National Security Agency Domestic and Corporate Surveillance: To What Extent Has the National Security Agency Violated Civil and Business Liberties While Protecting National Security?

By

Jessica Lindsay Kelso

A thesis submitted in partial fulfillment of the requirements for the degree of Bachelor of Science in Finance and Graduation with Honors College and Business Honors Program Distinction
Muma College of Business
University of South Florida

Thesis Chair: Dr. Charles Michaels, PhD.
Committee: Dr. Doreen MacAulay, PhD.

Word Count: 3564

Keywords: NSA Domestic Surveillance, Privacy, National Security, Fourth Amendment

Table of Contents

Abstract

Preserving individual freedoms and constitutional guarantees of liberty and privacy should trump national security concerns and should be the focal point of the National Security Agency's (NSA) mission. The purpose of this study is to examine the expanding role of the NSA's domestic surveillance apparatus since September 11th, 2001 and more importantly, the balance between civil liberties and national security in the United States. This study gained insights into the assortment of clandestine NSA information gathering techniques imposed on U.S. citizens, the role of U.S. companies in bulk NSA domestic surveillance activities, and a review of the associated impact on Fourth Amendment rights under the U.S. Constitution. This study's findings suggest that the NSA has veered from its original mission of collecting foreign intelligence to essentially spying on American citizens and corporations, and propose that additional congressional oversight and greater transparency of the Agency is warranted to ensure that every citizen's Fourth Amendment rights are preserved and American businesses are not tainted by surveillance efforts.

Introduction

The National Security Agency (NSA) was established over 60 years ago with the primary mission to monitor, collect, and process foreign intelligence and protect the United States against espionage. It originated to decipher coded communications during World War II, but morphed into today's clandestine electronic information gathering behemoth. It accomplishes its mission through a myriad of methods, including syphoning metadata from telephone records, monitoring individuals through internet company servers, tracking credit card purchases, and intercepting cellular messages and location data. Present-day NSA operations include an estimated 40,000 employees and a projected annual budget of $12 billion.

Preserving individual freedoms and constitutional guarantees of liberty and privacy should trump national security concerns and should be the focal point of the NSA's mission. An investigation into the numerous data collection methods, along with a description of the tools and methods employed by the NSA to surveil United States citizens will be reviewed. The proverbial tightrope of balancing security and privacy, in relation to domestic surveillance, will be examined. More importantly, arguments in favor and against the use of domestic NSA surveillance techniques will be discussed. These arguments will inform the conclusion that will address both the ethical and constitutional questions that arise from domestic surveillance.

Domestic Surveillance Techniques

With the evolution of devices from analog to digital, the NSA has changed its surveillance tactics to focus on the internet and telecommunications companies (Fisher). These companies have become subject to secret court orders forcing them to comply with back doors into their software, providing encryption keys, and generally making their customers' communications available to the government. Some of the key NSA software that captures this information has code names such as PRISM, XKeyscore, and BLARNEY.

One of the primary surveillance techniques used by the NSA to gather raw intelligence is a program called PRISM. PRISM, a program that began in 2007, is a code name for a data collection effort involving nine internet companies including Google, Facebook, Microsoft, and Apple (Greenwald and MacAskill). The items collected vary from email and videos to photos and online chats. The existence of this program was leaked to the public in 2013 by ex-NSA contractor Edward Snowden. He said, "I can't in good conscience allow the U.S. government to destroy privacy, internet freedom and basic liberties for people around the world with this massive surveillance machine they're secretly building" (Greenwald, "No Place to Hide"). Snowden contended that the mass data collection on American citizens was far greater than anyone had previously imagined, going as far as to classify the activities of the NSA as criminal and dangerous. Leaked documents indicate that PRISM is "the number one source of raw intelligence used for NSA analytic reports" (Gellman, Barton, and Poitras).

The PRISM program utilizes extensive data mining efforts to collect

information and analyze that data for patterns of terrorist or other potential criminal activity. “...Snowden brought into the public eye a veritable bevy of controversial U.S. surveillance enterprises, including the PRISM program under section 702, and the bulk telephone metadata program under section 215 of the USA Patriot Act. Here, in the flesh, was clear and incontrovertible evidence not just of the extent to which the government was already knee-deep into the collection of data but also of the controversial nature of such a haystack-before-the-needle approach to information gathering” (Vladeck). Recently, congress has passed the USA Freedom Act which replaces section 215 of the Patriot Act. The title of the act originally was a ten-letter backronym, a specially constructed phrase that is supposed to be the source of a word that is an acronym. In this case, it stood for “Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act” It eliminates the controversial bulk collection of the phone data of millions of Americans who have no ties to terrorism. Now, phone companies will retain the data, and the NSA can obtain information on targeted individuals with the permission of a federal court. President Obama at the time stated, “...the administration will announce new rules requiring intelligence analysts to delete private information they may incidentally collect about Americans that has no intelligence purpose, and to delete similar information about foreigners within five years” (Ball and Spencer).

