A Step Too Far: Protecting Privacy in a Digital Age

Sophia D. Mills

Sophomore at Marshall University

2014 Judge Dan O'Hanlon Essay Competition

Benjamin Franklin famously said that “those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety” (Labaree, 1963). Franklin’s words illustrate that, from the founding of this country, Americans have sought to strike a delicate balance between liberty and national security. I think most people would agree that as long as we live in a governed society, our liberty is somewhat restricted for our own well-being. After all, for the safety of adults, children, and pets in the neighborhood, one cannot drive seventy miles-per-hour on a residential road. Anyone seeking to board a plane knows the hassle of removing shoes and loading carry-on luggage onto a belt to be searched and scanned. These are restrictions on our liberty in the name of safety, but not many rational people would argue against the necessity of traffic laws and airport security. Therefore, “liberty” and “privacy” are not absolute. But how much privacy should we ask American citizens to sacrifice in the name of national security? Today, the ubiquity of technology is further complicating our notion of privacy. We live in a strange world in which we willingly share our lives on websites like Facebook and Twitter, but, at the same time, view our phones as intimate pieces of our lives. Americans’ strong connection to technology has helped make “Edward Snowden” a household name.

In May of 2013, Snowden unearthed classified NSA documents about the agency’s secret programs and practices. Among other information, Snowden revealed the existence of PRISM, a program that stores and updates Americans’ telephone metadata for up to five years. “Metadata” is information about a phone call, cataloging only time, location, and length of a conversation—not the conversation itself. Snowden entrusted journalist and former civil rights attorney, Glenn Greenwald, with the information that would soon light up the country. Snowden flew to Hong

Kong to meet Greenwald and, in the security of a locked hotel room, spilled secrets on the powerful government agency.

Snowden first showed himself to the world through a recorded television interview. His public debut was met with surprise, as people were shocked that someone as young and unassuming as Snowden was in the position to become the most important whistleblower in recent history. Snowden, himself, expressed surprise about his power after being hired by the CIA in 2006, writing "I don't have a degree of ANY type...in fact, I don't even have a high school diploma" (Andrews, et al., 3). It was in 2012, when Snowden was hired as a systems administrator, that he started making illegal downloads of classified security documents (Andrews, et al., 5). After he collected documents proving his credibility, he reached out to Greenwald and to filmmaker Laura Poitras. When he accepted his last job as a government contractor with Booze Allen Hamilton, Snowden made his final dash to load flash drives with information on the program PRISM so he could leave his job and flee to Hong Kong to meet with the reporters (Andrews et al., 6).

Some call Snowden a "hero" and "patriot." Others regard him as a "traitor." One thing is certain: Snowden sparked a substantive debate among an often-apathetic public. For this, I think his actions have value, and I do not view Snowden as a villain. Though slightly dramatic and egotistical, Snowden did what, he felt, was an act of conscience. "Every person remembers some moment in their (sic) life where they witnessed some injustice, big or small, and looked away, because the consequences of intervening seemed too intimidating," said Snowden. He continued, "but there's a limit to the amount of incivility and inequality and inhumanity that each individual can tolerate. I crossed that line. And I'm no longer alone" (Andrews, et al., 2).

Snowden's revelations prompted legal challenges to the NSA's actions. Two prominent U.S. District Court cases have now shown that even the brightest legal authorities are split on the constitutionality of metadata collection. These cases are *ACLU v. Clapper (2013)* and *Klayman v. Obama (2013)*. In *ACLU v. Clapper*, Judge Pauley, a Clinton-appointee, rules in favor of metadata collection, while, in *Klayman v. Obama*, Judge Leon, a Bush-appointee, rules against metadata collection. Judge Pauley makes his decision largely based on the precedent set by the U.S. Supreme Court in *Smith v. Maryland (1979)*, the case which argues that the collection of telephone metadata does not constitute a "search" under the Fourth Amendment and, therefore, does not require a warrant. The majority opinion in *Smith* asserts that by placing a telephone call, an individual is knowingly releasing information to a third party (the telephone company) and has, therefore, no "legitimate expectation of privacy" (*Smith v. Maryland*, 442 U.S 735, 1979, p.p 738). Judge Pauley says metadata collection does little to invade privacy while still providing valuable security.

On the opposite side, Judge Leon writes of the NSA's actions as almost "Orwellian." Judge Leon argues that, because the role of technology has transformed since 1979, the precedent of *Smith* cannot be applied to a 2013 case. He says that our constant use of phones allows metadata to be more revealing than ever, therefore making such information more private than in 1979. He continues to question the overall effectiveness of the program in his attempt to balance national security interests with privacy concerns.

