# Privacy and Government Surveillance



David W Mitchell

ICTN 6823 601

July 21, 2016

## Abstract

Federal government's broad powers to act for public safety and national security are limited by the First Amendment and Fourth Amendment. The 9/11 attack have open the doors on warrantless surveillance programs. The mass collection of sensitive information has been challenged by many as an invasion of privacy. Snowden's release of sensitive information has brought to light the true challenges between government surveillance and privacy. There is a true need to balance government surveillance and privacy in order to protect America. Lawmakers are starting to recognize this with the introduction of new laws to tackle and balance privacy with government surveillance. These improved laws must be introduced on a national level.

The National Security Agency NSA was directive in 1952 by President Truman. President Truman believed that communication intelligence function was a national responsibility rather than just the responsibility of the military (Burns, 1990). Secretary Lovett had the basic responsibility for starting the agency. The roles of the NSA include operational and technical control over all military communication intelligence collection. The NSA today have a broader scope of responsibilities including global monitoring, collection, and processing of information and data for foreign intelligence and counterintelligence purposes. NSA is charge with protection of U.S. government communications and information systems against penetration and network warfare (Simpson, 2016). Most of the NSA's program rely on passive electronic collection including bugging electronic systems and engaging in sabotage through subversive software (Burns, 1990). NSA also provide special collection service in a number of countries including eavesdropping device, close surveillance, and breaking & entering.

The Guardian newspaper reported the release of classified information obtained by Edward Snowden on several US spying programs (Edward Snowden: Leaks that exposed US spy programme, 2014). The release of this information by Snowden proves that the NSA conducts government surveillance of American citizens. The NSA program called Prism allowed the NSA to receive emails, video clips, photos, voice and video calls, social networking details, logins and other data held by US Internet firms (Kelion, 2013). Snowden's release of information named companies such as Microsoft, Google, Facebook, Apple and Yahoo as participation in this program. This program call about following the 9/11 attacks when President Bush administration gave NSA permission to bypass the courts for warrantless surveillance (Kelion, 2013). Congress voted in 2005 to

offer immunity to firms that co-operated with the NSA requests. The NSA was supposed minimize the risk of inadvertently examining data bout US citizens and residents (Kelion, 2013).

The beginning of surveillance before the Prism program required government agencies to get court orders asking Internet companies to hand over data. The courts were the ones who protected U.S. citizens from having their data illegally obtain by the government. Prism circumvented the process of going through the court system. Prism allowed mass amounts of data to be obtained without a warrant from the courts. The massive amount of data release to the NSA didn't allow the data on terrorist to be separated from data on American citizens. Prism took large amounts of data and helped the government find discrete, manageable strands of information (Braun, Flaherty, Gillum, & Apuzzo, 2013). In Prism, the government identifies who it wanted to monitor and sent a selector to the service provider. The selector information was then obtained by a government directive from the service provider.

Wiretapping is another program that has been given increase powers by the Patriot Act. Wiretapping has been around with the NSA and federal law enforcement agencies since the 1970s. The current wiretapping policy lacks guidelines addressing modern terrorist threat even though it had a significant effect for personal security (Mullikin & Rahman, 2010). The Supreme Court had sanctioned warrantless wiretapping in the case United States v. United States District Court in 1972. Originally, wiretapping was implemented to avoid the red tape of bureaucracy (Mullikin & Rahman, 2010). President Bush administration was able to block an investigation by the Justice Department on the NSA wiretapping program. It was determine that it was more important to protect the program

than to compromise security. The Bush wiretapping program ended in 207 after public pressure. However, the FISA Amendment Act of 2008 expanded wiretapping and granted immunity to telephone companies (Niarchos, 2014).

Another surveillance program of the NSA was called Upstream. The Upstream program allowed the NSA to collect communication on fiber cables and infrastructure as data pass through undersea fiber-optic cables. The program Upstream allowed the NSA to conduct pattern analysis on a huge trove of metadata. The interception of the domestic cables carried about 80 percent of the world's telecommunication (Kaufman, 2013). This invasion of privacy was a warrantless acquisition of metadata and contents concerning American communications (Kaufman, 2013). A copy of every electronic and text communication that passed through the fiber-optic networks allowed the NSA to search inside every message. Nearly 99 percent of the world's communication travel over the undersea fiber-optic cables. Upstream surveillance is considered legal under Section 702 of the 2008 Foreign Intelligence Surveillance Act (Federal Court Dismisses ACLU, Wikipedia Case Against NSA's 'Upstream' Surveillance , 2015).

The Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 was "created to compel providers of electronic communications services to assist the government in acquiring foreign intelligence information concerning non-US persons located outside the United States" (FISA Amendments Act of 2008 Section 702 summary document, 2008). Section 702 provides the framework of the requirements but it does not say how that framework must be used. The unevaluated data collected by NSA may be shared with government agencies such as CIA and FBI. Section 702 does not give NSA the right to target someone because they are located outside the United States. Section 8

gives NSA the ability to share raw data with second party partners. Domestic communication may not be shared with second party partners (FISA Amendments Act of 2008 Section 702 summary document, 2008). The semi-annual assessment of compliance with the targeting and minimization procedures was provided to the Court and Congress by the Department of Justice and Office of the Director of National Intelligence. The current FISA Amendments Act Section 702 is set to sunset at the end of 2017.

These massive surveillance practices caused the American Civil Liberties Union to file a lawsuit with the U.S. District Court for the District of Maryland (Federal Court Dismisses ACLU, Wikipedia Case Against NSA's 'Upstream' Surveillance , 2015). The U.S. District Court granted a government motions to dismiss the case on the grounds the plaintiffs "had not plausibly alleged that their communications were being monitored by the NSA" (Federal Court Dismisses ACLU, Wikipedia Case Against NSA's 'Upstream' Surveillance , 2015). The ACLU attorney believes that the courts have wrongly insulated the NSA's spying from judicial scrutiny. The dismissal is at odds with overwhelming public records of warrantless surveillance (Federal Court Dismisses ACLU, Wikipedia Case Against NSA's 'Upstream' Surveillance , 2015). The ACLU had previous changed the FISA Amendments Act and the Supreme Court dismissed it in 2013 stating that ACLU lacked standing to establish parties in the case were surveillance or harmed (Federal Court Dismisses ACLU, Wikipedia Case Against NSA's 'Upstream' Surveillance , 2015).

These programs operate with limited scrutiny and could possible endanger the future relationship of foreign nations with the United States. A single NSA analyst or contractor such as Edward Snowden had access to all data collected on citizens and terrorist. This is

how the details of the Prism and Upstream programs came to light with the American citizens (Ball, 2013). President Obama defended the NSA programs and informed the US citizens that "you can't have 100 percent security and also have 100 percent privacy and zero inconvenience" (Miller & Jose, 2013). Citizens do not believe that they should give up liberties for a little safety. Citizens are also concern that these programs violate or circumvent the constitution (Whittaker, 2014).

Telephony metadata created by Verizon for communication between US government collected information about phone calls but not the conversations (mornin, 2014). NSA may analyze the data in according to procedures once it is collected. The government believes the metadata program is consistent with the First and Fourth Amendments (mornin, 2014). The analyst may query any phone number that connected to a suspect's number by up to three degrees of separation (NSA Surveillance Programs and the First Amendment, 2015). This was modified to two degrees of separation by President Obama after the information became public. The US government also believes that call record data lacks protection under the Fourth Amendment. The U.S. Supreme Court's 2012 decision in *United States v. Jones* questions the constitutionality of metadata collection. The fourth Amendment gives "the right of 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" (Legal Information Institute, n.d.). A Supreme Court decision in *Smith v. Maryland* determines that telephone metadata is not a search for Fourth Amendment purposes because there is a lack of privacy in information voluntarily expose to the telephone

company (Litt, 2016). The fourth amendment does not apply to U.S. persons outside the United States (mornin, 2014).

The U.S. Court of Appeals for the 2nd Circuit rule that "Communication does not lose constitutional protection as speech simply because it is expressed in the language of computer code". "Mathematical formulas are written in code and are protected by the First Amendment" (Tsukayama, 2016). However, it still being challenge today if encryption is being protected under the First Amendment. Apple has challenged this several times to protect the end users privacy with encrypted iPhones. The first amendment currently provides them protection against written a code specifically so the government can access data on their encrypted devices. The argument in Apple's case is computer code is an expression of an idea and protected by the first amendment (Lohr, 2016). This was ruled by a Federal District Court in 1996 that code was speech and protected by the First Amendment.