A powerful weapon of mass surveillance in the NSA’s arsenal is XKeyscore. It is essentially the NSA’s “Google for all the world’s private

communications" (Marquis-Boire et al.). It makes tracking an individual's complete internet usage as easy as entering an email address into the system. XKeyscore taps into the backbone of all internet traffic and stores emails, documents, usernames, and passwords for three to five days. Newly uncovered NSA documents have revealed that tens of billions of records are stored in this program's database. XKeyscore is capable of surveilling people based on patterns of questionable behavior. For example, it is possible to discern the online activities of people based on their location, nationality, and websites visited (Lehr).

BLARNEY is another top-secret surveillance program operating around the world. It is the international version of the PRISM program. BLARNEY "gathers up metadata- technical information about communications, traffic, and network devices- as it streams past choke points along the backbone of the internet." Metadata focuses on when and where the communications were sent, not on the contents (Gellman, Barton, and Poitras).

A vast sea of data is collected by the NSA each month. For example, one month in 2013, the NSA collected almost 100 billion "pieces" of intelligence worldwide. During that same period, three billion pieces of intelligence were collected in the United States. A "piece" of intelligence would be an email or a phone call.

These three programs constitute only a small fraction of all the clandestine surveillance methods available to the NSA. The NSA records as much information as it can, limited only by the technical demands of collecting, storing,

and analyzing vast quantities of information. As mentioned, this includes nearly all the metadata for nearly all the telephone calls made in the United States, and massive amounts of Internet traffic processed at a network of over 150 data centers around the world. They collect information on “nearly everything a user does on the internet” (Marquis-Borie, Greenwald, and Lee).

Balancing Security and Privacy

Proponents of enhanced NSA surveillance point to the increase in security it provides to American citizens. The intelligence collected provides detailed information on the activities of potential terrorists and threats to US interests. These measures provide enhanced security and wellbeing to the nation. However, “six-in-ten Americans (61%) oppose the government monitoring communications of U.S. citizens… those Americans don’t see a need to sacrifice civil liberties to be safe from terrorism” (Gao).

A recent Pew Research center poll found that “a majority of Americans (54%) disapprove of the U.S. government’s collection of telephone and internet data as part of anti-terrorism efforts, while 42% approve of the program.” In this groundbreaking survey, “74% said they should not give up privacy and freedom for the sake of safety, while just 22% said the opposite” (Gao). In other words, most American citizens do not wish to be spied on in exchange for increased safety. Benjamin Franklin, one of the founding fathers of the United States, commented that “those who would give up essential liberty, to purchase a little temporary safety, deserve neither liberty nor safety” (Wittes). Franklin said this in

1755, and it still holds true today. Based on this survey, most Americans would likely agree with this quote.

Many U.S. companies are complicit in supporting the NSA's domestic surveillance efforts, including several companies that provide the backbone to U.S. communications systems such as AT&T, Verizon, and Global Crossing. Many of these companies facilitate tapping into undersea or land-based communications cables or providing consulting and enabling technologies that support the NSA's clandestine operations to trace or intercept American citizen's communications.

"Americans understand that we need to give due weight to both privacy and national security. But right now, Americans aren't getting even the most basic information about what's going on with the NSA's surveillance programs, and whether their privacy is being violated," Sen. Al Franken told State of the Union (Gao). "...Given the apparent scope of the NSA program, the number of violations of the human right to privacy could easily climb into the millions, billions, or even trillions. The extensive and systematic nature of the program could thus compel the conclusion that the United States is violating the human right to privacy within its borders on a truly colossal scale" (Sinha).

A meaningful balance between privacy and security in the information age is necessary. "The government can, indeed, listen to, copy, file, regenerate, archive, transcribe, and publicize just about any so-called secret communication it wants. There are legitimate reasons to compile information on who might be calling whom and with what frequency. Yet it is also important to remember that

just because the government can do something – which is often enough an excuse for them to do it – does not mean the government should do something" (Roff). This indicates that the balance is off kilter, with the government erring on the side of increased security at the cost of personal freedoms.

