2014

A New Balance: National Security and Privacy in a Post 9-11 World

Russell B. Wilson
Colby College

A New Balance: National Security and Privacy in a Post 9-11 World

Russ Wilson
Government Honors Thesis, May 2014
Advisor: Dr. L. Sandy Maisel
Second Reader: Dr. Cal Mackenzie

Abstract

The terrorist attacks on September 11, 2001 shocked the American security apparatus, placing greater pressure on the security actions of the U.S. government, particularly regarding information gathering. Laying out a framework that examines different notions of national security and privacy, this paper examine three case studies to illustrate the role of the government and the inherent friction between privacy and security that increased information gathering inherently creates. The shifting balance between the two variables forces us to reexamine how we want our government to protect us and what we will sacrifice in order to ensure our own well being. With the government's actions after 9/11, intelligence agencies admittedly sacrificed some individual privacy in order to ensure national security. Must we, as Americans, give up some of our civil liberties in the age of metadata and cloud technology to ensure our security? Or, do the government's actions represent an unwarranted and unnecessary violation of our privacy? By examining the government's actions leading up to, immediately following, and extending past 9/11, this paper seeks to explore these questions and contextualize the evolution of the government's national security strategy and the subsequent implications for America moving forward in the 21st century.

Introduction

The terrorist attacks on September 11, 2001 shocked the American security apparatus. Nineteen terrorists armed only with box cutters found a way to strike at the heart of the country with the largest national defense budget and most advanced military in the world. Their effectiveness called into question the government's ability to protect its own citizens and spurred debate to strengthen and adapt the nation's defense capabilities. Part of the shifting security calculus meant that obtaining accurate information about the intentions and actions of those seeking to harm American citizens is now seen as paramount to eliminating surprise attacks and ensuring our safety. The presence of Transportation Security Administration (TSA) officers, the use of high-tech body scanners and the confiscation of shampoo bottles greater than three-ounces at airport security checkpoints all serve as physical manifestations of the increased need for airport security, but the most substantial changes have occurred behind the scenes in the way the United States has chosen to monitor potential threats to national security.

Fundamentally, the attacks highlighted the lack of accurate information about individuals looking to harm the United States and the inefficiencies present in the surveillance strategy of the country (9/11 Report: Joint Congressional Inquiry 2003, xv). Through legislation and executive action, the Federal government sought greater coordination between agencies and increased flexibility in information gathering. Passed by lawmakers in the wake of the terrorist attacks, the Patriot Act stands as the hallmark piece of legislation seeking to harness technology in order to mitigate the risk of potential attacks against U.S. citizens. However, increasing the use of technology creates potential problems for today's society, as gathering more information runs the risk of violating

citizens' privacy. Electronic surveillance pits the security interest of the nation against individuals' ability to retain control over personal information. Does this surveillance protect or harm Americans? If it does diminish the civil liberties of the nation's citizens, is there a way to balance the need for national security with privacy interests?

Laying out a framework that defines national security and privacy in the United States today, I examine three case studies to illustrate the role of the government and the inherent friction between privacy and security that increased information gathering inherently creates. The shifting balance between the two variables forces us to reexamine how we want our government to protect us and what we will sacrifice in order to ensure our own well being. With the government's actions after 9/11, intelligence agencies admittedly sacrificed some individual privacy in order to ensure national security. Must we, as Americans, give up some of our civil liberties in the age of metadata and cloud technology to ensure our security? Or, do the government's actions represent an unwarranted and unnecessary violation of our privacy? By examining the government's actions leading up to, immediately following, and extending past 9/11, the following paper seeks to explore these questions and contextualize the evolution of the government's national security strategy and the subsequent implications for America moving forward in the 21st century.

I. Literature Review

Privacy

The literature on privacy, while extensive, fails to reach a consensus on one distinct right to privacy and how it should apply in today's modern age of technology.

