billing customers. Capturing the duration of calls, their origin, and destination allows companies to determine how much to bill for each call, or in the era of prepaid phone plans, how each call fits within the plan's limits. The same goes for text messaging, though rather

---

[138] "Are They Allowed to Do That?" *Brennan Center For Justice at New York University School of Law*, last accessed February 4, 2016, https://www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf. Emphasis in original.

[139] "H.R. 3162: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (107th Congress, 2001-2002)," *Library of Congress*, last accessed December 17, 2015, https://www.congress.gov/bill/107th-congress/house-bill/3162/text?overview=closed&resultIndex=1

[140] *In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 06-05 (FISA Ct. 2006)

[141] Greenwald, "NSA Collecting Phone Records…"

than duration, metadata instead reflects the number of texts sent and received. Without this information, a phone company will lack the necessary means to successfully bill customers, and the collection of metadata has significant implications for marketing as well.

It is questionable whether the U.S. Congress actually intended for the intelligence community to gain such unlimited access to this kind of data. Rather, the standard has generally required that any data captured or targeted be "relevant" to an active investigation.[142] The Office of the Director of National Intelligence's (ODNI) response to the issue of potential Fourth Amendment violations was that the actual searches and seizures took place only after the metadata was collected; the original step of gathering that information was preliminary only, and did not trigger a Fourth Amendment question.[143]

New Procedures under USA FREEDOM Act

Currently, following the passage and implementation of the Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-Collection and Online Monitoring (USA FREEDOM) Act, the legal authority, as the IC read it at the very least, to collect metadata was allowed to lapse by Congress. A six month "buffer" to allow the programs to wind down expired on November 29th, 2015.

---

[142] "Are They Allowed to…"

[143] James Clapper, "DNI Statement on Recent Unauthorized Disclosures of Classified Information," *Office of the Director of National Intelligence*, June 6, 2013, http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information; and Robert S. Litt, "Privacy, Technology and National Security: An Overview of Intelligence Collection" (speech at The Brookings Institution, Washington, DC, July 19, 2013), transcript available at http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/896-privacy,-technology-and-national-security-an-overview-of-intelligence-collection. Litt serves as the General Counsel for the ODNI.

From that date on, while phone companies are still required to maintain metadata files for a lengthy period of time, the U.S. government will no longer hold and control those files itself; rather, the IC or federal law enforcement "must now get a court order to ask telecommunications companies to enable monitoring of call records of specific people, or groups, for up to six months."[144] The vocal outrage from some Congressmen and Senators, along with civil libertarians on the conservative side of the political aisle and anti-surveillance liberals, led to the passage of the new law; Edward Snowden's revelations had the rare effect of bringing together the far sides of the political spectrum.

Representative Jim Sensenbrenner (R-WI-5), the initial sponsor of the USA PATRIOT Act, expressed displeasure in the days following the Snowden leaks at how his bill was interpreted by the intelligence community, calling the 215 programs "dragnet collection of phone data with rubberstamp approval by a Foreign Intelligence Surveillance Act court" and terming them "incredibly troubling."[145] Later, Sensenbrenner also sponsored the USA FREEDOM Act.[146] Within two weeks of the Snowden leaks, Representatives Justin Amash (R-MI-3) and John Conyers, Jr. (D-MI-13) introduced a bill to limit "the federal government's ability under the Patriot Act to collect information on Americans who are not connected to any ongoing investigation."[147] The

---

[144] "NSA Ends Bulk Collection of US Phone Records," *Al Jazeera*, November 28, 2015, http://www.aljazeera.com/news/2015/11/nsa-ends-bulk-collection-phone-records-151128172222095.html; *see also* "NSA Scrapping Contentious Spy Program," *Reuters*, November 10, 2015, http://www.reuters.com/video/2015/11/10/nsa-scrapping-contentious-phone-spy-prog?videoId=366266601; and "H.R. 2048: Uniting and Strengthening…"

[145] Jim Sensenbrenner, "Jim's Column: Combating Abuse of Patriot Act," *Office of Congressman Jim Sensenbrenner*, June 13, 2013, http://sensenbrenner.house.gov/news/documentsingle.aspx?DocumentID=339292

[146] "H.R. 2048: Uniting and Strengthening…"

[147] "NSA Surveillance: Amash, Conyers Introduce Major Bill," *Office of Congressman Justin Amash*, June 18, 2013, http://amash.house.gov/press-release/nsa-surveillance-amash-conyers-introduce-major-bill

bill, which was unsuccessful and died in committee without ever having been voted upon, attracted fifty-two additional bi-partisan cosponsors.[148]

Following Snowden's leaks President Obama said that he would welcome a debate on the issue of mass surveillance in light of Snowden's leaks, and DNI Clapper said that some of the ongoing discussion was valuable.[149] Even the FISA Court weighed in on the controversy. An opinion by Judge Dennis Saylor, released in September 2013, argued that releasing more FISC opinions "would contribute to an informed debate [and]…assure citizens of the integrity of this Court's proceedings."[150]

The USA FREEDOM Act eventually accomplished some of the reforms that had been called for in the months following the Snowden leaks, and passed with overwhelming majorities in both the House of Representatives (338-88)[151] and the Senate (67-32).[152] Among those voting against the bill were Senators Rand Paul (R-KY) and Bernie Sanders (D-VT), both of whom felt that the USA FREEDOM Act remained too

[148] "H.R. 2399: LIBERT-E Act (113th Congress, 2013-2014)," *Library of Congress*, last accessed March 17, 2016, https://www.congress.gov/bill/113th-congress/house-bill/2399?resultIndex=1

[149] Andy Greenberg, "Intelligence Officials Admit that Edward Snowden's NSA Leaks Call for Reforms," *Forbes*, September 13, 2013, http://www.forbes.com/sites/andygreenberg/2013/09/13/intelligence-officials-admit-that-edward-snowdens-leaks-call-for-reforms/#5a109b054ee5

[150] *In re Orders of this Court Interpreting Section 215 of the Patriot Act*, No. BR 13-02 (FISA Ct. 2013). Judge Saylor's actual opinion no longer appears on the website of the federal court system, but the Federation of American Scientists has archived a copy on its website, available at http://fas.org/irp/news/2013/09/fisc-091313.pdf

[151] "Final Vote Results for Roll Call 224," *United States House of Representatives*, May 13, 2015, http://clerk.house.gov/evs/2015/roll224.xml

[152] "On the Passage of the Bill (H.R. 2048)," *United States Senate*, June 2, 2015, http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=114&session=1&vote=00201

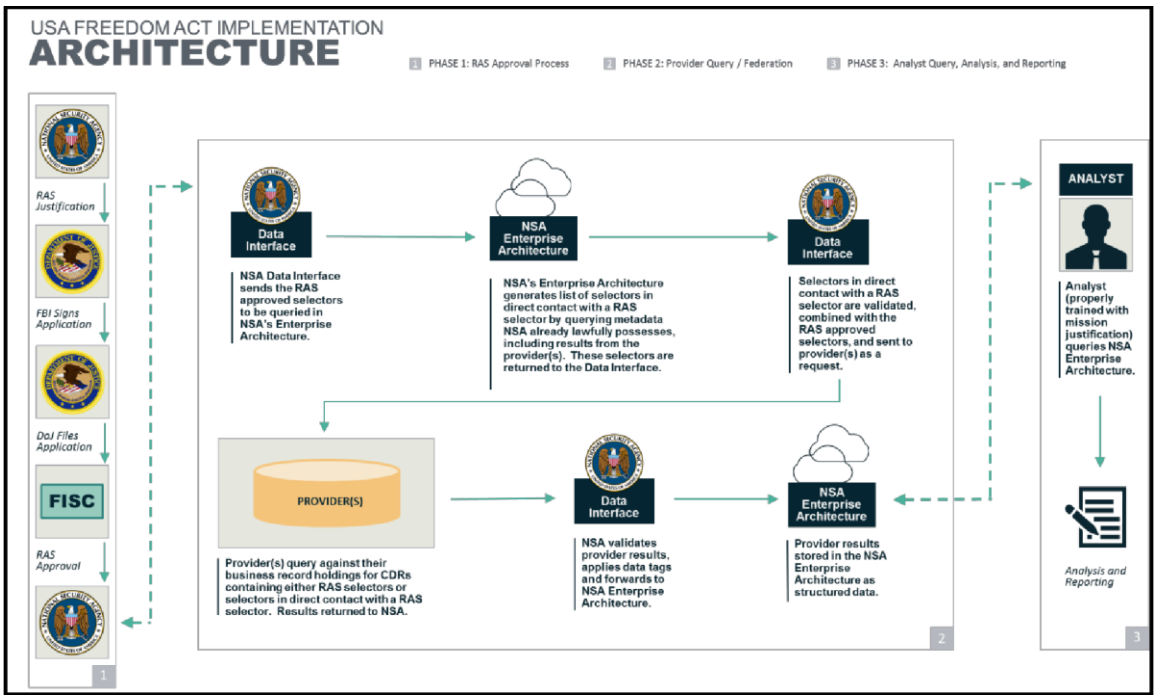
invasive and that even with the new restrictions the NSA was violating the Constitution.[153]

A great deal of improvement in the system has been made despite the objections of Senators Paul and Sanders. The process to obtain materials from the various companies that hold data—such as telephone or internet service providers—is specific and detailed, requiring several steps to acquire metadata or other telecommunications information that are systematic and codified in the law. (See Figure 8)[154]

The new law requires the NSA to notify the FBI that there is reasonable, articulable suspicion (RAS) "that the specific selection term to be used as a basis for the production is associated with a foreign power, or an agent of a foreign power, engaged in international terrorism or activities in preparation therefore." Representatives from the FBI then present a signed application to the Department of Justice, which files the application with the FISC. If the FISC approves the application (affirming that there is RAS), the NSA Data Interface sends the selector(s) to be queried to the NSA Enterprise Architecture. Selectors are validated, data is retrieved from metadata that "NSA already lawfully possesses," and additionally sends the request to providers to query against their own records. These results must also be validated and then stored in the NSA Enterprise Architecture before an analyst finally may query the Enterprise Architecture. In an

[153] *See* Bill Chappell, "Senate Approves USA Freedom Act, Obama Signs It, After Amendments Fail," *National Public Radio*, last updated June 2, 2015, http://www.npr.org/sections/thetwo-way/2015/06/02/411534447/senateis-poised-to-vote-on-house-approved-usa-freedom-act; and Jeremy Diamond, "NSA Surveillance Bill Passes After Weeks-Long Showdown," *CNN*, last updated September 7, 2015, http://www.cnn.com/2015/06/02/politics/senate-usa-freedom-act-vote-patriot-act-nsa/

[154] Civil Liberties and Privacy Office, "Transparency Report: The USA FREEDOM Act Business Records FISA Implementation," *National Security Agency*, January 15, 2016, available at https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf



F8: "USA FREEDOM Act Implementation Architecture" flowchart

emergency, the Attorney General may temporarily authorize a query pending an application to the FISC, which must be submitted within seven days.

Beyond the new procedures for obtaining data from providers, other changes include new reporting requirements to the FISC, more opportunities for private companies to reveal to the public how many FISA orders they receive, and limits the number of "hops"[155] that can be made to two. Most importantly, it requires either the declassification of legally significant FISC cases or the production of an unclassified summary if declassification is not possible. Additionally, the FISC must establish a panel of public advocates to represent the interests of the people in certain cases that involve significant legal questions. These new procedures do slightly delay NSA analysts receiving the data for which they are searching, but it does significantly lower the

[155] See next chapter for explanation of a "hop"

associated Constitutional concerns surrounding the NSA's collection of data from the various providers.[156] However, this does not entirely alleviate the Fourth Amendment issue due to the reduced reasonable, articulable suspicion constraint the NSA must follow, rather than *probable cause* as required by the Fourth Amendment.

Fourth Amendment Questions

U.S. citizens, and non-citizens on U.S. soil, are entitled to certain guarantees of protection against the government. Foremost among these are the rights collectively organized in the "Bill of Rights," those first ten amendments to the Constitution that spell out the liberties the founders believed most important. In this case, there is one that in particular requires attention; the Fourth, which requires that any search and seizure be preceded by a warrant based on probable cause. To fully articulate the arguments, a complete understanding of the Amendment itself is necessary. Stemming from Britain's 1215 document the *Magna Carta* like many of the original ten amendments to the Constitution, the Fourth Amendment affirms the right to be free from unwarranted searches. Technology today allows new kinds of searches and seizures, of a variety that the Founding Fathers could never have imagined. Early in his book describing the process of receiving and publishing leaked documents from Edward Snowden, Glenn Greenwald remarks that, "[t]echnology has now enabled a type of ubiquitous surveillance that had previously been the province of only the most imaginative science fiction writers."[157]

---

[156] "USA Freedom Act: What's In, What's In," *Washington Post*, June 2, 2015, https://www.washingtonpost.com/graphics/politics/usa-freedom-act/

[157] Greenwald, *No Place to Hide,* 2

Simple and relatively uncomplicated, particularly in terms of the normally exceptionally complex U.S. Constitution, the Fourth Amendment states that to conduct a search or seizure, there must be a duly issued warrant, which is issued *upon probable cause*. According to Director of National Intelligence James Clapper, however, the standard for his employees is rather lower. The NSA uses the "reasonable suspicion" standard,[158] presumably basing this on the rules laid out in *Terry v. Ohio*. *Terry* was intended to allow police officers to make investigative stops based on "reasonable, articulable suspicion" that a crime had occurred, was occurring, or was about to occur, and conduct cursory pat downs for weapons, but not evidence of the crime.[159] However, that standard applies when there is a crime believed to have occurred, be occurring, or be about to occur, not a "fishing expedition" where a line is simply thrown out into the water under the theory that somewhere, someone is, or might be, doing something wrong. Additionally, this standard was never intended to become a substitute for *probable cause* in application for a warrant, or even to be used as the basis for a warrantless search under one of the exceptions carved out by the Supreme Court. In all criminal cases, searches for evidence of a crime or for a hidden person require probable cause to be expressly delineated, and in the case of a warrant application, that probable cause must actually explain exactly what the item, or items, to be searched for are, and where the officer anticipates they are located.

---

[158] Paul D. Shinkman, "Spy Chief Says Taps Analyzed Only for 'Reasonable Suspicion,'" *U.S. News and World Report*, June 7, 2013, http://www.usnews.com/news/articles/2013/06/07/spy-chief-says-taps-analyzed-only-for-reasonable-suspicion

[159] *Terry v. Ohio,* 392 U.S. 1 (1968)

General Hayden argues that while this makes sense for criminal cases, the standard needs to be different for non-law enforcement intelligence operations. As he put it, there should not be

> a blank check…for the intel guys… But traditionally, in American law, we've made that distinction… [T]hat's why we try to [separate] information gathered for intelligence purposes, from information for law enforcement purposes. There's a membrane between the two… [I]t's always easier…to get a FISA [warrant] for foreign intelligence purposes, than it would be for the [FBI] to get one for law enforcement purposes. [This is because if the NSA] overreaches, [it's] squeezing your privacy. If the [Federal] Bureau [of Investigation] overreaches, they're squeezing your privacy and threatening your liberty, because they can put you in jail.[160]

The federal government of the United States agrees, arguing that due to the grave threat of terrorism and the potential for massive casualty numbers, there needs to be a different system in place for the national security apparatus to operate. However, a strict reading of the Constitution, as well as any number of court decisions on the Fourth Amendment or the right to privacy, argues otherwise. While there are several "exceptions" to the warrant requirement that have been enumerated over the years by the Supreme Court, each of them requires some form of emergency or exigency. Those exigencies result in a situation in which the evidence of the crime being investigated will disappear, be destroyed, or be unavailable for some reason, or an emergency involving risk to the life or safety of a person who is unable to immediately assist himself or herself.[161] In rare circumstances, what has become known as the "substantial government

[160] Hayden, in discussion with the author, September 21, 2015

[161] *See Warden v. Hayden*, 387 U.S. 294 (1967), which allowed entry to a private residence during "hot pursuit," *Terry v. Ohio*, and *Schmerber v. California*, 384 U.S. 757 (1966), which held that a warrantless blood draw from a drunk driving suspect was not a violation because the evidence (the alcohol infused blood) would become unrecoverable in the time it took to obtain a warrant.

interest" test has been used to justify semi-intrusive seizures, but not searches.[162] Few would argue that a police officer or federal agent who knows that a terrorist's bomb, known (or even believed) to be set to explode imminently, is behind a locked door should stand back and await a warrant; this is no different from the situation of an armed hostage-taker holding a gun to someone's head behind the same closed door. Widespread and untargeted surveillance or data seizure fails to satisfy even the loosest definition of exigency. Thus, the arguments and rationales for the types of programs being run by the National Security Agency have become that the standard must be lowered in the case of terrorism related issues.