According to Keith Alexander, former director of the NSA, the efforts of the NSA have thwarted 54 terrorist attacks worldwide: 25 in Europe, 13 in the United States of America, 11 in Asia, and 5 in Africa (Elliott and Meyer). The NSA, President Obama, and members of congress claim these numbers are accurate; however, there is no substantial evidentiary support to validate this claim.

A discussion of individual privacy and liberties would not be complete without acknowledging the constitutional protections afforded by the Fourth Amendment to the United States Constitution. It's the principle constitutional protection against government spying. The first ten amendments of the U.S. Constitution were ratified in 1791, and are known collectively as The Bill of Rights. It Fourth Amendment reads:

> *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. (U.S. Constitution)*

In the current vernacular, it prohibits unreasonable searches and seizures and sets out requirements for search warrants based on probable cause as determined by a neutral judge or magistrate. These protections were eroded by provisions in the Patriot Act following the 9/11 terrorist attacks on the World Trade Center and the Pentagon, and the attempted attack on the White House. Specifically, Section 215 authorizing the NSA's mass phone data collection program which allowed targeted searches of individual Americans telephone data without the permission of the federal courts. This controversial domestic surveillance program on all American citizens was superficially amended in mid-2015 to the USA Freedom Act, which directs telecommunications companies to provide individual, targeted data directly to the NSA with the federal court's permission, potentially eroding these privacy protections provided by the Fourth Amendment. In its quest to secure the American populous, the NSA has garnered both support and opposition to its data collection methods.

Arguments Supporting and Rejecting NSA Domestic Surveillance

The National Security Agency's domestic surveillance apparatus has both defenders and detractors. The defenders acknowledge the role the NSA plays in safeguarding Americans from another September 11th-like terrorist attack, and justify the additional data gathering powers granted this Agency by pointing to the terrorist attacks that were intercepted and thwarted as a result of spying on millions of American citizens. According to General Keith B. Alexander, former NSA Director under Presidents Bush and Obama, "…the number of terrorist plots foiled by the NSA's huge database of every phone call made in or to America

was only one or perhaps two - far smaller than the fifty-four originally claimed by the administration" (Waterman). Alexander left his position at the NSA after revelations of the extent of the NSA spying, and the effectiveness of those efforts, were revealed during congressional hearings.

The detractors, however, posit that the surveillance authority given to the NSA has not made Americans any safer from terrorist attacks because the probability of an attack is so low. NSA leaker Edward Snowden stated that, "bathtub falls and police officers kill more Americans than terrorism, yet we've been asked to sacrifice our most sacred rights for fear of falling victim to it" (Greenwald, "Edward Snowden"). Statistically, a U.S. citizen is 55 times more likely to be killed by a police officer than a terrorist... and a citizen stands a better chance of dying from brain eating parasites, texting while driving, and falling out of bed than a terrorist attack on American soil (McCarthy). Daniel Benjamin, former Coordinator for Counterterrorism at the United States Department of State, stated that, "The total number of deaths from terrorism in recent years has been extremely small in the West. And the threat itself has been considerably reduced. Given all the headlines, people don't have that perception; but if you look at the statistics, that is the case."

Arguments in Favor of NSA Surveillance

The NSA has the capability to surveil both foreign and domestic threats posed by armies and navies around the world, however many of today's threats originate with a small number of "bad actors" around the world. According to the NSA, its ability to interrogate suspected terrorists has been severely curtailed,

and it's incredibly hard to penetrate the operations of these small terrorist groups with spies or double agents. That leaves "signals intelligence," or monitoring terrorists Internet usage and phone calls, as the last resort to prevent attacks on the United States. The NSA monitors communications to potentially save lives and thwart terrorist activities. The NSA admits that, in their quest to curtail the possibility of future terrorist attacks, U.S. citizens communications are inadvertently collected resulting in their privacy being disregarded.

Total individual privacy is achievable; total national security is achievable; however, the two cannot exist conterminously. National security can be surrendered in exchange for individual rights and privacy, and vice versa. The true enemy is not the disconcerting amount of government involvement in the personal information of American citizens; it is the terrorist threats against America. General Keith Alexander maintained that "a terrorist attack is even worse for a country's basic freedoms [than NSA surveillance]." Many Americans are concerned about their government becoming too entangled in their private lives by surveilling personal phone calls, emails, etc., but few seem to realize just how harmful these surveillance programs are to innocent Americans. The NSA's primary objective of espionage is to stop foreign or domestic terrorists from causing destruction on the soil of America and that of its allies. Therefore, the proponents of the NSA contest that the agency is not actually paying any attention to the matters of honest American citizens it is surveilling; instead, it is targeting the suspicious keywords and phrases used by potential terrorists in the hopes of foiling their plots of destruction.