When watching the news coverage of the NSA leaks, I was frustrated by those who had an almost radical, conspiracy-laden opposition to the government's actions. I still feel that many NSA opponents are too dramatic—including Edward Snowden and Glenn Greenwald. However,

after reading the eloquent, reasonable opinions of both Judge Pauley and Judge Leon, I feel that the pro-metadata collection argument boils down to two important points: 1) people have no reasonable expectation of privacy because they are knowingly releasing metadata to their phone companies, and, therefore, to the government, and 2) metadata collection is extremely beneficial to our national security. Each of these points has flaws too substantial for me to support.

The Fourth Amendment to the United States Constitution 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." Each judge seeks to answer what constitutes a "search." Judge Leon argues that metadata collection is a "search," and, therefore, cannot be done without first obtaining a warrant. Judge Pauley claims that metadata collection is not a "search," so can be done without a warrant.

Judge Pauley mirrors the main argument in *Smith*: the petitioner, Mr. Smith, had no "reasonable expectation of privacy" when dialing the number of a woman he was accused of robbing because "telephone users, in sum, typically know that they must convey numerical information to the phone company and that the phone does in fact record this information for a variety of legitimate business purposes" (*Smith v. Maryland*, 442 U.S 735, 1979, p.p 743). The majority continues to reference precedent set by *Katz v. United States (1967)*, saying that even if the petitioner, himself, expected privacy when placing a call from his own home, this "expectation is not 'one that society is prepared to recognize as reasonable'" (*Smith v. Maryland*, 442 U.S 735, 1979, p.p 744). This seems like an incredibly subjective claim. How do we gauge

what society accepts as reasonable? Furthermore, even if public sentiment could be accurately measured, does the majority of society have the authority to trample on, or to expand, individual rights? Individual rights are often in place specifically to protect the minority and, therefore, cannot be reversed based on the whims of fellow Americans. In addition, what the majority opinion in *Smith* really expresses is the Justices'—not society's—belief that metadata collection is reasonable. After all, Mr. Smith—though a criminal— was still a member of society who believed he *was* entitled to keep his phone metadata private. The Justices are projecting their own beliefs upon "society," so it seems inappropriate to limit privacy rights based on the Justices' idea that society is ready to relinquish those rights.

The dissenting opinion in *Smith* also points out the majority's tautological argument: "...the court today says that those safeguards [granted in previous decisions] do not extend to the numbers dialed from a private telephone, apparently because when a caller dials a number the digits may be recorded by the telephone company for billing purposes. But that no more than describes the basic nature of telephone calls" (*Smith v. Maryland*, 442 U.S 735, 1979, p.p 747). To make a phone call, a person must, by definition, release information to the phone company. This is the only way to complete a call. The fact that information is automatically recorded by the phone company really says nothing about an individual's right to privacy, and does not address whether the government can store metadata in a massive database.

In addition, the majority in *Smith*, and Judge Pauley, argue that the average telephone user knows that, once he releases metadata to a third party, the information is free to be accessed by the government, or, in recent times, handed over in lists to the NSA. It would take political and legal knowledge to think: "Since I am dialing a phone number, I am sending metadata to my

phone company. When making my call, I have no reasonable expectation of privacy because I am voluntarily giving my data to a third party. This data will then go into PRISM, the NSA's metadata collection system." This is a complicated chain of logic for many people to understand.

As the landmark criminal case *Miranda v. Arizona* conveys, citizens' protection under the law should not be based upon their knowledge. Instead, the famous case dealing with rights of the accused argues that the least knowledgeable are the ones most in need of protection:

> "The defendant who does not ask for counsel is the very defendant who most needs counsel. We cannot penalize a defendant who, not understanding his constitutional rights, does not make the formal request, and, by such failure, demonstrates his helplessness. To require the request would be to favor the defendant whose sophistication or status had fortuitously prompted him to make it" (*Miranda v. Arizona*, 384 U.S. 436, p.p 472).

Likewise, the argument that individuals are waiving their privacy rights by making a phone call expects people to possess knowledge they may not possess.

The majority's argument seems to imply that, because a person knows that information will be recorded, he or she has no right to keep the information private. Would the government have the right, under this precedent, to open a person's outgoing mail as long as the sender were informed that it would be opened? The dissenting Justices summarize this as "[allowing] government to define the scope of Fourth Amendment protections" (*Smith v. Maryland*, 442 U.S 735, 1979, p.p 750). The government would simply have to "announce its intent" and a person would no longer have a reasonable expectation of privacy in the eyes of the court.