For the government's seizure of metadata, the rationale in *Michigan State Police v. Sitz* makes a great deal of sense; the mere seizure of metadata does not cause any undue stress to the individuals whose data has been seized. In fact, it is almost guaranteed that they will not know about the seizure due to the classified nature of the seizure.[163]

Another argument that General Hayden made was that the "third party doctrine," which was established by *Smith v. Maryland*[164] and *United States v. Miller*,[165] allows the government to receive records about an individual or group that are held by a third party without a warrant and without violating the Fourth Amendment. General Hayden explained that "[t]hose phone bills belong to Verizon," after all.[166] Because "[t]he laws

---

[162] *See Michigan State Police v. Sitz*, 496 U.S. 444 (1990), which allowed drunk driving checkpoints, and *United States v. Martinez-Fuerte*, 428 U.S. 543 (1976), which allowed fixed checkpoints near, but not at, border crossing.

[163] *American Civil Liberties Union v. National Security Agency,* 493 F.3d 644 (6th Cir. 2007)

[164] *Smith v. Maryland*, 442 U.S. 735 (1979)

[165] *United States v. Miller*, 425 U.S. 435 (1976)

[166] Hayden, in discussion with the author, September 21, 2015

that govern online privacy are older than the World Wide Web" there are few protections for people using the internet and other modern technologies such as smart phones.[167] Most recently, in 2015, the Eleventh Circuit Court of Appeals upheld the applicability of the third party doctrine as it applies to modern cellular phones and providers in *United States v. Davis*.[168]

Even if the third party doctrine is accepted as applicable in this case, however, the federal government did go out of its way to get a warrant through the FISA Court, in effect admitting that there was a search or seizure taking place that required that warrant. Thus, while the third party doctrine is worth examining for future cases in which the phone companies turn over information willingly, in the specific case of the seizure of data and metadata here, it was involuntary; Verizon, and presumably other companies, received a court order from the FISC. While not relating specifically to metadata, Yahoo! was ordered—and threatened when it did not comply—to turn over data it felt was not within the purview of the government to seize.

The key, then, to evaluating this issue in the context of the Fourth Amendment is to remember that the search itself is not the proximate cause of injury; rather, the seizure is. Though the warrants that are issued to search the data recovered are issued by a judge and are requesting access to specific records and files,[169] they require a far lower standard than the Fourth Amendment specifies. Even if that were ignored, it still does not permit or allow the *seizure* of the data that is to be later searched. The court orders that made

---

[167] Michael W. Price, "Rethinking Privacy: Fourth Amendment 'Papers' and the Third Party Doctrine," *Georgetown University Law Center's Journal of National Security Law and Policy* 8, no. 2, available at https://www.brennancenter.org/sites/default/files/analysis/Mike%20Price%20-%20Rethinking%20Privacy.pdf

[168] *United States v. Davis*, 573 Fed. Appx. 925 (11th Cir. 2014)

[169] Darby

that possible are demonstrably illegal for two reasons: first, that they fail to particularly describe the items to be seized; and second, for their breadth, which places no limits on the "area" from which to seize data.

Judge Richard Leon, sitting for the U.S. District Court for the District of Columbia, wrote in his decision on *Klayman v. Obama* that "[t]he almost-Orwellian technology that enables the government to store and analyze the phone metadata of every telephone user in the United States is unlike anything that could have been conceived in 1979"[170] in declaring mass metadata seizures unconstitutional.[171] This followed a 2014 Supreme Court decision that disallowed searches of cell phones incident to arrest,[172] which Klayman, representing himself, argued was substantially similar to the actions of the NSA in PRISM and MUSCULAR, except that there was no prior arrest or criminal charge, nor even suspicion of criminality, facing the people who were having their records seized.

Richard Posner, a federal judge sitting on the Court of Appeals for the Seventh Circuit and one of the most prominent non-Supreme Court members of the Judicial Branch, disagrees in the strongest terms: "I think privacy is actually overvalued," he said. "Much of what passes for the name of privacy is really just trying to conceal the disreputable parts of your conduct. Privacy is mainly about trying to improve your social and business opportunities by concealing the sorts of bad activities that would cause other people not to want to deal with you."[173] Judge Posner is a giant in his field, and his

---

[170] Referring to 442 U.S. 735 (1979)

[171] Quoted in: Warren, "Judge Rules NSA Collection…" Judge Leon stayed his finding pending an appeal, which was heard in November of 2014.

[172] *Riley v. California*, 573 U.S. ____ (2014)

[173] Gross, "Judge: Give NSA Unlimited…"

judicial opinions carry tremendous weight, but it is hard to understand where this particular sentiment—which is not based on a case in front of him, but simply his own personal beliefs and legal acumen—comes from. He fails to explain how the desire to maintain privacy for the reasons he presents means that the protections of the Constitution should not apply. Regardless, his judgment is important in that he is the most notable jurist on record with this opinion. Beyond that, he is one of the preeminent legal minds in the United States, and has often expressed many libertarian-leaning opinions.

Due Process—Fifth and Fourteenth Amendments

It is difficult to even sue the United States government over the NSA's tracking or information gathering. Attorneys from the Solicitor General's and U.S. Attorney's offices routinely argue that plaintiffs lack standing to sue, saying that these parties have not suffered any harm,[174] and it is nearly impossible to show evidence of direct harm, or even that an individual has been subjected to the NSA's information intake, due to the classification of virtually information related to these matters. Not only does the U.S. government argue this, but judges have agreed with it at the highest levels; the Sixth Circuit Court of Appeals in 2007[175] and the Supreme Court in 2013 ruled that the ACLU and Amnesty International, respectively, lacked standing to sue as they had not incurred any injury, nor was such imminent.[176] Of course, the plaintiffs may well have suffered

[174] *Citizenfour*

[175] 493 F.3d 644 (6th Cir. 2007)

[176] *James R. Clapper v. Amnesty International USA, et al*, 568 U.S. ____ (2013), No. 11-1025. *See also* David Kravets' July 9th, 2013 article in *Wired*, "NSA Phone Snooping Cannot be Challenged in Courts, Feds Say."

harm, or may be facing imminent harm, but are unable to provide or gain access to evidence that would prove that they have. Despite the normal rules of evidence, or even just a simple Freedom of Information Act request, requiring that the government turn over documents related to the cases, the national security secrets argument allows it to do the exact opposite.

Under this legal theory, only someone who has been charged with a crime would be able to challenge the constitutionality of a system that has wide ranging, sweeping coverage. In the words of Associate Justice of the Supreme Court Sonia Sotomayor, according to the government's argument, "if there was a constitutional violation in the interception…no one could ever stop it until they were charged with a crime, essentially."[177] According to U.S. Solicitor General Donald B. Verilli, Jr., government having the authority to capture information (metadata, in this case) from each and every American provides neither imminent or actual harm, but simply a "speculative… connection between the grant of authority and a claim of injury."[178]

The problem that presents itself here, however, is that the government is effectively denying *due process* rights, guaranteed in the Fifth and Fourteenth Amendments, by denying the opportunity to challenge the legality of these programs. Due process, which applies to both criminal cases and to the general activity of the government, is the only specific item mentioned twice in the Constitution,[179] for good reason; it requires the government to "operate within the law…and provide fair procedures." A list of requirements for due process to be achieved derived from an

[177] Oral Arguments, 568 U.S. _____ (2013), No. 11-1025, 4

[178] Ibid, 10

[179] In the 5th and 14th Amendments

article by Judge Henry Friendly provides ten such and is still "highly influential." This includes "the right to know opposing evidence," such as records that reflect the capture and possession of data material to the plaintiffs in both the ACLU and Amnesty International cases, or lack thereof.[180]

Another of Judge Friendly's requirements was an unbiased tribunal. Being able to challenge warrants only long after the fact, or in the confines of the Foreign Intelligence Surveillance Court (FISC), fails to satisfy the requirement for what Associate Justice Robert Jackson referred to as "a neutral and detached magistrate."[181] The FISC employs judges who have not endured the standard rigorous process of Senatorial "advice and consent" that virtually all other federal judges and justices do prior to their appointment to this particular bench.[182] Because so-called "FISA judges" are not considered to be "Article III" appointees, whose existence is supported and mandated by the eponymous portion of the Constitution of the United States, they are among the small handful of judges and justices serving in their positions within the federal government who are not appointed by the president dependent upon the advice and consent of the Senate. The Chief Justice of the Supreme Court, instead, appoints the members of the FISC for a period of not more than seven years.[183] These judges are members of the

[180] Peter Strauss, "Due Process," *Cornell University Law School Legal Information Institute*, last accessed February 5, 2016, https://www.law.cornell.edu/wex/due_process

[181] *United States v. Johnson*, 333 U.S. 10 (1948), at 14

[182] "Constitution of the United States," in Art. II, Sec. 2. *See also* explanation on the website of the Federal Judicial Center, www.fjc.gov/federal/courts.nsf/autoframe!openform&nav=menu1&page=federal/courts.nsf/page/183.

[183] Nick Harper, "FISA's Fuzzy Line between Domestic and International Terrorism," *The University of Chicago Law Review* 81, no. 3 (2014), 1129. *See* the aforementioned article on the FJC website for the list of judges who are not subject to Art. II, Sec. 2 approval. *See* 50USC§1803(d).

judiciary already and have previously been scrutinized,[184] but unlike other judges who are "promoted" or assigned to new posts, where there is an opportunity to question the candidates on specific issues related to their work or their recent decisions, they are simply assigned in this case. This results in judges who are not subject to the same scrutiny upon appointment and who are more likely to act as agents of the Chief Justice's agenda rather than as impartial, "neutral and detached magistrates," lest they suffer any recrimination for failing to follow the Chief Justice.

This has resulted in a situation in which the FISA court judges rejected fewer than a dozen warrant requests over the first thirty-three years of their existence, just three one-hundredths of a percent of the overall requests.[185] Rather than the adversarial model that exists in other criminal courts, with no opposing attorneys or petitioners, the judges in the FISC appear in many ways to work *with* the federal government to obtain warrants, including informing requesting officers how to improve their petitions.[186] This cooperative effort is anathema to the normal system of laws in the United States where a judge who rejects a warrant tells an officer why the standard was not met, not how to rewrite the application.

Judges are by their very nature intended to be impartial arbiters of justice, taking no side but that of the law. Appointing them to oversee just one small section of the statutory codes of the country, with what could only be a small number of applicants—if only due to the highly classified nature of the situations which would tend to precipitate a

[184] "The Foreign Intelligence Surveillance…"

[185] Evan Perez, "Secret Court's Oversight Gets Scrutiny," *The Wall Street Journal* (New York, NY), June 9, 2013, http://www.wsj.com/articles/SB10001424127887324904004578535670310514616

[186] Darby

FISA warrant request—puts them in the position of becoming too close to those petitioning them, removing objectivity.

Governmental Necessity

"Laws are silent when arms are raised…" Cicero told Pompey's judges, "when he who waits will have to suffer an undeserved penalty before he can exact a merited punishment."[187] It is Cicero's argument that is heard time and time again when the federal government of the United States defends its capture of Americans' phone call and email data, or when it passes laws or internal regulations that lower the standard of evidence needed to obtain a warrant. Government's job is to provide protection from external, and occasionally internal, threats to the country, as codified in the Constitution of the United States.[188] Preventing an "undeserved penalty," in the case of the United States from the actions of terrorists, is the goal of both the military and the civilian leaders of the country and, thus, they cannot simply wait.

Governmental necessity as a reason to do something is also codified in the Constitution through the "Necessary and Proper Clause" in Article II, which enumerates the responsibilities and roles of the legislature. It states that Congress shall have the power "[t]o make all laws which shall be necessary and proper for carrying into execution the foregoing powers, and all other powers vested by this Constitution in the

[187] Marcus Tullius Cicero, "Pro Tito Annio Milone ad iudicem oratio," translated by C.D. Yonge, accessed April 14, 2015, http://www.perseus.tufts.edu/hopper/text?doc=urn:cts:latinLit:phi0474.phi031.perseus-eng1:11. Translated from "Inter arma enim silent leges," the first portion is often alternately translated as "In times of war, the law falls silent."

[188] "Constitution of the United States." Various articles give Congress and the President authority or responsibility to act in defense of the Union, including: the Preamble, Art. I, Sec. 8; Art. I, Sec. 9; Art. III, Sec. 4.

government of the United States, or in any department or officer thereof."[189] While not removing the requirement that these laws be congruent with the rights the Constitution endows to the people, it does allow Congress a great deal of leeway. If the federal government is required by the Constitution to defend and protect the people of the United States, then it would follow that Congress can enact whatever laws are "necessary and proper" to allow the President and the executive branch to do just so.

And so, how to determine which takes precedence: the powers of the government; or the rights of the people? There is no simple or easy answer, and it most likely comes down to being determined on a case by case basis. In this case, the government's need to protect the people against attack is paramount to the government, and with the agreement of the people that terrorism is a major, growing threat, maybe even the greatest threat the nation faces, there is wide leeway being given to the government. (See Figure 9)[190] To some extent, if the people give their approval, tacit or overt, to a government program, that program should exist. The issue is determining where the line between "acceptable because the people say so" and "unacceptable even with the peoples' consent" should be defined. Combining the government arguing necessity and the people howling for a solution has resulted in past tragedies, not the least of which being the internment of Japanese-Americans during the Second World War[191]

---

[189] Ibid

[190] "Views of Government's Handling of Terrorism Fall to Post-9/11 Lows," *Pew Research Center*, December 15, 2015, http://www.people-press.org/2015/12/15/views-of-governments-handling-of-terrorism-fall-to-post-911-low/

[191] *See* "Teaching With Documents: Documents and Photographs Related to Japanese Relocation During World War II," *United States National Archives*, last accessed February 5, 2016, https://www.archives.gov/education/lessons/japanese-relocation/

Growing share cite terrorism as the most important problem facing the U.S.

Most important problem facing nation ...

	Dec 2014	Dec 2015	Change
	%	%	
Terrorism	1	18	+17
Economy (general)	14	9	-5
Defense/National security	2	8	+6
Immigration	12	7	-5
Unemployment	10	7	-3
ISIS/War in Iraq/War in Syria	2	7	+5
Dissatisfaction with government, Obama	10	6	-4
Gun control/Too many guns/ Mass shootings	1	5	+4
Political gridlock/division	8	5	-3
NET: Foreign/International	**9**	**32**	+23
NET: Terrorism/ISIS/ National security	*4*	*29*	+25
NET: Economic issues	**34**	**23**	-11

Source: Survey conducted Dec. 8-13, 2015.
Note: see topline for all mentions and full trend.