In a recent national survey by the Pew Research Center and the Washington Post conducted in June 2013, “most Americans (56%) say the NSA’s program of tracking the telephone records of millions of Americans is an acceptable way for the government to investigate terrorism. Additionally, 62% say it’s important for the federal government to investigate possible threats, even if that intrudes on personal privacy.” These poll results show strong support for government surveillance of Americans’ telephone records; however, only 45% say the government should be able to monitor everyone’s email and other online activities if officials say this might prevent future terrorist attacks (“Majority Views NSA Phone Tracking”). Therefore, NSA supporters believe that the surveillance of American citizens is justified if national security is guaranteed.

Arguments Against NSA Surveillance

The NSA collects massive amounts of unwarranted information on the vast majority of internet-using Americans in order to broadly sweep over the information and look for any suspicious material. Although the NSA’s intentions are generally regarded as benevolent by the public at large, the specific programs of espionage used on Americans are often regarded as an infringement on individual rights.

According to a 2014 Pew Research Center survey, a majority of Americans (54%) disapprove of the U.S. government’s collection of telephone and internet data as part of anti-terrorism efforts, with 74% indicating that they should not give up privacy and freedom for the sake of safety. Further, according to the survey, only 9% of Americans say they have a lot of control over how

much information is collected about them, with only 6% of respondents indicating that they are confident that the government agencies can keep their records private and secure, and 25% changing the way they use the Internet since the Snowden allegations of NSA spying on American citizens.

There is also the question of how much power should be given to the government, and more specifically, to the secret courts that oversee the NSA. The Foreign Intelligence Surveillance Court (FISC), which was established in 1978 by Congress, monitors and approves the actions of the NSA. This secret Court "entertains applications made by the United States Government for approval of electronic surveillance, physical search, and certain other forms of investigative actions for foreign intelligence purposes" ("EPIC"). Out of the nearly 36,000 requests submitted for warrants over 35 years, FISC only denied 12 requests (EPIC - FISA Court Orders). Clearly, FISC is not reluctant to cooperate with the efforts of the NSA. This harkens to the predications of the dystopian society described by George Orwell in his perennial classic entitled *1984*.

The New America Foundation, a nonprofit think tank, investigated the 227 Al Qaeda-affiliated supporters that have been charged with committing an act of terrorism in the United States since September 11, 2001. It found "just 17 of the cases were credited to NSA surveillance, and just one conviction came out of the government's practice of spying on its own citizens." That one charge was "against a San Diego cab driver for sending money to a terrorist group in Somalia. There was no threat of an actual attack." Accordingly, the NSA's

massively intrusive surveillance activities have provided a mere pittance of definitive evidence that might be used to prevent domestic terrorism.

Conclusion

The National Security Agency has a long history of protecting the United States against foreign and domestic terrorists. It accomplishes its mission by using a variety of data collection methods. The intelligence methods employed force a tradeoff between securing the citizens of the Unites States and maintaining individual privacy. At the heart of this issue is personal liberty.

The process by which the NSA completes its tasks is not transparent. In other words, prior to the disclosures by NSA-leaker Edward Snowden, Americans were unaware of the extent of spying on their telephone calls, emails, and messages. In exchange for citizens' diminished liberties, the NSA claims to have thwarted multiple terrorist attacks against Americans. There is no evidence to support this claim.

The Fourth Amendment provides constitutional protections for each Americans' privacy and liberty. The lack of transparency with NSA surveillance programs, and a secret court that rubber-stamps most NSA search requests, has led to the apparent degradation in these protections.

Domestic surveillance by the NSA has both defenders and detractors. The defenders point to heightened national security and terrorist attacks that were avoided as a result of their efforts. Detractors, on the other hand, suggest that Americans are not any safer from terrorist attacks despite the additional

surveillance authority granted to the NSA. Those that defend the NSA's surveillance techniques are willing to sacrifice individual basic freedoms for national security; however, those that object to domestic surveillance techniques, the majority of Americans, wish to keep those their constitutionally guaranteed freedoms intact.