Part of the struggle comes from the acknowledgement that a concept of privacy is subject to change over time with shifting social norms and differing views of what truly counts as private. Similarly, while each individual possesses what he or she views as a sphere of privacy, the framers did not include a distinct right of privacy in the Constitution (DeCew 1986, 160). Certainly, as with most issues in the American polity, the notion of privacy has received a great deal of attention since the writing of the Constitution, but the question about a distinct right still remains.

Scholarly work on the philosophical and legal question of privacy starts with Warren and Brandeis's (1890, 205) "The Right to Privacy," in which the authors quote Judge Cooley, stating that the right of privacy is the right "to be let alone." Limiting others' access to oneself plays a central role in their notion of privacy, as any citizen "is entitled to decide whether that which is his shall be given to the public" (Warren and Brandeis 1890, 199). However, as the literature evolved on the topic, others challenge Warren and Brandeis, stating that the right "to be let alone" creates too broad a conception for a reasonable definition (See Parent 1984, 342; Introna 1997, 262; DeCew 1986, 150; Moor 1990, 71; Solove 2002, 1101). The difficulty with deriving an agreed upon right stems from the other rights and values that inherently interact with an individual's notion of privacy. Secrecy, autonomy, liberty and solitude all overlap with one's ability to claim privacy as a separate right. Building on Warren and Brandeis's paper, much of the debate on the topic started in the 1960s and focused more broadly on privacy's intrinsic and instrumental values (Moor 1990, 80). Many authors lay out the different strands of privacy, mentioning multiple ways of viewing the concept philosophically, as well as debating how to define it as a distinct, measurable right that

captures what it must without remaining too obtuse to provide any sort of practical use (See Introna 1997, 262-265; Tavani 2007, 3; Parent 1984, 342-346; Solove 2002, 1099; Nissenbaum 1998, 570; Moor 1990, 70; Schoeman 1984, 201-207).

Much of the literature surrounding privacy revolves around criticizing existing philosophical and legal formulas, demonstrating the fact that it remains easier to challenge aspects of privacy than to assert a concise definition. That said, these common critiques form a basis for the definitions that follow Warren and Brandeis' original assertion. By examining these themes, one appreciates the slippery nature of privacy and the challenge facing one who seeks to define a distinct right succinctly.

The principle of non-intrusion stems directly from the right "to be let alone," but this principle is too unwieldy philosophically. The state of being free from physical invasions into one's life largely means an individual's complete separation from society (Parent 1984, 342; Moor 1990, 71). However, seclusion does not necessarily mean one enjoys privacy, and privacy is not just isolation from other people. An intrusion into a home constitutes an invasion, but the ability to interact physically with someone overall does not dictate an individual's notion of privacy (Tavani 2007, 6). Furthermore, relying on the separation of an individual from other people also shows a difference between the condition of privacy and the right to privacy—can one distinguish between losing privacy voluntarily and a violation of a fundamental right (Introna 1997, 262)? Non-intrusion cannot make this distinction well; and, while access to an individual contains aspects of privacy, seclusion and non-intrusion do not fully capture privacy as a philosophical concept or a right. They do encapsulate notions of one's autonomy from others, but autonomy and privacy are not always synonymous.

A second concept of privacy revolves around the control of one's own personal information, giving an individual the ability to limit what others can see or access. DeCew (1986, 167) links privacy to property rights in this manner—one's privacy allows a person to retain control over personal information, and he can choose when to allow others to access it. However control over personal information conflates privacy with other distinct concepts, namely autonomy and secrecy. This definition of privacy remains too broad—it is hard to justify the possibility of an infringement of privacy if that breach occurs in a public sphere, i.e. if one observes another person walking down the street but that person did not want to be seen (Parent 1984, 344; Tavani 2007, 7-8). Can an interaction such as this truly be viewed as a violation of privacy? Basing the level of privacy of a "reasonable person standard"—what an average person would consider private—helps in this respect, but it still leaves a wide variation of what one could consider as important in regards to privacy (DeCew 1986, 168-9).