PEW RESEARCH CENTER

F9: Pew Research Center poll "Growing share cite terrorism as the most important problem facing the U.S" showing that 18% of Americans view terrorism is the "most important problem" facing the United States, an 18 fold increase from the previous year

and the blacklisting of suspected communists during the Cold War.[192]

[192] *See* Robert Justin Goldstein, "Prelude to McCarthyism: The Making of a Blacklist," *Prologue Magazine* 38, no. 3 (Fall 2006), available at http://www.archives.gov/publications/prologue/2006/fall/agloso.html

Miscellany

The FISA courts' lack of an accused who is capable of and allowed to mount a defense is *prima facie* evidence of a failure to meet the "case and controversy" requirement embodied in Article III, Section 2 of the Constitution, which states:

> The judicial Power shall extend to all Cases, in Law and Equity, arising under this Constitution, the Laws of the United States, and Treaties made, or which shall be made, under their Authority…--to Controversies between two or more States;--between a State and Citizens of another State;--between Citizens of different States;--between Citizens of the same State claiming Lands under Grants of different States, and between a State, or the Citizens thereof, and foreign States, Citizens or Subjects.[193]

Beginning with John Jay, the first Chief Justice of the Supreme Court, this section was interpreted to mean that only in cases wherein there was a genuine conflict between parties could there be a role for the federal judiciary.[194] In fact, under *Muskrat v. United States*, it is quite possible that the entire matter is unconstitutional simply because Congress, via appropriations of funds, is the only entity paying for arguments before the courts in the case of these warrants, a scenario banned under this 1911 decision that has never been overturned. The decision stated that if Congress is the only party paying, then there is no real controversy to be decided.[195] It can thus be argued that any and all decisions by the FISC are invalid and the court lacks standing due to its prohibition on the presentation of evidence and argumentation by a defendant.

The Ninth Amendment must not be forgotten either, stating that simply because it does not appear in the Constitution, something is not precluded from being a right of the

---

[193] Ibid

[194] "Constitutional Limitations on Judicial Power: Standing, Advisory Opinions, Mootness, and Ripeness," *University of Missouri-Kansas City School of Law*, accessed April 26, 2015, http://law2.umkc.edu/faculty/projects/ftrials/conlaw/caseorcontroversy.htm

[195] *Muskrat v. United States*, 219 U.S. 346 (1911)

people.[196] This amendment was used heavily in Justice Arthur Goldberg's concurrence in the case of *Griswold v. Connecticut*, which established the right to privacy as an unenumerated right of the people.[197] If people do indeed have the right to privacy that may well extend to situations such as these where the government has established a program which inherently invades the privacy of the citizenry, even if it does not do so in a manner which causes wholesale direct harm. Since one of the main arguments that proponents of the NSA's programs, including General Hayden and the DNI, have made is that there is no direct harm even if there is "incidental" or otherwise unintended collection, the fact that privacy may be invaded or limited does violate the unenumerated right laid out in *Griswold*. It should also be noted that the International Covenant on Civil and Political Rights, which the United States signed in 1977 and ratified in 1992,[198] bans "arbitrary…interference with [any person's] privacy, family, home or correspondence."[199] Indiscriminate collection of email or communications metadata would logically fall under the auspices of this treaty's ban on arbitrary interference with correspondence.

An additional concern for privacy advocates is the relationship between the NSA and federal law enforcement. According to *Reuters* and the *Washington Post*, the NSA provides classified communications and signals intelligence to the Drug Enforcement

---

[196] "Bill of Rights." The Ninth Amendment covers what are known as "unenumerated rights."

[197] *Griswold v. Connecticut*, 381 U.S. 479

[198] "Treaties in Force: A List of Treaties and Other International Agreements of the United States in Force on January 1, 2013," *United States Department of State*, available at http://www.state.gov/documents/organization/218912.pdf. See page 399 for the timeline of the United States' involvement in this convention. The State Department did not release full reports for the years 2014 or 2015, making this document the most recent complete list of United States treaty and convention obligation. No changes have been made to the U.S. obligations under this convention.

[199] "International Convention on Civil and Political Rights," *United Nations Human Rights Office of the High Commission*, last accessed March 2, 2016, http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

Agency (DEA). In August 2013, *Reuters* revealed that the DEA engages in what is called "parallel construction," wherein agents conduct an investigation based on the classified information received from the intelligence community and then use what is learned during that investigation to, as one former DEA agent stated, "work it backwards to make it clean."[200] This could lead to an issue under the same "fruit of the poisonous tree" rule addressed in a previous chapter, as well violate a defendant's right to receive all possible exculpatory evidence during discovery. The Supreme Court has ruled that if a federal law enforcement agency used evidence derived from Section 702 it programs must be revealed during discovery and defense attorneys must be allowed to challenge its admissibility.[201] However, the DEA's use of parallel construction may have resulted in a situation where this did not occur, thus violating defendants' rights under the Sixth Amendment.[202]

[200] John Shiffman and Kristina Cooke, "Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans," *Reuters*, August 5, http://www.reuters.com/article/us-dea-sod-idUSBRE97409R20130805

[201] Ellen Nakashima, "Chicago Federal Court Case Raises Questions About NSA Surveillance," *Washington Post*, June 21, 2013, https://www.washingtonpost.com/world/national-security/chicago-federal-court-case-raises-questions-about-nsa-surveillance/2013/06/21/7e2dcdc8-daa4-11e2-9df4-895344c13c30_story.html

[202] Brian Fung, "The NSA is Giving Your Phone Records to the DEA. And the DEA is Covering it Up," *Washington Post*, August 5, 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/05/the-nsa-is-giving-your-phone-records-to-the-dea-and-the-dea-is-covering-it-up/

HOW EFFECTIVE IS DOMESTIC SURVEILLANCE?

"Your successes are unheralded—your failures are trumpeted," President John F. Kennedy said to a gathering of Central Intelligence Agency workers in November of 1961.[203] That is the nature of the intelligence community, and the reason it is so difficult to evaluate the effectiveness of any particular program or group thereof. There are reporters like Barton Gellman and James Bamford who have made their names and reputations on work about the IC, but by and large the wall of secrecy that surrounds the NSA, CIA, and other "three letter" agencies is challenging to penetrate. To a great extent, the assertions of members of the IC, Congress, and the executive branch about the efficacy of the sixteen intelligence agencies must simply be relied upon to be accurate.[204] Due to situations in the past when members of the intelligence community and government in general have lied about, covered up, or otherwise ignored malfeasance, or even just made mistakes—a problem that any group so large will have to face at some point—many in America do not trust the U.S. government. In general, the country's trust in the government is at an all-time low among all generations. (See Figure 10)[205]

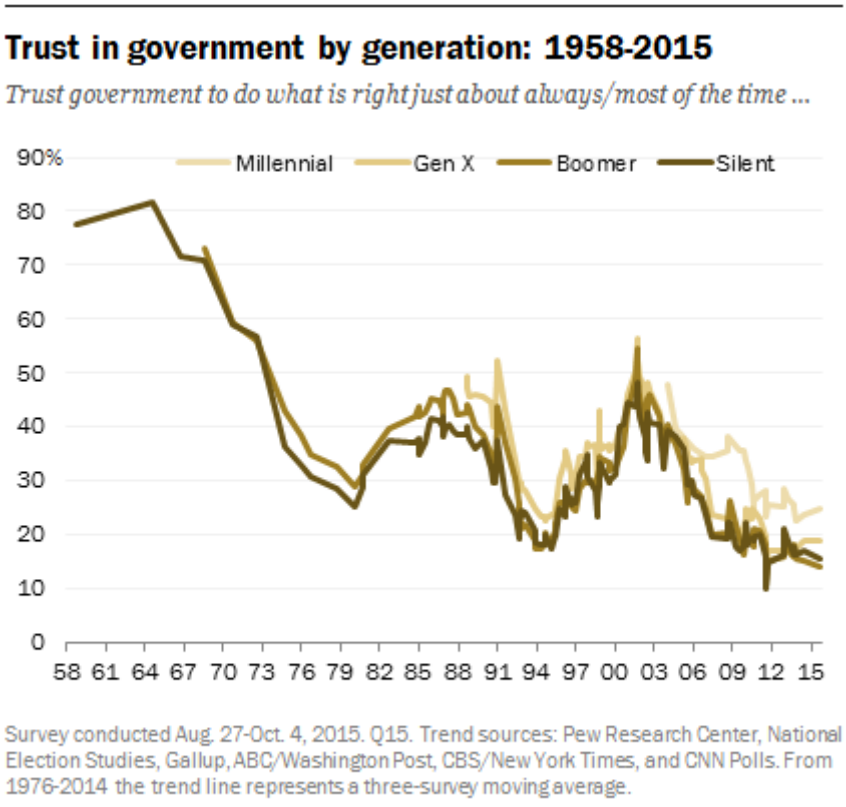
This means that Americans, primarily through the work of investigative journalists, are taking a closer look at what is going on inside government and providing the citizenry a more complete look at not only what their government is doing, but how

[203] John F. Kennedy, "Valediction" (speech at awards ceremony for Allen Dulles, Langley, VA, November 28, 1961), available at https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol6no1/html/v06i1a07p_0001.htm

[204] A list of all sixteen agencies that make up the United States' intelligence community is available at http://www.dni.gov/index.php/intelligence-community/members-of-the-ic

[205] "Beyond Distrust: How Americans View Their Government," *Pew Research Center*, November 23, 2015, http://www.people-press.org/2015/11/23/1-trust-in-government-1958-2015/

they are doing it, why they are doing it, and even how well it is being done. This has been aided by unprecedented leaks from the intelligence community and law enforcement over the last two decades, and in some cases unprecedented access to the IC, as in the



F10: Pew Research Poll "Trust in government by generation: 1958-2015" showing trust in government for each generation. "Millenials" are ages 18-34, "Gen Xers" are 35-50, "Boomers" are 51-69, and "Silents" are 70-87. Just 25%, 19%, 14%, and 16% of each group, respectively, "says they can trust the federal government just about always or most of the time"

example of James Bamford while writing his seminal book on the NSA, *Body of Secrets* in the latter years of Bill Clinton's presidency.[206] Decreasing trust in government has numerous causes, but when a person who is already concerned about the actions of

[206] Bamford, *Body of Secrets*, ix

government is presented with information like what Snowden leaked, it is easy to understand how this could increase that unease.

Still, the best estimates of the efficacy of the 702 and 215 programs are just that: estimates. The need to keep collection methods secret has led to President Kennedy's statement to the CIA becoming a self-fulfilling prophecy within the entire intelligence community.

Understanding how metadata is used offers a glimpse into why the intelligence community considers it to be an important and useful tool. First, it is far easier to sort through and analyze than voice recordings which require a person to actually listen and determine if they are important; even if a computer program transcribes everything it will almost certainly not be entirely accurate due to accents, dialectic differences, and slang usage. Thus, it "ultimately requires at least some human analysis, and that inherently limits the scale at which it can be used."[207] Conversely, metadata can be analyzed almost entirely by computer programs, with only the final analytical connections needing human intervention.

When the NSA or another intelligence agency believes it has located the phone number, landline or wireless, of a terrorist suspect, it will examine every call or text that number has made or received, capturing the telephony metadata of every number found. This is called a "hop." After that, the agency may "hop" again once or twice, depending on how far an official decides is necessary.[208] This can result in thousands and thousands

[207] Matt Blaze, "Phew, NSA is Just Collecting Metadata. (You Should Still Worry)," *Wired*, June 19, 2013, http://www.wired.com/2013/06/phew-it-was-just-metadata-not-think-again/

[208] Philip Bump, "The NSA Admits it Analyzes More People's Data than Previously Revealed," *The Wire*, July 17, 2013, http://www.thewire.com/politics/2013/07/nsa-admits-it-analyzes-more-peoples-data-previously-revealed/67287/

of numbers—and thus people—being "targeted" in this manner because of one single suspect. When used on internet traffic metadata, rather than telephony metadata, the implications are even grander; according to research scientists from Facebook and the University of Milan, "the average number of acquaintances separating any two people in the world…[is] 4.74."[209] This means that those three "hops" potentially gives the NSA access to tens of *millions* of people's metadata.

Arguments for Effective Use

Immediately following the revelations of widespread metadata seizures and surveillance efforts by the NSA, members of the intelligence community began publicly defending the efficacy of the programs involved. In his June 6th, 2013 press release response to the first of the Snowden leaks, DNI Clapper stated that "[a]cquiring this information [metadata from Verizon] allows us to make connections related to terrorist activities over time."[210] Others have noted the efficacy of related programs in deterring and negating "the cyber threat facing the United States."[211] Even the president, a former critic of the intelligence community and constitutional law professor,[212] voiced his opinion soon after the leaks, saying that "by sifting through this so called metadata, they [the IC] may identify potential leads with respect to folks who might engage in terrorism… [M]y assessment…was that [these programs] help us prevent terrorist

[209] John Markoff and Somini Sengupta, "Separating You and Me? 4.74 Degrees," *New York Times*, November 21, 2011, http://nyti.ms/1BC5pRJ

[210] Clapper, "DNI Statement on Recent…"

[211] Kelly, Erin. "Newly Revealed NSA Surveillance Program Draws Support, Ire." *USA Today*. June 4, 2015. http://www.usatoday.com/story/news/nation/2015/06/04/obama-administration-nsa-surveillance-internet/28472865/.

[212] Jason M. Breslow, "Obama on Mass Government Surveillance, Then and Now," *PBS*, May 13, 2014, http://www.pbs.org/wgbh/frontline/article/obama-on-mass-government-surveillance-then-and-now/

attacks."[213] Six months later, he added that he "felt that they made us more secure, but also…nothing…indicated that our intelligence community has sought to violate the law or is cavalier about the civil liberties of their fellow citizens."[214]

In response to the Snowden leaks, Duke University sociology professor Kieran Healy wrote a tongue in cheek piece entitled "Using Metadata to Find Paul Revere," explaining how metadata could have been used by the British government to destroy the American Revolution before it even began. While intended to be humorous, the blog post also highlights the incredible capability of metadata analysis, showing how using Samuel Adams, a known revolutionary, as a starting point, just a few "hops" would pinpoint Revere as the key figure within the various revolutionary groups connected to every independence group and almost every member of those groups. (See Figure 11)[215] Ironically, although Healy was trying to cast a negative light on these programs with his writing; it also makes the point that metadata has the potential to be incredibly effective in the fight against terrorism.