Judge Pauley continues his argument by expressing the supposed limits on the NSA's power to "query" a number in the database. To run a search on a number, FISA courts must approve a query which learns the metadata of "numbers within three 'hops' of the 'seed.'" (*American Civil Liberties Union v. Clapper,* Civil Action No. 13-3994, slip op. 2013, p.p 40). The "seed" is a number which the NSA identifies as suspicious, but as stated by Pete Yost and Matt Apuzzo, "when the NSA identifies a suspect, it can look not just at his phone records, but also the records of everyone he calls, everyone who calls those people and everyone who calls those people" (2013). If the average person dialed forty different numbers, a "three-hop analysis" would search the metadata of 2.5 million Americans (Yost & Apuzzo, 2013). In 2012, the NSA ran 288 queries (Stone, 2013). So, while Judge Pauley tries to downplay the number of phone numbers queried, we should remember that, after the usual "three hops," the amount of metadata that falls under surveillance can be vast.

Next, Judge Pauley says the effectiveness of metadata collection "cannot be seriously disputed" (*American Civil Liberties Union v. Clapper,* Civil Action No. 13-3994, slip op. 2013, p.p 49). However, the testimony Pauley cites in his case may be exaggerated, as outside sources suggest the NSA's effectiveness is not largely grounded in its metadata collection efforts. In 2013, the non-partisan New America Foundation conducted a study of claims made by NSA officials. This study "examined records for investigations into 225 people who have been indicted, convicted or killed by the U.S. for their reported ties to Al-Qaeda and Al-Qaeda-affiliated groups...after Sept. 11, 2001" (Moskowitz, 2014). Of those cases, only four of the investigations were initiated because of metadata collection, and no imminent terrorist attacks were prevented because of the program.

The program's failure to prevent imminent attacks is ironic, as Judge Leon shows that "speed" has been the NSA's main argument in support of metadata collection. The NSA speaks of "time-sensitive situations," saying we need "immediate" action, and we cannot lose "valuable time." But, again, there is no proof that metadata collection has prevented an imminent attack. The New America Foundation study shows that traditional methods—such as using information obtained from the FBI, CIA, and "communities, families, and informants"—were more powerful than metadata collection. The study concludes, "surveillance of American phone metadata has had no discernible impact on preventing acts of terrorism and only the most marginal of impacts on preventing terrorist-related activity, such as fundraising for a terrorist group" (Moskowitz, 2014). The report also suggests that the more beneficial tactic for national security would be for the intelligence community to more closely scrutinize the information it already holds as a result of "traditional law enforcement," instead of looking to obtain more data. This failure to study information in our possession was also true in the case of two 9/11 hijackers living in San Diego and has "also [been] the unfortunate pattern we have seen in several other significant terrorism cases," reports Al Jazeera (Moskowitz, 2014).

Therefore, I feel that Judge Pauley's two main arguments in support of metadata collection prove shaky when scrutinized, making Judge Leon's argument the more logical. Judge Leon argues that the precedent of *Smith* cannot be applied to modern-day America because 1) the pen register in *Smith* targeted one person for fewer than two weeks, whereas PRISM collects information on millions of Americans and stores it for five years, and 2) the role of technology in our lives has evolved.

"The number of mobile [phone] subscribers in 2013 is more than 3,000 times greater than in 1984," Judge Leon cites (*Klayman v. Obama,* Civil Action No. 13-0851, slip op. 2013, p.p 51). Judge Pauley dismisses this statistic, saying that the definition of metadata has not changed. However, because of the heightened role of cell phones in our lives, the government can now learn more information about the phone user; so while the definition of metadata is unchanged, the personal details that can be extracted from metadata have spiked. For this reason, metadata should be treated as more private than in 1979, when cell phones did not even exist, much less dominate our personal lives (*Klayman v. Obama,* Civil Action No. 13-0851, slip op. 2013, p.p 53).

Because telephone usage is, arguably, necessary for business, personal safety, and socialization, our phones are more intimately connected to us than ever before, therefore strengthening our expectation of privacy. In fact, if we were to venture back to Judge Pauley's argument about what society recognizes as private, his already-subjective argument backfires. A *USA Today* poll shows that fifty-three percent of Americans disapprove of the metadata collection program, and a stunning seventy percent of Americans believe they "shouldn't have to give up privacy and freedom in order to be safe from terrorism" (Page, 2014).

Because Judge Leon agrees that the plaintiffs in *Klayman* do have a reasonable expectation of privacy, the NSA's collection of metadata constitutes a "search." By definition, "warrantless searches...are unreasonable under the Fourth Amendment"(*Klayman v. Obama,* Civil Action No. 13-0851, slip op. 2013, p.p 56). Even so, precedent sets exceptions for warrantless searches under "special needs," as the government argues in *Klayman*. Judge Leon recognizes, as I do, that in unique situations, the urgency of national security trumps individuals'

privacy rights. This brings us back to our original question: how much privacy should we sacrifice in the name of national security? Based on the underwhelming effectiveness of the NSA's metadata collection, I do not think this program justifies chipping away at privacy rights.