The vast majority of Americans are divided in their concerns about government surveillance of digital communications (Raine & Madden, 2015). Americans believe that every citizen should have the right to their own privacy with who they talk with through communication. On the other hand, some citizens believe that law-abiding citizens have nothing to hide. They believe that it is a small price to pay for maintaining our safe environment from terrorist activities (Raine & Madden, 2015). A survey conducted by Pew Research showed that 87% of Americans were aware of government surveillance. In the survey, 52% of Americans are very concern or somewhat concern about the surveillance program. Figure 1 shows survey responses on how concern Americans is about the surveillance of different communication applications.

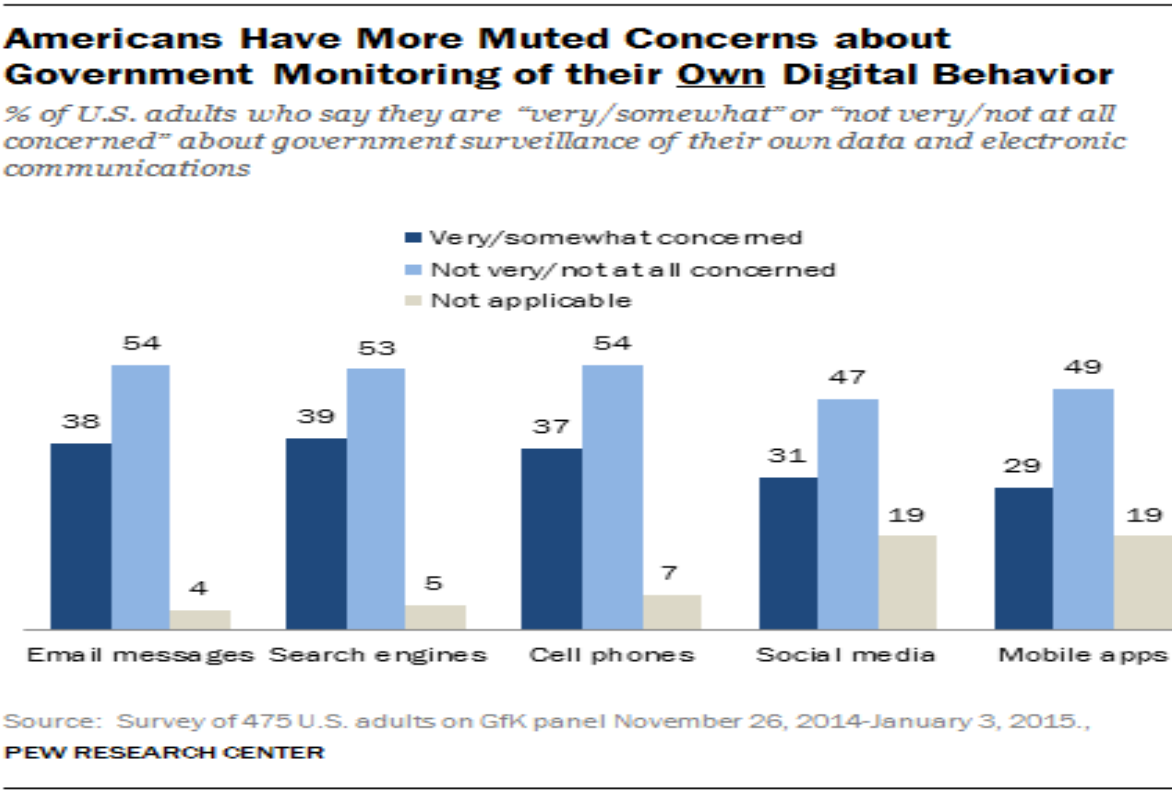


Figure 1: Pew Research center survey response from concern Americans about different communication application being surveillance.

The National Security Agency has ended its massive phone surveillance program as of November 29, 2015 (fingas, 2015). The Senate passed the USA Freedom Act bill that limited massive phone surveillance under section 215 of the Patriot Act. This still leaves many of the other surveillance powers untouched. Agents now have to get a court order to collect data from telecoms and the warrant will only last for six months at a time. The NSA will only have access to five years of legacy data through February 2015 (fingas, 2015). The ending of this program wouldn't be possible without the release of information about government surveillance programs by Edward Snowden.