General Hayden also spoke of the effectiveness of these types of programs, both in their own right and for the fact that they "force [the] enemy into less efficient modes of communication." While explaining that he would always prefer to intercept most of an enemy's, in this case terrorists', communications, "[i]f you take away the agility, flexibility, that's a plus."[216] This is backed up in terrorist literature, such as the aptly

---

[213] Barack Obama, "Statement by the President" (speech and press conference, San Jose, CA, June 7, 2013)

[214] Barack Obama, "Remarks by the President on Review of Signals Intelligence" (speech at the Department of Justice, Washington, DC, January 14, 2014)

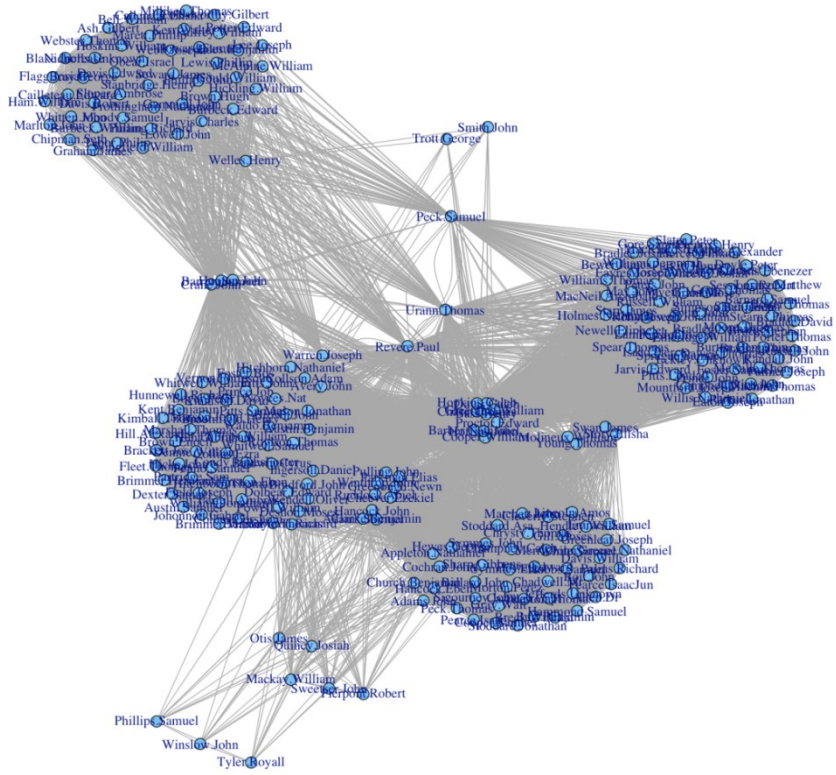
[215] Kieran Healy, "Using Metadata to Find Paul Revere," *kieranhealy.org* (blog), June 9, 2013, http://kieranhealy.org/blog/archives/2013/06/09/using-metadata-to-find-paul-revere/

[216] Hayden, in conversation with the author, September 21, 2015

titled online handbook "How to Survive in the West," which was anonymously published in the summer of 2015. With some paranoia about the NSA's capabilities, the guide says that

> if you mention the name Osama on a phone, your phone conversation will suddenly get extra triggered by space agencies. Whereas if you spoke casually and described him instead, your phone would be recorded (everyones [sic] phone conversations are), but it probably would be ignored unless there was already some suspicion/case against you.[217]

Regardless of the accuracy of this statement, it clearly shows that the NSA's efforts have



F11: Paul Revere's Connections Chart from Kieran Healy showing the extent to which metadata can uncover connections, with Paul Revere as the example

been rewarded on one level by forcing terrorists to adapt to new methods of

[217] "How to Survive in the West: A Mujahid Guide," published 2015

communicating, which at worst slows them down, and at best disrupts active planning and plotting. In light of the massive uptick in terrorist plots directed at the west in the last two years, this has a great deal of value.[218]

Claims of efficacy do not just come from the current administration and former NSA officials. In one slide from the XKEYSCORE presentation, the NSA itself claimed to have captured over 300 terrorists using the program. (See Figure 12)[219] This does not

F12: XKEYSCORE Successes training slide from NSA alleging success on massive scale

say specifically whether or not any of those terrorists were in the United States, but either

[218] *See* Majority Staff of the Homeland Security Committee, "Terror Threat Snapshot: September 2015," *Chairman of the Committee on Homeland Security of the House of Representatives*, September 4, 2015, available at https://homeland.house.gov/wp-content/uploads/2015/09/Complete-September-Terror-Threat-Snapshot.pdf. Please note that the author worked extensively on and provided a significant portion of the research for this product.

[219] "XKeyscore Presentation From 2008…"

way, if true, that is a significant number of enemies to have removed from a global, irregular battlefield.

Even then-Senator Mark Udall (D-CO), a noted critic of the programs revealed by Edward Snowden and a member of the Senate Select Committee on Intelligence (SSCI) during his one term in the Senate, defended PRISM, saying in the days after the leaks that "it's been very effective."[220] Together with Senator Ron Wyden (D-UT), Udall led the charge against what he viewed as illegal and invasive intrusions into the private lives of American citizens,[221] so having his endorsement of one of these programs is a powerful argument for its effectiveness.

Another unlikely supporter of PRISM and other 702 programs is the PCLOB. The PCLOB is a congressionally chartered independent agency intended to

> analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties; and ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism.[222]

After being given several briefings on the program's operations, technical details, and procedure rules by officials from the IC and Department of Justice,[223] the Board, in a report requested by a 'bipartisan group of U.S. Senators…[and] House Minority Leader

---

[220] Jennifer Rubin, "Shedding Light on the PRISM Program," *Washington Post*, June 10, 2013, https://www.washingtonpost.com/blogs/right-turn/wp/2013/06/10/shedding-light-on-the-prism-program/

[221] "Wyden, Udall on Revelations that Intelligence Agencies Have Exploited Foreign Intelligence Surveillance Act 'Loophole,'" *Office of Senator Ron Wyden*, April 1, 2014, https://www.wyden.senate.gov/news/press-releases/wyden-udall-on-revelations-that-intelligence-agencies-have-exploited-foreign-intelligence-surveillance-act-loophole

[222] Garrett Hatch, "Privacy and Civil Liberties Oversight Board: New Independent Agency Status," *Congressional Research Service*, August 27, 2012, available at http://www.fas.org/sgp/crs/misc/RL34385.pdf

[223] "Report on the Surveillance…," 2-3

Nancy Pelosi,"[224] stated that Section 702 "has proven valuable in the government's efforts to combat terrorism as well as in other areas of foreign intelligence."[225] Indeed, PRISM allegedly "generated an average of four items per day for the President's daily intelligence briefing in 2012."[226]

Combined, the programs authorized under Sections 215 and 702 are claimed by former NSA Director Keith Alexander to have assisted in the prevention of forty two terrorist plots and twelve arrests for material support to terrorism.[227] This needs to be examined in the context of potential harm to Americans' civil liberties, but it is not an insignificant number of plots that have been foiled.

Arguments for Ineffectualness

For every argument, there is a counter, and this is equally true in the case of the effectiveness of the 215 and 702 programs. For every person in favor of these tools as important pieces in the counterterrorism puzzle, there is someone disagreeing and espousing the opinion that they are ineffective, wastefully expensive, or both. Though Senator Udall argued for PRISM's effectiveness, he was adamant that the 215 programs, which pulled in metadata, were far less important, saying "I am not convinced that it's

[224] Ibid, 1

[225] Ibid, 10

[226] Loren Thompson, "Why NSA's PRISM Program Makes Sense," *Forbes*, June 7, 2013, http://www.forbes.com/sites/lorenthompson/2013/06/07/why-nsas-prism-program-makes-sense/#385387b75eb7

[227] John W. Rollins, and Edward C. Liu, "NSA Surveillance Leaks: Background and Issues for Congress," *Congressional Research Service*, September 4, 2013

uniquely valuable intelligence that we could not have generated in other ways."[228] The PCLOB agreed again, with its report on the 215 program arguing that it

> has shown minimal value in safeguarding the nation from terrorism. Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack. And we believe that in only one instance over the past seven years has the program arguably contributed to the identification of an unknown terrorism suspect. Even in that case, the suspect was not involved in planning a terrorist attack and there is reason to believe that the FBI may have discovered him without the contribution of the NSA's program.[229]

According to the *Washington Post*, unnamed Obama Administration officials admitted that this was the case, acknowledging "that it had contributed in just one case involving material support for terrorism," rather than thwarting an actual attack.[230]

According to NSA officials who spoke with Washington Post reporter Ken Dilanian in March of 2015, the agency "considered abandoning its secret program to collect and store American calling records in the months before leaker Edward Snowden revealed the practice…because some officials believed the costs outweighed the meager counterterrorism benefits." Though there was doubt that General Alexander would approve the shutdown, there was a significant push from "top managers" to do so. Part of this was the ineffectiveness of the program itself, and part was due to the "high costs of vacuuming up and storing the 'to and from' information from nearly every domestic landline call…[while the] program was not central to unraveling terrorist plots." David

---

[228] Rubin

[229] "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," *Privacy and Civil Liberties Oversight Board*, January 23, 2014, available at https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf, 11

[230] Nakashima

Medine, the chairman of the PCLOB, said that while NSA officials had "put on a pretty strong defense for the program…their success stories didn't pan out."[231]

The very thing that makes these programs potentially successful also makes them extremely difficult to use. Deputy Attorney General James Cole told the House's intelligence oversight committee that "if you're looking for a needle in the haystack, you have to get the haystack first."[232] The issue with that assertion is that one would even be able to find the needle. After all, the needle in a haystack analogy is used to denote a search that is either impossible or so close to it that there is no point in even making the attempt. Thus, the assertion that "they need to compile a giant haystack of data to find needles quickly"[233] is, *prima facie*, absurd. With even the Obama administration admitting that "Section 215 has been useful in a discrete number of terrorism cases," there is no strong argument that it is actually an effective tool that has been presented by anyone except the NSA itself, which has a vested interest in keeping an extremely expensive, technologically advanced program active.

This apparent lack of success on the part of the 215 programs brings into question their value. Considering the incredible cost in man hours, technology, and infrastructure, not to mention legal costs and the realized risk of it becoming, as one NSA senior staffer told Dilanian some in the agency feared, "deeply controversial if made public,"[234] it seems logical that the correct course of action would have been shutting them down well

---

[231] Ken Dilanian, "Before Snowden Leak, NSA Mulled Ending Call Collection," *Washington Post*, March 30, 2015

[232] Quoted in: Rollins and Liu

[233] Chris Strohm and Roger Runningen, "The NSA's Giant Haystack: Big Data Meets Big Surveillance," *Bloomberg*, last updated December 4, 2015, http://www.bloombergview.com/quicktake/nsa-data-telephone-surveillance

[234] Dilanian

before Edward Snowden even began leaking information. Additionally, as officials knew then and Congress has codified now, all metadata records would still have been available through FBI initiated subpoenas and warrants through the phone companies, which maintain the data for billing purposes.[235]

Considering the support throughout both the intelligence community and from outside, presumably independent observers and critics such as the members of the Privacy and Civil Liberties Oversight Board, for the 702 programs such as PRISM, it is impossible to deny their effectiveness; any questions about them will come down to issues of legality, personal privacy and the Fourth Amendment requirements for searches and seizures. 215 programs, on the other hand, have little to no support, and are so cumbersome and expensive that it is difficult to imagine how the money, time, and brain-power (both human and computer) poured into them are not being wasted.

[235] Ibid; and "H.R. 2048: Uniting and Strengthening…"

CONCLUSIONS

"The necessity of procuring good Intelligence is apparent and need not be further urged—All that remains for me to add is, that you keep the whole matter as secret as possible. For upon Secrecy, success depends in Most Enterprizes [sic] of the kind, and for want of it, they are generally defeated."[236] These words are as true today as they were in 1777 when George Washington wrote them, and they are the reason that the American people cannot be privy to every piece of information about their government's actions, as many would prefer. However, the people do have the right to know some things, and when their rights are violated, or government commits waste or fraud, it is within the purview of the people to object. In this case, there is one set of programs that the United States federal government used that some people inside and out of the intelligence community objected to based on their legal issues and efficacy; and a second set of programs that are effective and still legally questionable, but are well accepted to be useful, efficient, and important. These are the 215 and 702 programs, respectively. So the question becomes, at a time when "Congress and the nation are…divided about the proper balance between liberty and security,"[237] what to do with them?

Senator Frank Church may have best described the risks involved with programs such as these when, in 1975, he spoke the following words to describe the capabilities of the federal government in signals intelligence:

---

[236] George Washington to Elias Dayton, July 1777, quoted in: John Helgerson, *Getting to Know the President: CIA Briefings of Presidential Candidates 1952-1992* (Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 1995), 65

[237] Nakashima

> The United States government has perfected a technological capability that enables us to monitor the messages that go through the air…. That capability at any time could be turned around on the American people, and no American would have any privacy left, such is the capability to monitor everything—telephone conversations, telegrams, it doesn't matter. There would be no place to hide.[238]

Senator Church would be astounded by the capabilities of the NSA today, but he would also likely be horrified. No place to hide, indeed; virtually every American over the age of ten has a smartphone, tablet, or laptop, if not all of the above, all of which are connected to the internet or mobile network, and are thus potentially subject to some kind of monitoring by the National Security Agency. Failure to place checks and limits on this kind of power has led to a situation where the potential for abuse is indeterminably high.

To those who would say that safeguards are in place, with people watching over the system for abuses, Thomas Jefferson answers: "In questions of power, then, let no more be heard of confidence in man, but bind him down from mischief by the chains of the Constitution."[239] Recent NSA officials have even caused concerns for their predecessors, as General Hayden was said to have remarked on the "heartburn" that General Keith Alexander, who followed him as NSA director, caused him with his methods and approaches towards collection, which was said to take the attitude of "[l]et's not worry about the law. Let's just figure out how to get the job done."[240] This kind of attitude must not be allowed to pervade any portion of the United States government, but particularly not the military and intelligence communities.

---

[238] Quoted in: Greenwald, *No Place to Hide*, unnumbered page prior to index. This quote provided the book's title.

[239] Quoted in: Ibid, 24

[240] Shane Harris, "The Cowboy of the NSA," *Foreign Policy*, September 9, 2013, http://foreignpolicy.com/2013/09/09/the-cowboy-of-the-nsa/

Righting those wrongs needs to be the first step, and is a good start down the path toward reconciling the actions of government with the Constitution. The next step must be to immediately and permanently discontinue all warrantless collections of data, meta or otherwise, on American citizens and U.S. persons. Any warrants currently issued by FISA courts should be invalidated unless and until they have been reviewed by the judges serving on the Circuit Courts of Appeal in which each target is located, and they must meet both the traditional and constitutionally mandated standard of probable cause. Programs such as the sharing of information derived from warrantless collection of metadata with domestic law enforcement must immediately halt as well, with exceptions for exigent circumstances.

This is not to say that the programs must be shut down. The NSA can and, indeed, should track any non-U.S. persons who are not on American soil as it sees the need to; it is tasked with the collection of signals intelligence, and it should do just that, provided it does not violate the rights of United States citizens and others in American territory. Pulling data from American servers and switches is also acceptable in the case of non-U.S. person information (i.e. European phone or internet traffic that has only entered the United States due to the location of the servers and infrastructure the provider uses), as long as the companies involved either agree to provide such information willingly or are subject to a court order from a standard federal court. In certain cases, the third party doctrine could be applied, but it should be used sparingly and only in the last resort.

9/11 increased popular awareness about what threatens the United States. In the years following, the intelligence services did things that they would never have imagined

prior to that clear Tuesday morning's horrors, including waterboarding and "extraordinary" rendition by the Central Intelligence Agency,[241] the infiltration of mosques by Federal Bureau of Investigation agents,[242] and General Hayden opting against the tradition of "play[ing] a bit back from the line," and instead barreled full speed ahead through it. As Bamford has described it, "the NSA had long been 'gatherers'…they would become 'hunters.'[243]

Stewart A. Baker, an NSA General Counsel in the early to mid-1990s, said that "[t]oday the risk to civil liberties is largely theoretical. However theoretical [those] risks…may be, they cannot be ignored."[244] General Hayden spoke of "conceptual liberty loss." "This is about reasonable decisions that free people have to make all the time. Balancing two things, which are both virtues: security and liberty."[245] Both are right, in that much of what is at risk is not concrete or immediately harmful, but must be viewed skeptically, looking for balance; the key, however, is that rather than "all ties" going to more collection, they must lean towards more constitutional protectionism.

Even former NSA employees are speaking out against the agency, urging potential applicants to look elsewhere for work. Charles Seife, a Princeton educated "Director's Summer Program" NSA recruit from the early 1990s, and now a professor at New York University, wrote a lengthy open letter in *Slate* in August of 2013 decrying his

---

[241] *See* John Rizzo, *Company Man: Thirty Years of Controversy and Crisis in the CIA* (New York, NY: Scribner, 2014), for explanations of the thinking and rationale behind such actions.