I understand the American inclination to fear terrorism. I remember, as a child, staring at a hotel room television in Baltimore, Maryland, watching the World Trade Center collapsing in flames. Years later, I saw the faces of the slain 3,000 Americans sewn into a giant memorial tapestry hanging in the Pentagon. But we cannot allow the scars of 9/11 to exaggerate the threat of terrorism. Because acts of terror are shocking, we remember the lives taken by terrorism in 2001, but not the 29,573 people killed by guns, or the 13,290 killed by drunk driving the same year (Friedersdorf, 2013). Likewise, during the period of 1999-2010, which includes the most deadly terrorist attack in United States history, about 3,000 lives were lost due to terrorism, while 364,000 died from gun fire, and 150,000 were killed in drunk driving accidents.

By no means, though, does this suggest that we should do nothing to protect ourselves from attack. As Connor Friedersdorf writes in *The Atlantic*, "the U.S. should certainly try to prevent terrorist attacks, and there is a lot that government can and has done since 9/11 to improve security in ways that are totally unobjectionable" (2013). In fact, the White House was warned in 2001 of Al-Qaeda's suspected plans to attack American soil, but White House officials did not take immediate action, as they believed the claims were not specific (Ross & Sylvester, 2002). The fact that we were given warnings, but failed to act reiterates the finding of the New America Foundation's study. We can have the needed information without metadata collection; we just need to look at the information we already possess more closely. Friedersdorf ends by saying that

"the seeming contradictions in how we treat different threats suggest that we aren't trading civil liberties for security, but a *sense* of security" (2013).

In conclusion, I do not hold a radical view of the NSA's metadata collection program. In fact, I believe most people will not be directly affected or harmed by PRISM. However, I do believe in principle, and I believe in establishing the right precedent. Judge Pauley's argument sends the message that privacy can be eroded without strong justification, and that the safeguards in the Fourth Amendment can be easily disregarded. While we can be, and should be, a nation protected from terrorism, we must remember that the constitutional protections we guarantee our citizens are the true foundation of America's greatness. Now is not the time to abandon our most-cherished principles.

References

Andrews, S., Burrough, B., & Ellison, S. (2014, May 1). The Snowden Saga: A shadowland of secrets and light. *Vanity Fair*. Retrieved July 15, 2014, from http://vanityfair.com/politics/2014/05/edward-showden-politics-interview

American Civil Liberties Union v. Clapper, Civil Action No. 13-3994, slip op. (S.D.N.Y. Dec. 27, 2013)

Friedersdorf, C. (2013, June 10). The irrationality of giving up this much liberty to fight terror. *The Atlantic*. Retrieved July 18, 2014, from http://www.theatlantic.com/politics/archive/2013/06/the-irrationality-of-giving-up-this-much-liberty-to-fight-terror/276695

Klayman v. Obama, Civil Action No. 13-0851, slip op. (D.D.C., Dec.16, 2013)

Labaree, L. (1963). The papers of Benjamin Franklin. : Yale University Press.

Miranda v. Arizona, 384 U.S 436 (1966)

Moskowitz, P. (2014, January 13). Report suggests NSA surveillance has not stopped terrorism. *Al Jazeera America*. Retrieved July 15, 2014, from thhp://america.aljazeera.com/atricles/2014/1/13/review-finds-nsametadatacollectionhasntstoppedanattack.html

Page, S. (2014, January 20). Poll: Most Americans now oppose the NSA program. *USA Today*. Retrieved July 17, 2014, from http://www.usatoday.com/story/news/politics/2014/01/20/poll-nsa-surveillance/4638551

Ross, B., & Sylvester, L. (2002, May 15). Bush warned of hijackings before 9-11. *ABC News*. Retrieved July 18, 2014, from http://abcnews.go.com/US/story?id=91651&page=1

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

Stone, G. (2013, December 25). The NSA's telephone meta-data Program: Part I. *The Huffington Post*. Retrieved July 15, 2014, from http://www.huffingtonpost.com/geoffrey-r-stone/nsa-meta-data_b_4499934.html

Yost, P., Apuzzo, M. (2013, July 31) With 3 "hops," NSA gets millions of phone records. *Associated Press.* Retrieved July 25, 2014, from http://bigstory.ap.org/article/senate- panel-looking-limits-surveillance