Someone may also offer information about herself; and, once that information is in the public domain, she may lose control over how others use it. Since she offered the information to the public originally, it may be difficult to argue that she necessarily lost privacy (Introna 1997, 263). A caveat exists to this argument that the context of when and how one shares the information remains important. Just because one offers personal information to another does not necessarily mean it is open to all, i.e. offering information to a government agency or a doctor remains different than posting something on a social media platform (Nissenbaum 1998, 583). Fundamentally, limiting different levels of information to other individuals creates the relationships one makes in life, as

the access to personal details can create or prevent a level of social and intimate interaction (Introna 1997, 265-267).

Many of the constitutional cases for privacy revolve around the individual's liberty to act (DeCew 1986, 164-5; Moor 1990, 72). Decision-making power relates more to a notion of individual liberty and the ability one has to make a choice in a given situation; many of the legal precedence set regarding the freedom to act remains narrow in scope, focusing on a few cases. *Griswold v. Connecticut*, 381 U.S. 479 (1965) and *Roe v. Wade,* 410 U.S. 113 (1973), both addressing reproductive and family planning decisions, address specific areas of privacy and fail to conceptualize one specific right. Instead, the legal justification for a right to privacy seems up to interpretation, subject to which Justice reviews the facts at hand, as Moor (1990, 72-74) examines for *Griswold*. In the case, Justice Douglas states that "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance…Various guarantees create zones of privacy" (381 U.S. 485). Justice Goldberg uses the Ninth Amendment to protect the right to privacy, while Justice Harlan also agrees with a specific right but relies upon the due process clause of the Fourteenth Amendment. Justice Black takes a wholly different view of the case—the Connecticut law was wrong but no right of privacy exists in the Constitution or the Bill of Rights (Moor 1990, 73).

So while the Supreme Court deals with issues related to privacy, involving one's ability to protect certain information about oneself, no specific legal distinction for privacy exists, making a right to privacy harder to define strictly on a constitutional basis and is up to much debate among different Justices. Beyond the uncertain legal foundation

for a distinct, agreed upon right, basing privacy on an individual's freedom to act contains inherent flaws. Privacy concerns arise when evaluating the context of the decision and with whom one wants to share certain information. The ability of an individual to make the decision is not the primary privacy concern; the "nature of the decision" is much more important (DeCew 1986, 165). The liberty to act, even with variable legal defense, is not always directly related to privacy. Philosophically and legally, one's right to receive birth control or an abortion deals with liberty and not exclusively a right to privacy.

One last aspect of the debate among philosophers over the last couple decades worth mentioning is the ability of an individual to remain free from judgment by others. This notion blends one's control of personal information and non-intrusion, conflating privacy with autonomy and secrecy. The definition is problematic because, while wanting to control certain information, one cannot dictate how others interpret the information that they receive (Introna 1997, 263). Hoping for something as large in scope as filtering what others think of oneself is certainly too hard to expect as a right to privacy and even harder to enforce as one.

In the realm of enforcement, there exists a certain boundary, even if legally hazy, beyond which a breach in privacy is egregious and in violation of one's rights. While the Constitution does not provide for an explicit right to privacy, the entangled nature of the notion of privacy with liberty, autonomy and secrecy allows one to argue implicitly for privacy using the Constitution and Bill of Rights. The Fourth Amendment fills this role when dealing with the interaction with citizens on personal matters, stating:

> 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.

This standard implicitly states a right to privacy, or at least the right to avoid unjustified intrusion into one's affairs. The rapid technological advancement and proliferation of information over the Internet raises many questions as to how far legally the government can infringe upon an individual and what the threshold for probable cause must be. Moor (1997, 32) asserts a Justification of Exceptions Principle—"a breach of a private situation is justified if and only if there is a great likelihood that the harm caused by the disclosure will be so much less than the harm prevented that an impartial person would permit breach in this and in morally similar situations,"—to outline when the violation of the notion of privacy is ethically permissible. Even within this principle, much remains up for interpretation, as the extent of harm caused and prevented by a disclosure of certain information remains largely subjective and dependent on a case-by-case judgment as well as the individual reviewing the matter.