[242] Jerry Markon, "Mosque Infiltration Feeds Muslims' Distrust of FBI," December 5, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/12/04/AR2010120403720.html

[243] Bamford, *The Shadow Factory*, 108

[244] Bamford, *Body of Secrets*, 450-51

[245] Hayden, in discussion with the author, September 21, 2015

once-held "idealistic vision that we were doing something to help our country."[246] Although he does state that the agency did work that legitimately improved national security, at the time the rules—and the circumstances—were different. Now he sees abuses and urges his former colleagues—both those still working and retired—to speak out against those misapplications of NSA authority, stating:

> I can only guess how much more horrified the ex-NSAers I know—you, my former colleagues, my friends, my professors, and my mentors—must be. Unlike me, you have spent much of your working lives helping the NSA build its power, only to see your years of work used in a way it was never supposed to be used. You could speak out now in a way that violates neither your secrecy agreement nor your honor. It's hard to believe that the professors I know at universities around the country would remain silent as the NSA abuses their trust and misuses their work.[247]

Altering the process by which the NSA obtains metadata, as prescribed in the USA FREEDOM Act, is a good start; companies holding this data for themselves, rather than being compelled to hand it to the government, is a significant improvement over the previous system wherein the NSA simply seized the data.[248] This system is still not perfect, as the standard being used is still "reasonable and articulable suspicion," below that of *probable cause*.[249] It also fails to address the issues inherent in the FISA Court, but it is a step in the right direction.

Former NSA employees and critics William Binney, Thomas Drake, and Kirk Wiebe—all of whom consider themselves whistleblowers for their parts in revealing what

---

[246] Charles Seife, "An Open Letter to My Former NSA Colleagues," *Slate*, August 22, 2013, http://www.slate.com/articles/health_and_science/science/2013/08/nsa_domestic_spying_mathematicians_should_speak_out.html

[247] Ibid

[248] "H.R. 2048: Uniting and Strengthening…"

[249] Civil Liberties and Privacy Office, "Transparency Report: The USA FREEDOM

they saw as wasteful NSA programs in the early 2000s[250]—have said that the USA FREEDOM Act does not alleviate the concerns expressed by Seife. Wiebe declared in April 2015 that the bill would simply be "more of the same" and was "not going to change anything."[251]

In the corporate technology sector, on the other hand, there was general approval for the new bill after its passage in June of 2015. Google and Facebook both issued statements after President Obama signed the USA FREEDOM Act into law supporting the new statute. A Facebook vice president, Susan Molinari, wrote that the "vote represents a critical first step toward restoring trust in the Internet, but it is only a first step. We look forward to working with Congress on further reforms in the near future."[252] Symantec, a major information technology security company, issued a statement praising the bill that "strikes the right balance between protecting national security and the privacy of citizens around the world," while calling the measure "long overdue."[253]

What the tech sector failed to acknowledge is that the USA FREEDOM Act's authors neglected to void the constitutionally indefensible reasonable, articulable suspicion standard used in the obtaining court orders from the FISC to search and seize data from telecommunications companies. The Fourth Amendment clearly defines what

---

[250] Drake pled guilty to a misdemeanor after initially being charged under the Espionage Act for revealing to Congress, and allegedly the press, what he saw as waste in the Trailblazer Project

[251] Steven Nelson, "NSA Whistleblowers Oppose Freedom Act, Endorse Long-Shot Bill," *U.S. News & World Report*, April 27, 2015, http://www.usnews.com/news/articles/2015/04/27/nsa-whistleblowers-oppose-freedom-act-endorse-long-shot-bill

[252] Angela Swartz, "What Silicon Valley Tech Firms Think of the USA Freedom Act's Approval," *Silicon Valley Business Journal*, last updated June 3, 2015, http://www.bizjournals.com/sanjose/news/2015/06/02/what-silicon-valley-tech-firms-think-of-the-usa.html

[253] Ibid

is needed to obtain a warrant, and while the new architecture meets the specificity requirement, it fails to meet the probable cause standard. Emergent situations aside, RAS is not a legitimate standard for a search or seizure, and the Supreme Court has said this many times. The use of the *Terry v. Ohio* standard in everyday activity is a clear violation of the legal precedent, and should be ended in subsequent legislation.

Violation of constitutional protections has other negative effects beyond simply the harm, or potential harm, to American citizens. Among the potential ramifications is an impact on government recruiting efforts. The NSA prides itself on its people, and well they should; the agency "is said to be the largest employer of mathematicians in the United States and perhaps the world." It employs "[a]nalysts, engineers, physicists,…linguists, and computer scientists" in untold numbers.[254] Certainly there are thousands of brilliant, highly skilled, and highly educated people working there who could easily make significantly more money in the private sector, but have, for a variety of reasons, chosen to work for the United States government.

In March of 2015, *National Public Radio* broadcast a story examining the difficulties the NSA was beginning to have recruiting the talented young people they need, focusing on a young man who grew up with the intentions of one day working at the agency located not far from his childhood home. This young man, Daniel Swann, was finishing up a dual Bachelor's and Master's degree at Johns Hopkins in cybersecurity, and "is exactly the type of person the National Security Agency would love to have working for it." But in the wake of the Snowden leaks, for all of Swann's

[254] Harvey A. Davis, "Statement for the Record before the Governmental Affairs Subcommittee on International Security, Proliferation, and Federal Services," *U.S. Senate Committee on Governmental Affairs*, March 12, 2002

prior intent and expectations, he decided not even to apply. "I can't see myself working there…partially because of these moral reasons," he said.[255]

According to the *NPR* story,

> [t]his year, the NSA needs to find 1600 recruits. Hundreds of them must come from highly specialized fields like computer science and mathematics. So far, it says, the agency has been successful. But with its popularity down, and pay from wealthy Silicon Valley companies way up, agency officials concede that recruitment is a worry. If enough students follow Daniel Swann, then one of the world's most powerful spy agencies could lose its edge.[256]

Considering the importance of the National Security Agency, losing talent of that nature could be devastating to the United States. Actions to prevent this concern from becoming reality must be taken. That does mean increasing pay to compete, at least peripherally, with private companies, but also it requires mitigating concerns and moral qualms that do not exist when a computer programmer or math genius goes to work at Facebook or Intel.

Adding a new moral or ethical component into the calculation of potential recruits will make it even more difficult for NSA to recruit qualified talent. Edward Snowden claimed he was leaking documents because of his objections to government surveillance possessing the potential ability to put "limits [on] the boundaries of [users'] exploration"[257] of the internet; this kind of thought process is likely to resonate with a group of young people that have spent their lives pushing those boundaries. Computer experts have been especially difficult to attract to government—particularly law enforcement—because of ultra-strict security background requirements, and so rules have

---

[255] Geoff Brumfiel, "After Snowden, the NSA Faces Recruitment Challenge," *National Public Radio*, March 31, 2015, http://www.npr.org/2015/03/31/395829446/after-snowden-the-nsa-faces-recruitment-challenge

[256] Ibid

[257] *Citizenfour*

had to be relaxed or reconsidered to attract that group.[258] Providing new reasons for those particular specialists to decide not to apply to an organization as vital to the nation's security and military strength as the National Security Agency is exactly the wrong thing to be doing. Even if the issues with the secret programs revealed in leaked documents are being exaggerated by anti-surveillance zealots—and both Laura Poitras and Glenn Greenwald would certainly qualify—the appearance is enough to cause many people to rethink the decision to apply or accept a job at the NSA. The inherent secrecy of the intelligence community makes any leak seem bigger, more explosive, and more controversial than the facts would lend an insider to believe, but to those looking in from the outside, the details can be scandalous and damaging.

The moral questions involved with this do not stop with applicants or even current employees of NSA or its IC counterparts. Americans pride themselves on being citizens of a country that holds the moral high ground and is a leader in the international community. Much of that stems from the U.S. Constitution, a document that enumerates rights that Americans hold dear and which provides protections for such civil liberties as free speech, fair trials, and freedom from overly aggressive government invasion of privacy. It becomes far more difficult to lecture other nations on their governments' abuses of civil liberties when the U.S. federal government is conducting intelligence operations that include the potential for serious abuses of its own. Even where actual abuse does not occur, the appearance that it could is problematic for many within and outside the United States. The actions of government are always ripe for interpretation by experts and laypersons alike; in a situation like the collection of metadata where a

[258] Charles Levinson, "FBI Weighs Looser Pot Rules for New Hires," *Wall Street Journal*, May 20, 2014, http://www.wsj.com/articles/SB10001424052702304422704579574374286817550

customer has no real expectation that their metadata will not be collected and exploited by his or her service provider for billing and marketing purposes, the extra step of providing that information to the government without a warrant or any allegation of criminal activity is easily viewed as abusive and overly intrusive.

More concerning than the current legal issues with the programs is the potential for future abuse. During the early years of the Cold War, President Dwight D. Eisenhower posited that if South Vietnam fell to the communist forces of the North, it would trigger a chain reaction in the region, resulting in the fall of capitalism throughout Southeast Asia.[259] The same types of concerns are present when examining issues of domestic intelligence collection. If government is allowed to conduct a few programs that violate the Constitution in the name of security, what is to stop it from doing more? The current "issue of the day" is terrorism, but tomorrow could easily bring a return to the days where the most important matter for government is the War on Drugs and suddenly instead of being used to search for foreign terrorists, the NSA is targeting U.S. drug dealers using the public health crisis that is the heroin epidemic in the Northeast United States[260] as an excuse. The *Necessary and Proper Clause* of the Constitution could be cited as justification for this about face as easily as it can be applied to the current usage of the NSA's metadata collection programs. No one can predict what the next crisis to face the United States will be, but with any calamity will come calls for government to do something, anything, to stop the next threat, regardless of what it may be.

---

[259] Jean Collins, "The Domino Theory," *The North American Review* 252, no. 3 (May, 1967), 19

[260] *See* Ben Schreckinger, "New England Confronts Heroin Epidemic," *Al-Jazeera America*, March 16, 2014, http://america.aljazeera.com/articles/2014/3/16/new-england-confrontsheroinepidemic.html

A similar argument is already playing out in the federal courts, with Apple and the Department of Justice fighting over whether a company can be required to write code that would open a "backdoor" for law enforcement to defeat the encryption that is currently protecting the cell phone of an American terrorist. DoJ contends that the software would only be for a specific device, while Apple argues that it could potentially be used to affect all similar pieces of hardware.[261] This controversy, which is part of a greater argument on encryption of personal devices, has even pitted the NSA against the FBI, with Admiral Mike Rogers, NSA's current director, arguing against encryption backdoors while FBI Director James Comey demands that companies make it easier for law enforcement to access encrypted cell phones, tablets, and computers.[262] At a time when end-to-end encryption is becoming more common and simple to use for even people who are not technologically proficient,[263] criminals ranging from child-pornography peddlers to drug dealers are able to take advantage of systems that the government will be unable to crack in all but the most limited circumstances. In this case, terrorists can use the same types of programs as common criminals, and if the U.S. government (or any other nation's intelligence service, for that matter) does manage to locate a phone number, e-mail address, or other identifier, exploitation of that

[261] *See* Jim Finkle and Joseph Menn, "Privacy Versus Security at Heart of Apple Phone Decrypt Order," *Reuters*, February 18, 2016, http://www.reuters.com/article/us-apple-encryption-idUSKCN0VQ2AK

[262] Jonathan Keane, "NSA Director Actually Says Encryption Backdoors Are a Bad Idea," *Digital Trends*, January 23, 2016, http://www.digitaltrends.com/computing/nsa-director-actually-says-encryption-backdoors-are-a-bad-idea/

[263] Jenna McLaughlin, "Bill that Would Ban End-to-End Encryption Savaged by Critics," *The Intercept*, April 8, 2016, https://theintercept.com/2016/04/08/bill-that-would-ban-end-to-end-encryption-savaged-by-critics/. Several common computer, cellular telephone, and tablet applications now include end-to-end encryption without requiring any modification or settings changes by the user. Additionally, cellular telephones running the Apple iOS or Android operating systems are easily encrypted, requiring the user to make only very minor changes using instructions that are found numerous websites.

information has become significantly more difficult. Add in the fact that terrorists are instructed to switch phones regularly to avoid being tracked,[264] and suddenly the IC is faced with a moving target that it would take a "billion billion years" to decrypt;[265] in other words, more than 200 million times longer than Earth has been in existence. This debate is not nearly over, even though the Department of Justice has withdrawn one of its lawsuits against Apple demanding assistance in unlocking an iPhone.[266]

While this issue is by no means the same as the concern over NSA being able gain access to Americans' email and phone data, it is part of a greater debate over the role of law enforcement and the intelligence community where national security, privacy, and emerging technology all come together. As Marc Goodman, a technology expert and "futurist" who has worked with the FBI, Interpol, and in municipal law enforcement, wrote,

> The more we plug our devices and our lives into the global information grid—whether via mobile phones, social networks, elevators, or self-driving cars—the more vulnerable we become to those who know how the underlying technologies work and how to exploit them to their advantage and to the detriment of the common man. Simply stated, when everything is connected, everyone is vulnerable.[267]

While Goodman was discussing how criminals can take advantage of widespread connectivity, his point is equally applicable to the NSA and the rest of the American

---

[264] "How to Survive in…"

[265] Mohit Arora, Sr., "How Secure is AES Against Brute Force Attacks," *EE Times*, May 7, 2012, http://www.eetimes.com/document.asp?doc_id=1279619. This number assumes the use of a 128 bit encryption key, which uses a randomized string of 128 numbers (in binary, using just 1s and 0s) creating a total of $3.4x10^{38}$ possible combinations. This is the level of encryption used by common communications applications such as Facebook Inc.'s WhatsApp.

[266] Katie Benner and Eric Lichtblau, "U.S. Says it Has Unlocked iPhone Without Apple," *New York Times*, March 28, 2016, http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?_r=0. Multiple other lawsuits are still ongoing.

[267] Marc Goodman, *Future Crimes: Everything is Connected, Everyone is Vulnerable, and What We Can Do About it* (New York, NY: Doubleday, 2015), 2

intelligence community. The near-ubiquity of wired and wirelessly connected devices, also known as the "internet of things," has made NSA's job both more difficult by increasing the amount of collectable data, and much simpler by making available data and communication information that would have been nearly impossible to obtain even ten years ago, much less during the Cold War era. Patrick Tucker, another "futurist," wrote that the "rate by which we can extrapolate meaningful patterns from the data of the present is quickening as rapidly as is the spread of the Internet because the two are inexorably linked. The Internet is turning prediction into an equation."[268] This will only become truer in the future as technology advances, giving intelligence agencies increasingly more targets for collection. The more data-points that are available to collect and analyze, the clearer the image of how people live their lives will become. Tucker explained that

> [t]he little actions, transactions, and exchanges of daily life do have a rhythm…and correspond to one another in a manner not unlike a melody… If you're like most people, your life has a certain routine… Any tune composed of a repetitious sequence of notes becomes predictable. With sensors, geographic information systems, and geo-location-based apps, more of those notes become audible.[269]

Although you can "turn down the signal that you're sending out [by cutting your use of internet and global positioning system-enabled devices], that doesn't actually make you less predictable."[270] Even the option of limiting data output will become increasingly difficult in the future as a greater percentage of the devices that average Americans use

[268] Patrick Tucker, *The Naked Future: What Happens in a World That Anticipates Your Every Move?* (New York, NY: Penguin Group, 2014), xiii

[269] Ibid, xvi

[270] Ibid, 29

on a daily basis are added to the "internet of things" and that output becomes automatic and normal.

It is hardly noteworthy today when Facebook recognizes in which specific restaurant a user is dining, or Google Maps recommends the best route home at 5:00pm on weekdays because the Android operating system tracks when users come and go from common locations and determines what must be the user's place of employment. The opening scenario of Tucker's book *The Naked Future*, wherein a smartphone in the future informs the user that when leaving work, he will run into an ex-girlfriend who will tell him that she is engaged, is not that far-fetched; a high powered computer with access to a combination of long-term metadata and location data plus Facebook posts for both people could easily determine that this scenario is likely to play out.[271] Putting that kind of power into the hands of corporations is scary in its own way; putting it into the hands of a government that has repeatedly demonstrated that it has the capacity and will to break the law in times of what it considers dire need is legitimately terrifying if the right safeguards are not enacted.