The overarching verdict, based on the arguments presented, would point to preserving individual freedoms and constitutional guarantees of liberty and privacy over national security concerns for American citizens. Based on the NSA leaks, it is apparent that, despite surveilling millions of American citizens, very few terrorist attacks have been prevented. Although it is important to maintain a careful balance between privacy and security, the National Security Agency has veered from its initial mission of collecting foreign intelligence to spying on Americans. The NSA is ripe for additional congressional oversight and greater transparency, resulting in the resumption of the privacies guaranteed to every American by the Fourth Amendment.

Bibliography

Ball, James and Spencer, Ackerman. “NSA Loophole Allows Warrantless Search for U.S. Citizens’ Email and Phone Calls.” The Guardian, 2013.

Cahall, Bailey, David Sterman, Emily Schneider, and Peter Bergen. "Do NSA's Bulk Surveillance Programs Stop Terrorists?" New America RSS. New America, 13 Jan. 2013.

Elliott, Justin, and Theodoric Meyer. "Claim on “Attacks Thwarted” by NSA Spreads Despite Lack of Evidence." Top Stories RSS. N.p., 23 Oct. 2013.

"EPIC - Foreign Intelligence Surveillance Act Court Orders 1979-2014." FISA Court Orders 1979-2014. Electronic Privacy Information Center, 2015.

Fisher, Benjamin B. “Ticker, Tailor, Soldier, Snowden.” International Journal of Intelligence and Counterintelligence, 32 (1), 178-191, 2019.

Fitzpatrick, Collins T. "Protecting the Fourth Amendment So We Do Not Sacrifice Freedom for Security." Wis. L. Rev. (2015): 1.

Franklin, Benjamin. Pennsylvania Assembly: Reply to the Governor, November 11, 1755.—The Papers of Benjamin Franklin, ed. Leonard W. Labaree, vol. 6, p. 242 (1963).

Gao, George. "What Americans Think about NSA Surveillance, National Security and Privacy." Pew Research Center RSS. N.p., 29 May 2015.

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

Greenwald, Glenn, and Ewen MacAskill. "NSA Prism Program Taps in to User Data of Apple, Google and Others." The Guardian. N.p., 7 June 2013.

Greenwald, Glenn. "Edward Snowden: NSA Whistleblower Answers Readers’ Questions." The Guardian, 3 Oct. 2014.

Greenwald, Glenn. No place to hide: Edward Snowden, the NSA, and the US surveillance state. Macmillan, 2014.International, Amnesty. "Big Data Before and After Snowden." (2014).

Jordan, Sara R. "Beneficence and the Expert Bureaucracy: Ethics for the Future of Big Data Governance." Public Integrity 16.4 (2014): 375-394.

Kalanges, Shaina. "Modern Private Data Collection and National Security Agency

Surveillance: A Comprehensive Package of Solutions Addressing Domestic Surveillance Concerns." N. Ill. UL Rev. 34 (2013): 643.

Lehr, Peter. “Prediction and Postdiction: Real-Time Data Mining and Data Analytics.” Counter-Terrorism Technologies. Springer, Cham, 2019, 81-99.

"Majority Views NSA Phone Tracking as Acceptable Anti-terror Tactic." Pew Research Center for the People and the Press RSS. Pew Research Center, 10 June 2013.

Marchetti, Victor, John D. Marks, and Melvin L. Wulf. The CIA and the Cult of Intelligence. New York: Knopf, 1974.

Marquis-Boire, Morgan, Glenn Greenwald, and Micah Lee. "XKEYSCORE: NSA's Google for the World's Private Communications." The Intercept. N.p., 1 July 2015.

McCarthy, Tom. "Police Killed More than Twice as Many People as Reported by US Government." The Guardian, 4 Mar. 2015.

Roff, Peter. "A Better Way to Balance Privacy and Security." U.S. News and World Report, 27 Aug. 2013.

Sinha, G. Alex. "NSA Surveillance since 9/11 and the Human Right to Privacy." (2013).

U.S. Constitution. Art./Amend. IV.

"US Partners Ready Resources to Fight Common Threat." MSNBC The Cycle http://www.msnbc.com/the-cycle/watch/arrests-across-europe-in-anti-terror-raids-385428547996

Vladeck, S.I. “Big Data Before and After Snowden.” Journal of National Security, Law, and Policy, 7, 333, 2019.

Wittes, Benjamin. "Would Ben Franklin Trade Liberty for Wiretapping?" The Brookings Institution. N.p., 12 June 2013.

Waterman, Shaun. "NSA Chief’s Admission of Misleading Numbers Adds to Obama Administration Blunders." Washington Times. The Washington Times, 2 Oct. 2013.

http://www.fisc.uscourts.gov/