The reformers are looking to score big on ending another surveillance program. The Senate Judiciary Committee and Internet surveillance experts are having a hearing with

focus on 702 surveillance program (Rosenthal, 2016). The 702 surveillance is the 1978 law that authorizes NSA to collect internet traffic of foreigners. Privacy groups see this as enabling the NSA to incidentally collect data on American citizens (Rosenthal, 2016). NSA allows other government agencies to search the 702 database to help with criminal investigations. This program is set to expire at the end of 2017 and advocates are hoping to force changes to the law. The government wasn't able to provide any examples in which metadata collection had stopped plots or attacks (Rosenthal, 2016). However, officials believe that section 702 does play an important role in preventing terrorist attacks according to the White House panel review of the NSA programs after the Snowden leak (Rosenthal, 2016). Privacy advocates are encouraged that public hearings are happening now. This is the time that Congress can start considering reforms.

A house panel is taking a step towards updating the electronic privacy law that allows agents to read American emails without a warrant (Kelly, 2016). The 1986 Electronic Communication Privacy Act was written before email was a means of communication. The Email Privacy Act introduced by the committee will update the law to require agents to get a warrant before searching anyone's emails. This bill is need because of Congress failure to keep pace with technology that put every American at risk of warrantless searches (Kelly, 2016). The Senate Judiciary Committee is looking at introducing similar legislation. The civil liberties advocates are keeping a close eye on those separate efforts by lawmakers. Civil liberties groups believe American do not expect to keep federal agents from reading their social media but they expect the government to stay out of their email (Kelly, 2016). There may be constitutional problems with having technology companies decide what terrorist speeches are in social media. This does raise First

Amendment free speech issues with technology companies deciding what is consider a terrorist alert posting in social media.

Edward Snowden's disclosure of classified information has fuel a debate about the scope of the government's surveillance powers (Manes, 2016). Surveillance transparency and reform has been the discussion in all three branches of federal government and state capitals. These discussions led Congress to pass the USA Freedom Act to shut down rather than expand surveillance powers (Manes, 2016). In addition, the U.S. Court of Appeals found mass call-tracking program unlawful. These changes to the programs only happen because the surveillance program was publicly disclosed.

In conclusion, the balance between government surveillance and privacy wouldn't be a discussion today without the release of government surveillance program information by Edward Snowden. Edward Snowden unlawful release of information opened the eyes of the public and lawmakers on various surveillance programs. These outdated surveillance programs seem to circumvent the First and Fourth Amendments due to terrorist. The 9/11 attack allowed the federal government to implement broader warrantless surveillance programs. The programs were accepted at the time by the public because they saw it as protecting America from terrorist. The mass collection of sensitive information has been challenged by many as an invasion of privacy increased for citizens. Lawmakers are finally starting to recommend updates to the outdated and illegal surveillance programs in order to protect Americans privacy. These bills and amendments are long overdue from the lawmakers. Individual state governments are looking at updating their local laws to protect citizen privacy. The balance between protection and privacy is a hard task for lawmakers but it is possible in America.

References

Ball, J. (2013, August 21). *Edward Snowden NSA files: secret surveillance and our revelations so far*. Retrieved from The Guardian: https://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations

Braun, S., Flaherty, A., Gillum, J., & Apuzzo, M. (2013, June 15). *Secret to Prism program: Even bigger data seizure*. Retrieved from Yahoo Finance: http://finance.yahoo.com/news/secret-prism-program-even-bigger-data-seizure-140309206.html

Burns, T. L. (1990). *The Origins of NSA.* Center for Cryptologic History.