The standard for what is an emergency or a great necessity for the government is different for the al-Qa'ida hunting NSA post-September 11th, 2001 than it was for the paranoid J. Edgar Hoover and his civil rights activist hunting FBI in the 1960s. General Hayden posited that the TSA's intrusive searches would not have been upheld by the courts before 9/11; in the post-9/11 world, that agency is simply an accepted part of the hassle of flying.[272] National changes in attitude can be rapid or gradual, but in either case without firm, clear laws in place the whims of the people or the government can be used

[271] Ibid, xi-xii

[272] Hayden, in discussion with the author, September 21, 2015

to justify actions that would previously have been anathema, and it is impossible to predict what will spur opinion change in these areas. General Hayden wrote that "[a]voiding the hard choices creates a whipsaw effect, based on the perceptions of the moment, and ultimately costs us both freedom and security."[273]

Tucker also correctly makes the point that "the worst possible move we as a society can make right now is demand that technological progress reverse itself. This is futile and shortsighted."[274] Americans must instead adopt laws and regulations that do not restrict the technological abilities of private citizens, corporations, or even the NSA; rather, these laws need to restrict how the government can *use* its new technology. Rather than simply deploying a new piece of software because it will collect more intelligence, the NSA, FBI, and the rest of the IC need to have a process by which they vet that software both internally and with the oversight of Congress and experts who can examine it with disinterest. This could include the Privacy and Civil Liberties Oversight Board, as it already has a similar role in examining programs, but this function would add a more proactive nature to the Board's activities.

This process would certainly take longer than simply using the in-house general counsels that each agency and the DNI employ, but it will help to ensure that the people have an unbiased arbiter protecting their rights. Using an additional safeguard proposed by General Hayden, collaboration with the media through more openness,[275] will also lead to a broadening of trust between the citizenry and the government and offers a new

---

[273] Michael V. Hayden, *Playing to the Edge: American Intelligence in the Age of Terror* (New York, NY: Penguin Press, 2016), 35

[274] Tucker, xviii

[275] Michael Hayden (retired General, United States Air Force, former Director, Central Intelligence Agency and National Security Agency, former Principal Deputy Director of National Intelligence) in discussion with the author, September 28, 2015

form of oversight. Obviously he did not mean tell the media everything that the NSA or CIA is doing, but giving them an explanation of what is happening, rather than a "no comment" every time, will allow journalists to provide more information to their readers, listeners, or viewers, and give people a more informed perspective on the issues at hand. It will also give the people an opportunity to form more nuanced, informed opinions on the validity, necessity, and legality of the intelligence community's activities.

As Matthew Aid wrote regarding the Bush Administration's warrantless collection program:

> Sadly, it seems likely that it will take years before the classified storage vaults are opened and a better understanding of the NSA warrantless eavesdropping program becomes available. Until then, it will be impossible for the American public to fully understand, much less appreciate, the implications of the NSA program and the culture of fear that gave birth to it and continues to sustain it today.[276]

This sentiment applies as well today as it did when it was written in 2008. The proselytizing about the risk of terrorism, by both the government and the media, poses as great a danger to the rights of Americans as any other single portion of the equation that leads to programs such as those described herein. There is no doubt that the best intentions motivated the production and implementation of PRISM, XKEYSCORE, and the myriad of other systems that cause concern among civil liberty advocates, but in this case, it is not the thought that counts. The United States "Constitution… shall be the supreme law of the land; and the judges in every state shall be bound thereby."[277] That law is paramount, and the intelligence agencies can, and should, find ways to do their jobs protecting American lives and interests, within its bounds. Either way, Senator Ron

[276] Aid, 299

[277] "Constitution of the United States: Amendments 11-27," *U.S. Archives*, accessed January 29, 2016, http://www.archives.gov/exhibits/charters/constitution_amendments_11-27.html

Wyden said it best: "The fight to protect Americans' constitutional rights…is not over."[278] As long as there is a struggle between the rights of the people and the responsibilities of government, that fight will never be over, and never should be. Government needs to protect the people, and the people need to protect themselves from an overzealous government. The passage of the USA FREEDOM Act was a step in the right direction. Although nothing will ever satisfy everyone, a good outcome should be achievable provided that Congress, the executive, and the American people work together to find the right balance.

[278] Nakashima

BIBLIOGRAPHY

"22 U.S. Code §6010: 'United States Person' Defined." *United States Government Printing Office*. Last accessed January 27, 2016. https://www.gpo.gov/fdsys/pkg/USCODE-2010-title22/pdf/USCODE-2010-title22-chap69-sec6010.pdf

"50 U.S. Code §1806(A): Compliance with Minimization Procedures; Privileged Communications; Lawful Purposes." *United States Government Printing Office*. Last accessed March 6, 2016. https://www.gpo.gov/fdsys/pkg/USCODE-2011-title50/pdf/USCODE-2011-title50-chap36-subchapI-sec1806.pdf

Aid, Matthew M. *The Secret Sentry: The Untold History of the National Security Agency*. New York, NY: Bloomsbury Press, 2009

Albanesius, Chloe. "Report: NSA Secretly Spied on Yahoo, Google Data Centers." *PC Magazine*. October 30, 2013. http://www.pcmag.com/article2/0,2817,2426590,00.asp

Ambinder, Marc. "Solving the Mystery of PRISM." *The Week*. June 7, 2013. http://theweek.com/articles/463418/solving-mystery-prism

American Civil Liberties Union v. National Security Agency. 493 F.3d 644 (6th Cir. 2007)

"Are They Allowed to Do That?" *Brennan Center For Justice at New York University School of Law*, last accessed February 4, 2016, https://www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf

Ariosto, David and Deborah Feyerick. "Christmas Day bomber sentenced to life in prison." *CNN*. February 17, 2012. http://www.cnn.com/2012/02/16/justice/michigan-underwear-bomber-sentencing/

Armando Schmerber v. State of California, 384 U.S. 757 (1966)

Arora, Mohit Sr., "How Secure is AES Against Brute Force Attacks." *EE Times*. May 7, 2012. http://www.eetimes.com/document.asp?doc_id=1279619

Baker, Al and William K. Rashbaum. "Police Find Car Bomb in Times Square." *New York Times*. May 1, 2010. http://www.nytimes.com/2010/05/02/nyregion/02timessquare.html?pagewanted=all&_r=0

Bamford, James. *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*. New York, NY: First Anchor Books, 2001

-----. "The NSA is Building the Country's Biggest Spy Center (Watch What You Say)." *Wired*. March 15, 2012. http://www.wired.com/2012/03/ff_nsadatacenter/

-----. *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*. New York, NY: Doubleday, 2008

Barnett, Mark L. "National Security Agency/Central Security Service." Unclassified presentation to the Greater Baltimore Committee, April 26, 2011

Bell, Ron. "Shedding Light on the Foreign Intelligence Surveillance Court (FISC): Court Findings from Our 2007-2008 Case." *Tumblr.com*. September 11, 2014. http://yahoopolicy.tumblr.com/post/97238899258/shedding-light-on-the-foreign-intelligence

Benner, Katie and Eric Lichtblau, "U.S. Says it Has Unlocked iPhone Without Apple." *New York Times*. March 28, 2016. http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?_r=0

"Beyond Distrust: How Americans View Their Government." *Pew Research Center*. November 23, 2015. http://www.people-press.org/2015/11/23/1-trust-in-government-1958-2015/

"Bill of Rights." *U.S. Archives*. Accessed April 14, 2015. http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html

Blaze, Matt. "Phew, NSA is Just Collecting Metadata. (You Should Still Worry)." *Wired*. June 19, 2013. http://www.wired.com/2013/06/phew-it-was-just-metadata-not-think-again/

Boerma, Lindsey. "NSA Secretly Mining User Data from U.S. Internet Giants." Last updated June 7, 2013. http://www.cbsnews.com/news/nsa-secretly-mining-user-data-from-us-internet-giants/

Breslow, Jason M. "Obama on Mass Government Surveillance, Then and Now." *PBS*. May 13, 2014. http://www.pbs.org/wgbh/frontline/article/obama-on-mass-government-surveillance-then-and-now/

Brumfiel, Geoff. "After Snowden, the NSA Faces Recruitment Challenge." *National Public Radio*. March 31, 2015. http://www.npr.org/2015/03/31/395829446/after-snowden-the-nsa-faces-recruitment-challenge

Bump, Philip. "The NSA Admits it Analyzes More People's Data than Previously Revealed." *The Wire*. July 17, 2013. http://www.thewire.com/politics/2013/07/nsa-admits-it-analyzes-more-peoples-data-previously-revealed/67287/

Chappell, Bill. "Senate Approves USA Freedom Act, Obama Signs It, After Amendments Fail." *National Public Radio*. Last updated June 2, 2015. http://www.npr.org/sections/thetwo-way/2015/06/02/411534447/senateis-poised-to-vote-on-house-approved-usa-freedom-act

Cicero, Marcus Tullius. "Pro Tito Annio Milone ad iudicem oratio." Translated by C.D. Yonge. Accessed April 14, 2015. http://www.perseus.tufts.edu/hopper/text?doc=urn:cts:latinLit:phi0474.phi031.perseus-eng1:11

Citizenfour. HBO Films. 2014. Viewed via *HBOGO*

Civil Liberties and Privacy Office. "Transparency Report: The USA FREEDOM Act Business Records FISA Implementation." *National Security Agency*. January 15, 2016. Available at https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf

Clapper, James. "DNI Statement on Recent Unauthorized Disclosures of Classified Information." *Office of the Director of National Intelligence*. June 6, 2013. http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information

-----. Testimony before Senate Select Committee on Intelligence, Washington, D.C., March 12, 2013

Collins, Jean. "The Domino Theory." *The North American Review* 252, no. 3 (May, 1967): 19-20

"Constitution of the United States." *U.S. Archives*. Accessed September 6, 2015. http://www.archives.gov/exhibits/charters/constitution_transcript.html

"Constitution of the United States: Amendments 11-27," *U.S. Archives*, accessed January 29, 2016, http://www.archives.gov/exhibits/charters/constitution_amendments_11-27.html

"Constitutional Limitations on Judicial Power: Standing, Advisory Opinions, Mootness, and Ripeness." *University of Missouri-Kansas City School of Law*. Accessed April 26, 2015. http://law2.umkc.edu/faculty/projects/ftrials/conlaw/caseorcontroversy.htm

Darby, John. "SIGINT and the National Security Agency." Presentation at MSU DSS Intelligence, Countintelligence, and Covert Action class, Vienna, VA, February 25, 2015

David Leon Riley v. California; United States v. Brima Wurie, 573 U.S. ____ (2014)

David Muskrat and J. Henry Dick v. United States, 219 U.S. 346 (1911)

Davis, Harvey A. "Statement for the Record before the Governmental Affairs Subcommittee on International Security, Proliferation, and Federal Services." *U.S. Senate Committee on Governmental Affairs*. March 12, 2002

Dershowitz, Alan. *Piers Morgan Live*. By Piers Morgan. CNN, June 6, 2013

de Vogue, Ariane. "Court Rules NSA Program Illegal." *CNN*. Last updated May 7, 2015. http://www.cnn.com/2015/05/07/politics/nsa-telephone-metadata-illegal-court/

Diamond, Jeremy. "NSA Surveillance Bill Passes After Weeks-Long Showdown." *CNN*. Last updated September 7, 2015. http://www.cnn.com/2015/06/02/politics/senate-usa-freedom-act-vote-patriot-act-nsa/

Dilanian, Ken. "Before Snowden Leak, NSA Mulled Ending Call Collection." *Washington Post*. March 30, 2015

Dreyfuss, Benjamin and Emily Dreyfuss. "What is the NSA's PRISM Program? (FAQ)." *CNET*. Last updated June 7, 2013. http://www.cnet.com/news/what-is-the-nsas-prism-program-faq/

"Email Statistics Report, 2015-2019." *Radicati Group, Inc.* March 2015. Available at http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf

Executive Order 12333 -- United States Intelligence Activities," *National Archives*, last accessed January 13, 2016, http://www.archives.gov/federal-register/codification/executive-order/12333.html

"Facebook Reports First Quarter 2015 Results." *Facebook*. April 22, 2015. http://investor.fb.com/releasedetail.cfm?ReleaseID=908022

"Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act." *Office of the Director of National Intelligence*. June 8, 2013. http://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf

Feinstein, Dianne and Mike Rogers. *This Week*. By George Stephanopolous. ABC. June 9, 2013

Ferran, Lee. "Ex-NSA Chief: 'We Kill People Based on Metadata.'" *ABC News*. May 12, 2014. http://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata/

Fidler, David. "While Ruling NSA Program Illegal, Appeals Court Suggests Path Forward." *Defense One*. May 11, 2015. http://www.defenseone.com/politics/2015/05/while-ruling-nsa-program-illegal-appeals-court-suggests-path-forward/112435/

"Final Vote Results for Roll Call 224." *United States House of Representatives*. May 13, 2015. http://clerk.house.gov/evs/2015/roll224.xml

Finkle, Jim and Joseph Menn. "Privacy Versus Security at Heart of Apple Phone Decrypt Order." *Reuters*. February 18, 2016. http://www.reuters.com/article/us-apple-encryption-idUSKCN0VQ2AK

"Fruit of the Poisonous Tree." *Cornell University Law School Legal Information Institute*. Last accessed March 5, 2016. https://www.law.cornell.edu/wex/fruit_of_the_poisonous_tree

Fung, Brian. "The NSA is Giving Your Phone Records to the DEA. And the DEA is Covering it Up." *Washington Post*. August 5, 2013. http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/05/the-nsa-is-giving-your-phone-records-to-the-dea-and-the-dea-is-covering-it-up/

Gearan, Anne. "'No Such Agency' Spies on the Communications of the World." *Washington Post*. June 6, 2013. https://www.washingtonpost.com/world/national-security/no-such-agency-spies-on-the-communications-of-the-world/2013/06/06/5bcd46a6-ceb9-11e2-8845-d970ccb04497_story.html

Gellman, Barton and Laura Poitras. "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program." *Washington Post*. June 7, 2013. https://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

Gellman, Barton and Matt Delong. "The NSA's Three Types of Cable Interception Programs." Last accessed April 26, 2015. http://apps.washingtonpost.com/g/page/world/the-nsas-three-types-of-cable-interception-programs/553/#document/p7/a129998

"Global Top 100 Companies by Market Capitalization." *PWC IPO Centre*. London, England, March 31, 2014

Goldman, David. "Obama and NSA: So What is Metadata Anyway?" *CNN*. January 17, 2014. http://money.cnn.com/2014/01/17/technology/security/obama-metadata-nsa/

-----. "What is the Cloud?" *CNN*. September 4, 2014. http://money.cnn.com/2014/09/03/technology/enterprise/what-is-the-cloud/

Goldstein, Robert Justin. "Prelude to McCarthyism: The Making of a Blacklist." *Prologue Magazine* 38, no. 3 (Fall 2006). Available at http://www.archives.gov/publications/prologue/2006/fall/agloso.html

Goodman, Marc. *Future Crimes: Everything is Connected, Everyone is Vulnerable, and What We Can Do About it*. New York, NY: Doubleday, 2015

Greenberg, Andy. "Intelligence Officials Admit that Edward Snowden's NSA Leaks Call for Reforms." *Forbes*. September 13, 2013. http://www.forbes.com/sites/andygreenberg/2013/09/13/intelligence-officials-admit-that-edward-snowdens-leaks-call-for-reforms/#5a109b054ee5.

Greenwald, Glenn. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Metropolitan Books, 2014

-----. "NSA Collecting Phone Records of Millions of Verizon Customers Daily." *Guardian* (London). June 6, 2013. http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

-----. "XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet." *Guardian* (London). July 31, 2013. http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

Greenwald, Glenn and Ewen MacAskill. "Boundless Informant: the NSA's Secret Tool to Track Global Surveillance Data." *The Guardian*. June 11, 2013. http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining

Greenwald, Glenn, Ewen MacAskill, Laura Poitras, Spencer Ackerman, and Dominic Rushe. "Microsoft Handed the NSA Access to Encrypted Messages." *Guardian* (London). July 12, 2013. http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

Gross, Grant. "Judge: Give NSA Unlimited Access to Digital Data." *PC World*. December 4, 2014. http://www.pcworld.com/article/2855776/judge-give-nsa-unlimited-access-to-digital-data.html

Harper, Nick. "FISA's Fuzzy Line between Domestic and International Terrorism." *The University of Chicago Law Review* 81, no. 3 (2014): 1123-1164

Harris, Shane. "The Cowboy of the NSA." *Foreign Policy*. September 9, 2013. http://foreignpolicy.com/2013/09/09/the-cowboy-of-the-nsa/

Hatch, Garrett. "Privacy and Civil Liberties Oversight Board: New Independent Agency Status." *Congressional Research Service*. August 27, 2012. Available at http://www.fas.org/sgp/crs/misc/RL34385.pdf

Hayden, Michael V. *Playing to the Edge: American Intelligence in the Age of Terror*. New York, NY: Penguin Press, 2016.

Hayden, Michael, Alan Dershowitz, Glenn Greenwald, and Alexis Ohanian. "Munk Debate on State Surveillance." Munk Debate, Toronto, ON, May 2, 2014. Video available at https://www.youtube.com/watch?v=_d1tw3mEOoE

Healy, Kieran. "Using Metadata to Find Paul Revere." *kieranhealy.org* (blog). June 9, 2013. http://kieranhealy.org/blog/archives/2013/06/09/using-metadata-to-find-paul-revere/

Helgerson, John. *Getting to Know the President: CIA Briefings of Presidential Candidates 1952-1992.* Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 1995

Vanden Heuvel, Katrina and Stephen F. Cohen. "Edward Snowden: A 'Nation' Interview." *The Nation*. November 17, 2014. http://www.thenation.com/article/snowden-exile-exclusive-interview/

"How to Survive in the West: A Mujahid Guide." Published 2015

"H.R. 2048: Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-Collection and Online Monitoring (USA FREEDOM) Act of 2015 (114th Congress, 2015-2016)." *Library of Congress*. https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf

"H.R. 2399: LIBERT-E Act (113th Congress, 2013-2014)," *Library of Congress*. Last accessed March 17, 2016. https://www.congress.gov/bill/113th-congress/house-bill/2399?resultIndex=1

"H.R. 3162: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (107th Congress, 2001-2002)." *Library of Congress*. Last accessed December 17, 2015. https://www.congress.gov/bill/107th-congress/house-bill/3162/text?overview=closed&resultIndex=1

"H.R. 6304: Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (110th Congress, 2007-2008)." *Library of Congress*. Last accessed December 17, 2015. https://www.congress.gov/bill/110th-congress/house-bill/6304/text?overview=closed&resultIndex=1

In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 06-05 (FISA Ct. 2006)

In re Orders of this Court Interpreting Section 215 of the Patriot Act, No. BR 13-02 (FISA Ct. 2013)

"Intelligence Activities—National Security Agency and Fourth Amendment Rights." Testimony at U.S. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Washington, D.C., October 29, 1975

"International Convention on Civil and Political Rights." *United Nations Human Rights Office of the High Commission*. Last accessed March 2, 2016. http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

James R. Clapper v. Amnesty International USA, et al. 568 U.S. ____ (2013), No. 11-1025

John W. Terry v. State of Ohio, 392 U.S. 1 (1968)

Keane, Jonathan. "NSA Director Actually Says Encryption Backdoors Are a Bad Idea." *Digital Trends*. January 23, 2016. http://www.digitaltrends.com/computing/nsa-director-actually-says-encryption-backdoors-are-a-bad-idea/

Kennedy, John F. "Valediction." Speech at awards ceremony for Allen Dulles, Langley, VA, November 28, 1961. Available at https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol6no1/html/v06i1a07p_0001.htm

Kravets, David. "NSA Phone Snooping Cannot be Challenged in Courts, Feds Say." *Wired*. July 9, 2013. Accessed April 13, 2015. http://www.wired.com/2013/07/spygate-snooping-standing/

Lee, Micah, Glenn Greenwald, and Morgan Marquis-Boire. "Behind the Curtain: A Look at the Inner Workings of NSA's XKEYSCORE." *The Intercept*. July 2, 2015. https://theintercept.com/2015/07/02/look-under-hood-xkeyscore/

Levinson, Charles. "FBI Weighs Looser Pot Rules for New Hires." *Wall Street Journal*. May 20, 2014. http://www.wsj.com/articles/SB10001424052702304422704579574374286817550

Lincoln, Abraham. "The Gettysburg Address." Speech at the dedication of the Soldiers' National Cemetery, Gettysburg, PA, November 19, 1863. Reproduced at http://www.abrahamlincolnonline.org/lincoln/speeches/gettysburg.htm

Litt, Robert S. "Privacy, Technology and National Security: An Overview of Intelligence Collection." Speech at The Brookings Institution, Washington, DC, July 19, 2013. Transcript available at http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/896-privacy,-technology-and-national-security-an-overview-of-intelligence-collection.

Lowenthal Mark. *Intelligence: From Secrets to Policy*, *Fifth Edition*. (Los Angeles, CA: CQ Press, 2012)

Majority Staff of the Homeland Security Committee. "Terror Threat Snapshot: September 2015." *Chairman of the Committee on Homeland Security of the House of Representatives*. September 4, 2015. Available at https://homeland.house.gov/wp-content/uploads/2015/09/Complete-September-Terror-Threat-Snapshot.pdf

"Majority Views NSA Phone Tracking as Acceptable Anti-terror Tactic: Public Says Investigate Terrorism, Even if it Intrudes on Privacy." *Pew Research Center*. June 10, 2013. http://www.people-press.org/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/

Markoff, John and Somini Sengupta. "Separating You and Me? 4.74 Degrees." *New York Times*. November 21, 2011. http://nyti.ms/1BC5pRJ

Marquis-Boire, Morgan, Glenn Greenwald, and Micah Lee. "XKEYSCORE: NSA's Google for the World's Private Communications." *The Intercept*. July 1, 2015. https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/

Masnick, Mike. "Latest Leak: NSA Collects Bulk Email Metadata on Americans." *techdirt*. June 27, 2013. https://www.techdirt.com/articles/20130627/09455923637/latest-leak-nsa-collected-bulk-email-metadata-americans.shtml

McLaughlin, Jenna. "Bill that Would Ban End-to-End Encryption Savaged by Critics." *The Intercept*. April 8, 2016. https://theintercept.com/2016/04/08/bill-that-would-ban-end-to-end-encryption-savaged-by-critics/

"Members: 113th Congress (2013-2014)." *U.S. Senate*. Accessed April 26, 2015. http://www.intelligence.senate.gov/members113thcongress.html

Michael Hayden (retired General, United States Air Force, former Director, Central Intelligence Agency and National Security Agency, former Principal Deputy Director of National Intelligence) in discussion with the author, September 21, 2015

----- in discussion with the author, September 28, 2015

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

Michigan Department of State Police, et al v. Sitz, et al, 496 U.S. 444 (1990)

"Moore's Law." *www.mooreslaw.org*. Accessed January 13, 2016. http://www.mooreslaw.org/

Moyer, Thomas J. "State of the Judiciary." Speech before the judges and justices of the Ohio court system, Columbus, OH, September 11, 2008

Nakashima, Ellen. "Chicago Federal Court Case Raises Questions About NSA Surveillance." *Washington Post*. June 21, 2013. https://www.washingtonpost.com/world/national-security/chicago-federal-court-case-raises-questions-about-nsa-surveillance/2013/06/21/7e2dcdc8-daa4-11e2-9df4-895344c13c30_story.html

-----. "Congressional Act on NSA is a Milestone in the Post-9/11 World." *Washington Post*. June 2, 2015. http://www.washingtonpost.com/world/national-security/congressional-action-on-nsa-is-a-milestone-in-the-post-911-world/2015/06/02/f46330a2-0944-11e5-95fd-d580f1c5d44e_story.html

Nelson, Steven. "NSA Whistleblowers Oppose Freedom Act, Endorse Long-Shot Bill." *U.S. News & World Report*. April 27, 2015. http://www.usnews.com/news/articles/2015/04/27/nsa-whistleblowers-oppose-freedom-act-endorse-long-shot-bill

"NSA Ends Bulk Collection of US Phone Records." *Al Jazeera*. November 28, 2015. http://www.aljazeera.com/news/2015/11/nsa-ends-bulk-collection-phone-records-151128172222095.html

"NSA Scrapping Contentious Spy Program." *Reuters*. November 10, 2015. http://www.reuters.com/video/2015/11/10/nsa-scrapping-contentious-phone-spy-prog?videoId=366266601

"NSA Slides Explain the PRISM Data-Collection Program." *Washington Post*. Last updated July 10, 2013. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

"NSA Surveillance: Amash, Conyers Introduce Major Bill." *Office of Congressman Justin Amash*. June 18, 2013. http://amash.house.gov/press-release/nsa-surveillance-amash-conyers-introduce-major-bill

Obama, Barack. "Remarks by the President on Review of Signals Intelligence." Speech at the Department of Justice, Washington, DC, January 14, 2014

-----. "Statement by the President." Speech and press conference, San Jose, CA, June 7, 2013

"On the Passage of the Bill (H.R. 2048)." *United States Senate*. June 2, 2015. http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=114&session=1&vote=00201

Oral Arguments. *James R. Clapper v. Amnesty International USA, et al*. 568 U.S. _____ (2013), No. 11-1025

Perez, Evan. "Secret Court's Oversight Gets Scrutiny." *The Wall Street Journal* (New York, NY), June 9, 2013. http://www.wsj.com/articles/SB10001424127887324904004578535670310514616

Pilkington, Ed. "Declassified NSA Files Show Agency Spied on Muhammad Ali and MLK." *The Guardian*. September 26, 2013. http://www.theguardian.com/world/2013/sep/26/nsa-surveillance-anti-vietnam-muhammad-ali-mlk

"Press Release: Facebook Opens First Data Center in Prineville, Oregon." *Facebook*. April 15, 2011. https://www.facebook.com/notes/prineville-data-center/press-release-facebook-opens-first-data-center-in-prineville-oregon/10150150581753133/

Price, Michael W. "Rethinking Privacy: Fourth Amendment 'Papers' and the Third Party Doctrine." *Georgetown University Law Center's Journal of National Security Law and Policy* 8, no. 2. Available at https://www.brennancenter.org/sites/default/files/analysis/Mike%20Price%20-%20Rethinking%20Privacy.pdf

Privacy and Civil Liberties Oversight Board. "Public Hearing: Consideration of Recommendations for Change: The Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act." Transcript, Washington, D.C., 2013.

"Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act." *Privacy and Civil Liberties Oversight Board*. July 2, 2014. Available at https://www.pclob.gov/library/702-Report.pdf

"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." *Privacy and Civil Liberties Oversight Board*. January 23, 2014. Available at https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf

Risen, James and Eric Lichtblau. "Bush Lets U.S. Spy on Callers Without Courts." *New York Times.* December 16, 2005. http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&_r=2&

Rizzo, John. *Company Man: Thirty Years of Controversy and Crisis in the CIA*. New York, NY: Scribner, 2014.

Rollins, John W. and Edward C. Liu. "NSA Surveillance Leaks: Background and Issues for Congress." *Congressional Research Service*. September 4, 2013

Rubin, Jennifer. "Shedding Light on the PRISM Program." *Washington Post*. June 10, 2013. https://www.washingtonpost.com/blogs/right-turn/wp/2013/06/10/shedding-light-on-the-prism-program/

"S. 758: The National Security Act of 1947 (80th Congress, 1947-1948)." *Oxford University Press*. Last accessed January 27, 2016. http://global.oup.com/us/companion.websites/9780195385168/resources/chapter10/nsa/nsa.pdf

"S. 1566: Foreign Intelligence Surveillance Act of 1978 (95th Congress, 1977-78)," *United States Government Printing Office*, last accessed January 29, 2016, https://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf

Savage, Charlie. "Declassified Report Shows Doubts about Value of N.S.A.'s Warrantless Spying." *New York Times*. April 24, 2015. http://www.nytimes.com/2015/04/25/us/politics/value-of-nsa-warrantless-spying-is-doubted-in-declassified-reports.html

-----. "George W. Bush Made Retroactive N.S.A. 'Fix' After Hospital Room Showdown." *New York Times*. September 20, 2015. http://www.nytimes.com/2015/09/21/us/politics/george-w-bush-made-retroactive-nsa-fix-after-hospital-room-showdown.html?_r=1

Schreckinger, Ben. "New England Confronts Heroin Epidemic." *Al-Jazeera America*. March 16, 2014. http://america.aljazeera.com/articles/2014/3/16/new-england-confrontsheroinepidemic.html

Seife, Charles. "An Open Letter to My Former NSA Colleagues." *Slate*. August 22, 2013. http://www.slate.com/articles/health_and_science/science/2013/08/nsa_domestic_spying_mathematicians_should_speak_out.html

Sensenbrenner, Jim. "Jim's Column: Combating Abuse of Patriot Act." *Office of Congressman Jim Sensenbrenner*. June 13, 2013. http://sensenbrenner.house.gov/news/documentsingle.aspx?DocumentID=339292

Shiffman, John and Kristina Cooke. "Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans." *Reuters*. August 5, 2013. http://www.reuters.com/article/us-dea-sod-idUSBRE97409R20130805

Shinkman, Paul D. "Spy Chief Says Taps Analyzed Only for 'Reasonable Suspicion.'" *U.S. News and World Report*. June 7, 2013. http://www.usnews.com/news/articles/2013/06/07/spy-chief-says-taps-analyzed-only-for-reasonable-suspicion.

Snowden, Edward. *Last Week Tonight with John Oliver*. By John Oliver. HBO, April 5, 2015

Stone, Jeff. "What is 'Metadata?' NSA Loses Surveillance Power on American Phone Calls, but 'Data About Data' Remains Hazy." *International Business Times*. June 2, 2015. http://www.ibtimes.com/what-metadata-nsa-loses-surveillance-power-american-phone-calls-data-about-data-1947196

Strauss, Peter. "Due Process." *Cornell University Law School Legal Information Institute*. Last accessed February 5, 2016. https://www.law.cornell.edu/wex/due_process

Strohm, Chris. "Lawmakers Probe Willful Abuses of Power by NSA Analysts." *Bloomberg*. August 24, 2013. http://www.bloomberg.com/news/articles/2013-08-23/nsa-analysts-intentionally-abused-spying-powers-multiple-times

Strohm, Chris and Roger Runningen. "The NSA's Giant Haystack: Big Data Meets Big Surveillance." *Bloomberg*. Last updated December 4, 2015. http://www.bloombergview.com/quicktake/nsa-data-telephone-surveillance

Swartz, Angela. "What Silicon Valley Tech Firms Think of the USA Freedom Act's Approval." *Silicon Valley Business Journal*. Last updated June 3, 2015. http://www.bizjournals.com/sanjose/news/2015/06/02/what-silicon-valley-tech-firms-think-of-the-usa.html

"Teaching With Documents: Documents and Photographs Related to Japanese Relocation During World War II." *United States National Archives*. Last accessed February 5, 2016. https://www.archives.gov/education/lessons/japanese-relocation/

"The Evolution of the U.S. Intelligence Community—An Historical Overview." *Federation of American Scientists*. February 23, 1996. http://fas.org/irp/offdocs/int022.html

"The Foreign Intelligence Surveillance Court." *Washington Post*. Accessed April 19, 2015. http://www.washingtonpost.com/politics/the-foreign-intelligence-surveillance-court/2013/06/07/4700b382-cfec-11e2-8845-d970ccb04497_graphic.html

Thompson, Dorothy. "What Price Liberty?" *Ladies Home Journal*, May 1958

Thompson, Loren. "Why NSA's PRISM Program Makes Sense." *Forbes*. June 7, 2013. http://www.forbes.com/sites/lorenthompson/2013/06/07/why-nsas-prism-program-makes-sense/#385387b75eb7

"Treaties in Force: A List of Treaties and Other International Agreements of the United States in Force on January 1, 2013." *United States Department of State*. Available at http://www.state.gov/documents/organization/218912.pdf

Tucker, Patrick. *The Naked Future: What Happens in a World That Anticipates Your Every Move?* New York, NY: Penguin Group, 2014

United States v. Amado Martinez-Fuerte, et al, 428 U.S. 543 (1976)

United States v. Johnson, 333 U.S. 10 (1948)

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

United States v. Quartavious Davis, 573 Fed. Appx. 925 (11th Cir. 2014)

Warden, Maryland Penitentiary v. Hayden, 387 U.S. 294 (1967)

Warren, Zach. "Judge Rules NSA Collection 'Almost Certainly' Violates Constitution." *Inside Counsel*. December 17, 2013. http://www.insidecounsel.com/2013/12/17/judge-rules-nsa-collection-almost-certainly-violat.