*Edward Snowden: Leaks that exposed US spy programme*. (2014, January 17). Retrieved from BBC News: http://www.bbc.com/news/world-us-canada-23123964

*Federal Court Dismisses ACLU, Wikipedia Case Against NSA's 'Upstream' Surveillance* . (2015, October 23). Retrieved from Inside Sources: http://www.insidesources.com/federal-court-dismisses-aclu-wikipedia-case-against-nsas-upstream-surveillance/http://www.insidesources.com/federal-court-dismisses-aclu-wikipedia-case-against-nsas-upstream-surveillance/

fingas, J. (2015, November 28). *The NSA's mass US phone surveillance ends tonight*. Retrieved from Engadget: https://www.engadget.com/2015/11/28/nsa-bulk-nsa-phone-surveillance-ends/

(2008). *FISA Amendments Act of 2008 Section 702 summary document.* Office of General Counsel. Retrieved from The Washington Post: https://www.washingtonpost.com/apps/g/page/world/fisa-amendments-act-of-2008-section-702-summary-document/1141/

Kaufman, B. M. (2013, August 9). *A Guide to What We Now Know About the NSA's Dragnet Searches of Your Communications*. Retrieved from American Civil Liberties Unioin: https://www.aclu.org/blog/guide-what-we-now-know-about-nsas-dragnet-searches-your-communications

Kelion, L. (2013, July 1). *Q&A: NSA's Prism internet surveillance scheme*. Retrieved from BBC News: http://www.bbc.com/news/technology-23051248

Kelly, E. (2016, February 21). *Congress looks to boost email privacy; increase social media surveillance*. Retrieved from USA Today: http://www.usatoday.com/story/news/2016/02/21/congress-looks-boost-email-privacy-increase-social-media-surveillance/80557184/

*Legal Information Institute*. (n.d.). Retrieved from Cornell University Law School: https://www.law.cornell.edu/constitution/fourth_amendment

Litt, R. S. (2016). The Fourth Amendment in the Information Age. *The Yale Law Journal*, 126.

Lohr, S. (2016, February 25). *Analyzing Apple's Argument That First Amendment Applies to Its Code*. Retrieved from NY Times: http://www.nytimes.com/2016/02/26/technology/in-apple-case-addressing-the-legal-status-of-code.html?_r=0

Manes, J. (2016). Online Service Providers and Surveillance Law Transparency. *The Yale Law Journal*, 125.

Miller, Z., & Jose, S. (2013, June 07). *President Obama Defends NSA Surveillance Programs As "Right Balance"*. Retrieved from Time: http://swampland.time.com/2013/06/07/president-obama-defends-nsa-surveillance-programs-as-right-balance/

mornin, J. (2014). NSA Metadata Collection and the Fourth. *Berkeley Technology Law Journal*, 986-1006.

Mullikin, A., & Rahman, S. M. (2010). THE ETHICAL DILEMMA OF THE USA. *International Journal of Managing Information Technology*, 32-38.

Niarchos, N. (2014, February 4). *Has the NSA Wiretapping Violated Attorney-Client Privilege*. Retrieved from The Nation: https://www.thenation.com/article/has-nsa-wiretapping-violated-attorney-client-privilege/

(2015). *NSA Surveillance Programs and the First Amendment.* American Constitution Society.

Raine, L., & Madden, M. (2015, March 16). *Americans' Views on Government Surveillance Programs*. Retrieved from Pew Research: http://www.pewinternet.org/2015/03/16/americans-views-on-government-surveillance-programs/

Rosenthal, M. J. (2016, May 10). *The Fight Over NSA Internet Surveillance Is Heating Up Again*. Retrieved from Mother Jones: http://www.motherjones.com/politics/2016/05/next-big-fight-over-nsa-surveillance-kicking-week

Simpson, D. (2016, March 6). *Intelligence Briefing: American Intelligence A Forced Restart*. Retrieved from Dni news: https://dninews.com/article/intelligence-briefing-american-intelligence-forced-restart

Tsukayama, H. (2016, February 26). *We asked a First Amendment lawyer if Apple's 'code is speech' argument holds water. Here's what he said.* Retrieved from The Switch: https://www.washingtonpost.com/news/the-switch/wp/2016/02/26/we-asked-a-first-amendment-lawyer-if-apples-code-is-speech-argument-holds-water-heres-what-he-said/

Whittaker, Z. (2014, June 30). *Legal loopholes could allow wider NSA surveillance, researchers say*. Retrieved from CBS News: http://www.cbsnews.com/news/legal-loopholes-could-let-nsa-surveillance-circumvent-fourth-amendment-researchers-say/