Whittaker, Zack. "Meet 'Muscular': NSA Accused of Tapping Links Between Yahoo, Google Datacenters." *ZDNet*. October 30, 2013. http://www.zdnet.com/article/meet-muscular-nsa-accused-of-tapping-links-between-yahoo-google-datacenters/

"Wyden, Udall on Revelations that Intelligence Agencies Have Exploited Foreign Intelligence Surveillance Act 'Loophole.'" *Office of Senator Ron Wyden*. April 1, 2014. https://www.wyden.senate.gov/news/press-releases/wyden-udall-on-revelations-that-intelligence-agencies-have-exploited-foreign-intelligence-surveillance-act-loophole

"XKeyscore Presentation From 2008 – Read in Full," *Guardian* (London), Wednesday, July 31, 2013, http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation

"Yahoo! Inc. (YHOO)." *Yahoo! Finance*. Accessed April 26, 2015. http://finance.yahoo.com/q?s=YHOO

APPENDICES

Appendix A

All bolding is added by the author, and is intended to highlight a relevant section. Several irrelevant amendments and sections have been removed.

Amendments to the Constitution of the United States of America

Amendment I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

Amendment IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Amendment V

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land

or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Amendment VI

In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the state and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the assistance of counsel for his defense.

Amendment IX

The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.

Amendment XIV

Section 1. **All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of**

life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

Appendix B

All bolding is added by the author, and is intended to highlight a relevant section. Several irrelevant sections have been removed.

The Constitution of the United States of America

Preamble

We the People of the United States, in Order to form a more perfect Union, establish justice, insure domestic Tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America.

Article I

Section 1. All legislative powers herein granted shall be vested in a Congress of the United States, which shall consist of a Senate and House of Representatives.

Section 3. The Senate of the United States shall be composed of two Senators from each state, chosen by the legislature thereof, for six years; and each Senator shall have one vote.

Section 8. The Congress shall have power to lay and collect taxes, duties, imposts and excises, to pay the debts and **provide for the common defense** and general welfare of the United States; but all duties, imposts and excises shall be uniform throughout the United States;

To declare war, grant letters of marque and reprisal, and make rules concerning captures on land and water;

To raise and support armies, but no appropriation of money to that use shall be for a longer term than two years;

To provide and maintain a navy;

To make rules for the government and regulation of the land and naval forces;

To provide for calling forth the militia to execute the laws of the union, suppress insurrections and repel invasions;

To provide for organizing, arming, and disciplining, the militia, and for governing such part of them as may be employed in the service of the United States, reserving to the states respectively, the appointment of the officers, and the authority of training the militia according to the discipline prescribed by Congress;

To exercise exclusive legislation in all cases whatsoever, over such District (not exceeding ten miles square) as may, by cession of particular states, and the acceptance of Congress, become the seat of the government of the United States, and to exercise like authority over all places purchased by the consent of the legislature of the state in which the same shall be, **for the erection of forts, magazines, arsenals, dockyards, and other needful buildings**;–And

To make all laws which shall be necessary and proper for carrying into execution the foregoing powers, and all other powers vested by this Constitution in the government of the United States, or in any department or officer thereof.

Section 10. No state shall enter into any treaty, alliance, or confederation; grant letters of marque and reprisal; coin money; emit bills of credit; make anything but gold and silver coin a tender in payment of debts; pass any bill of attainder, ex post facto law, or law impairing the obligation of contracts, or grant any title of nobility.

Article II

Section 2. **The President shall be commander in chief of the Army and Navy of the United States, and of the militia of the several states, when called into the actual service of the United States**; he may require the opinion, in writing, of the principal officer in each of the executive departments, upon any subject relating to the duties of their respective offices, and he shall have power to grant reprieves and pardons for offenses against the United States, except in cases of impeachment.

He shall have power, by and with the advice and consent of the Senate, to make treaties, provided two thirds of the Senators present concur; and he **shall nominate, and by and with the advice and consent of the Senate**, shall appoint ambassadors, other public ministers and consuls**, judges of the Supreme Court**, and all other officers of the United States, whose appointments are not herein otherwise provided for, and which shall be established by law: but the Congress may by law vest the appointment of such inferior officers, as they think proper, in the President alone, in the courts of law, or in the heads of departments.

Article III

Section 1. The judicial power of the United States, shall be vested in one Supreme Court, and in such inferior courts as the Congress may from time to time ordain and establish. The judges, both of the supreme and inferior courts, shall hold their offices during good behaviour, and shall, at stated times, receive for their services, a compensation, which shall not be diminished during their continuance in office.

Section 2. **The judicial power shall extend to all cases, in law and equity, arising under this Constitution**, the laws of the United States, and treaties made, or which shall be made, under their authority;–to all cases affecting ambassadors, other public ministers and consuls;–to all cases of admiralty and maritime jurisdiction;–**to controversies to which the United States shall be a party**;–to controversies between two or more states;–between a state and citizens of another state;– between citizens of different states;–between citizens of the same state claiming lands under grants of different states, and between a state, or the citizens thereof, and foreign states, citizens or subjects.
In all cases affecting ambassadors, other public ministers and consuls, and those in which a state shall be party, the Supreme Court shall have original jurisdiction. In all the other cases before mentioned, the Supreme Court shall have appellate jurisdiction, both as to law and fact, with such exceptions, and under such regulations as the Congress shall make.

Article IV

Section 4. The United States shall guarantee to every state in this union a republican form of government, and **shall protect each of them against invasion**; and on application of the legislature, or of the executive (when the legislature cannot be convened) **against domestic violence.**

Article VI

This Constitution, and the laws of the United States which shall be made in pursuance thereof; and all treaties made, or which shall be made, under the

authority of the United States, shall be the supreme law of the land; and the judges in every state shall be bound thereby, anything in the Constitution or laws of any State to the contrary notwithstanding.

Appendix C

All bolding is added by the author, and is intended to highlight a relevant section. Several irrelevant sections have been removed.

Executive Order 12333--United States intelligence activities

Timely and accurate information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons and their agents, is essential to the national security of the United States. All reasonable and lawful means must be used to ensure that the United States will receive the best intelligence available. For that purpose, by virtue of the authority vested in me by the Constitution and statutes of the United States of America, including the National Security Act of 1947, as amended, and as President of the United States of America, in order to provide for the effective conduct of United States intelligence activities and the **protection of constitutional rights**, it is hereby ordered as follows:

Part 1

Goals, Direction, Duties and Responsibilities With Respect to the National Intelligence Effort

1.1*Goals.* The United States intelligence effort shall provide the President and the National Security Council with the necessary information on which to base decisions concerning the conduct and development of foreign, defense and economic policy, and the protection of United States national interests from foreign security threats. All departments and agencies shall cooperate fully to fulfill this goal.
(a) Maximum emphasis should be given to fostering analytical competition among appropriate elements of the Intelligence Community.
(b) All means, **consistent with applicable United States law and this Order, and with full consideration of the rights of United States persons**, shall be used to develop intelligence information for the President and the National Security Council. A balanced approach between technical collection efforts and other means should be maintained and encouraged.
(d) To the greatest extent possible consistent with applicable United States law and this Order, and **with full consideration of the rights of United States persons**, all agencies and departments should seek to ensure full and free exchange of information in order to derive maximum benefit from the United States intelligence effort.

1.7*Senior Officials of the Intelligence Community.* The heads of departments and agencies with organizations in the Intelligence Community or the heads of such organizations, as appropriate, shall:
(a) Report to the Attorney General possible violations of federal criminal laws by employees and of specified federal criminal laws by any other person as provided in

procedures agreed upon by the Attorney General and the head of the department or agency concerned, in a manner consistent with the protection of intelligence sources and methods, as specified in those procedures;
(d) Report to the Intelligence Oversight Board, and keep the Director of Central Intelligence appropriately informed, concerning any intelligence activities of their organizations that they have reason to believe may be unlawful or contrary to Executive order or Presidential directive;
(i) **Ensure that the Inspectors General and General Counsels for their organizations have access to any information necessary to perform their duties assigned by this Order.**

1.12*Intelligence Components Utilized by the Secretary of Defense.* In carrying out the responsibilities assigned in section 1.11, the Secretary of Defense is authorized to utilize the following:
(a) *Defense Intelligence Agency,* whose responsibilities shall include;
(1) Collection, production, or, through tasking and coordination, provision of military and military-related intelligence for the Secretary of Defense, the Joint Chiefs of Staff, other Defense components, and, as appropriate, non-Defense agencies;
(2) Collection and provision of military intelligence for national foreign intelligence and counterintelligence products;
(3) Coordination of all Department of Defense intelligence collection requirements;
(4) Management of the Defense Attache system; and
(5) Provision of foreign intelligence and counterintelligence staff support as directed by the Joint Chiefs of Staff.
(b) ***National Security Agency,*** whose responsibilities shall include:
(1) Establishment and operation of an effective unified organization for signals intelligence activities, except for the delegation of operational control over certain operations that are conducted through other elements of the Intelligence Community. No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense;
(2) Control of signals intelligence collection and processing activities, including assignment of resources to an appropriate agent for such periods and tasks as required for the direct support of military commanders;
(3) Collection of signals intelligence information for national foreign intelligence purposes in accordance with guidance from the Director of Central Intelligence;
(4) Processing of signals intelligence data for national foreign intelligence purposes in accordance with guidance from the Director of Central Intelligence;
(5) Dissemination of signals intelligence information for national foreign intelligence purposes to authorized elements of the Government, including the military services, in accordance with guidance from the Director of Central Intelligence;
(6) Collection, processing and dissemination of signals intelligence information for counterintelligence purposes;

(7) Provision of signals intelligence support for the conduct of military operations in accordance with tasking, priorities, and standards of timeliness assigned by the Secretary of Defense. If provision of such support requires use of national collection systems, these systems will be tasked within existing guidance from the Director of Central Intelligence;
(8) Executing the responsibilities of the Secretary of Defense as executive agent for the communications security of the United States Government;
(9) Conduct of research and development to meet the needs of the United States for signals intelligence and communications security;
(10) Protection of the security of its installations, activities, property, information, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the NSA as are necessary;
(11) Prescribing, within its field of authorized operations, security regulations covering operating practices, including the transmission, handling and distribution of signals intelligence and communications security material within and among the elements under control of the Director of the NSA, and exercising the necessary supervisory control to ensure compliance with the regulations;
(12) Conduct of foreign cryptologic liaison relationships, with liaison for intelligence purposes conducted in accordance with policies formulated by the Director of Central Intelligence; and
(13) Conduct of such administrative and technical support activities within and outside the United States as are necessary to perform the functions described in sections (1) through (12) above, including procurement.

1.14*The Federal Bureau of Investigation.* Under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the Director of the FBI shall:
(a) **Within the United States** conduct counterintelligence and coordinate counterintelligence activities of other agencies within the Intelligence Community. When a counterintelligence activity of the FBI involves military or civilian personnel of the Department of Defense, the FBI shall coordinate with the Department of Defense;
(b) Conduct counterintelligence activities outside the United States in coordination with the CIA as required by procedures agreed upon by the Director of Central Intelligence and the Attorney General;
(c) Conduct within the United States, when requested by officials of the Intelligence Community designated by the President, activities undertaken to collect foreign intelligence or support foreign intelligence collection requirements of other agencies within the Intelligence Community, or, when requested by the Director of the National Security Agency, to support the communications security activities of the United States Government;

Part 2

Conduct of Intelligence Activities

2.1*Need.* Accurate and timely information about the capabilities, intentions and activities of foreign powers, organizations, or persons and their agents is essential to informed decision-making in the areas of national defense and foreign relations. Collection of such information is a priority objective and **will be pursued in a vigorous, innovative and responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded.**

2.3*Collection of Information.* Agencies within the Intelligence Community are authorized to collect, retain or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order. Those procedures shall permit collection, retention and dissemination of the following types of information:
(a) Information that is publicly available or collected with the consent of the person concerned;
(b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. **Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the FBI or, when significant foreign intelligence is sought, by other authorized agencies of the Intelligence Community, provided that no foreign intelligence collection by such agencies may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;**
(h) Information acquired by overhead reconnaissance not directed at specific United States persons;
(i) Incidentally obtained information that may indicate involvement in activities that may violate federal, state, local or foreign laws; and

2.4*Collection Techniques.* **Agencies within the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Agencies are not authorized to use such techniques as electronic surveillance, unconsented physical search, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the agency concerned and approved by the Attorney General. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes.** These procedures shall not authorize:
(a) The CIA to engage in electronic surveillance within the United States except for the purpose of training, testing, or conducting countermeasures to hostile electronic surveillance;
(b) Unconsented physical searches in the United States by agencies other than the FBI, except for:

> (1) Searches by counterintelligence elements of the military services directed against military personnel within the United States or abroad for intelligence purposes, when authorized by a military commander empowered to approve physical searches for law enforcement purposes, based upon a finding of probable cause to believe that such persons are acting as agents of foreign powers; and

(2) Searches by CIA of personal property of non-United States persons lawfully in its possession.

(c) Physical surveillance of a United States person in the United States by agencies other than the FBI, except for:

(1) Physical surveillance of present or former employees, present or former intelligence agency contractors or their present of former employees, or applicants for any such employment or contracting; and

(2) Physical surveillance of a military person employed by a nonintelligence element of a military service.

(d) Physical surveillance of a United States person abroad to collect foreign intelligence, except to obtain significant information that cannot reasonably be acquired by other means.

2.5*Attorney General Approval.* **The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power.** Electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be conducted in accordance with that Act, as well as this Order.

2.8*Consistency With Other Laws.* Nothing in this Order shall be construed to authorize any activity in violation of the Constitution or statutes of the United States.

2.12*Indirect Participation.* No agency of the Intelligence Community shall participate in or request any person to undertake activities forbidden by this Order.

Part 3

General Provisions

3.4*Definitions.* For the purposes of this Order, the following terms shall have these meanings:

(a) *Counterintelligence* means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs.

(b) *Electronic surveillance* means acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication, but not

including the use of radio direction-finding equipment solely to determine the location of a transmitter.

(d) *Foreign intelligence* means information relating to the capabilities, intentions and activities of foreign powers, organizations or persons, but not including counterintelligence except for information on international terrorist activities.

(7) The staff elements of the Director of Central Intelligence.

(i) *United States person* means a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

3.5*Purpose and Effect.* This Order is intended to control and provide direction and guidance to the Intelligence Community. **Nothing contained herein or in any procedures promulgated hereunder is intended to confer any substantive or procedural right or privilege on any person or organization.**