Despite these challenges, some definitions of privacy presented by philosophers are worth examining. Beyond the instrumental value of privacy, there exists an intrinsic notion of privacy that possesses its own worth beyond providing the foundations for liberty, autonomy, secrecy and other rights. Separating intrinsic from instrumental value creates a daunting task, but Parent (1984, 346) tries to address the flaws of the four avenues of thought listed above, stating that "privacy is the condition of a person's not having undocumented personal information about himself known by others." His definition incorporates the non-intrusion and control of information concepts to conclude that privacy cannot exist in a public sphere, but seclusion does not create the only condition in which one can enjoy privacy. This method relies upon a concept of personal

information, which includes "facts that most persons in a given society choose not to reveal about themselves…or to facts about which a particular person is extremely sensitive and which he therefore does not choose to reveal about himself" (Parent 1984, 347). In this manner, the facts that one learns or perceptions created in a public setting cannot violate the privacy of another individual.

While Parent does offer a view more confined and specific than "to be let alone," the reliance upon personal information and not allowing for privacy in any public situation creates a definition that is too narrow. Even if in public, eavesdropping on a conversation can constitute a violation of one's privacy, highlighting the way in which one acquires information is just as important as the information gathered (DeCew 1986, 152; Moor 1990, 76). Focusing only on the content of information in defining privacy, Parent overlooks the relationship between privacy and surveillance, an essential component when examining the actions taken to protect the national security interests of the United States. Furthermore, an undocumented fact about an individual that passes between people in conversation, if widely known, cannot truly be part of a violation of privacy because of the already established publicity of that fact before the private conversation even occurs (Moor 1990, 76; DeCew 1986, 153). The classification of information is critical to privacy, but by only focusing on the content of information and not how or what the access to this information entails, the definition remains too constrained in scope to create a coherent and manageable concept of privacy.

Addressing the concerns with Parent's definition while trying to incorporate the strengths of non-intrusion and limited control, Moor (1990, 76) states that "an individual or group has privacy in a situation if and only if in that situation the individual or group

or information related to the individual or group is protected from intrusion, observation, and surveillance by others." While this idea does not create a defined legal right of privacy, it allows for a workable way to see how outside influence interacts with the private matters of an individual or group. Not confining privacy to one facet—non-seclusion, divulgence of personal information, etc.—allows for different types of privacy and a definition that relies upon zones of privacy (Introna 1997, 264; Moor 1990, 78; Nissenbaum 1998, 570; Tavani 2007, 3). These zones refer to the information and situations where one can protect the information that he or she deems unnecessary or damaging to share with the public eye. Much of what one considers reasonable within a zone of privacy depends on cultural factors, shifting as new developments in technology change the way people interact with one another (Moor 1990, 30). Even open to change over time, allowing for privacy to cover multiple situations and circumstances allows for the best working definition of the concept.

Reviewing the relevant literature since Warren and Brandeis' seminal piece, one sees that philosophers understandably struggle to separate privacy from other concepts and to define one agreed upon right. However, many admit that common themes on the subject exist, allowing for a broad discussion, if not always agreement, on what a coherent legal or philosophical right necessarily entails. Privacy is innately personal, it requires some sort of control over the information shared with outside agents and the situation in which the information is divulged, and, in some circumstances, it can exist in public. Privacy entails a zone of information and circumstances about which an individual controls when and where outside influences can have access. Additionally, privacy receives greater attention with the increased use of computers and other forms of

technology to communicate. Social media allow personal information to flow more easily among people and makes "greased data"—public information that may have once been hard to find—much more accessible to any internet user (Moor 1990, 27). Fundamentally, the rise of technology illuminates the debate between private information and the public sphere. With the rise of technology, does the concept of what we consider private and public information change? While no agreed upon solution or answer exists to the question philosophically, there does exist a consensus that privacy holds a distinct, intrinsic value that must be preserved.

In regards to government surveillance and individuals' expectation of privacy, the context in which a person forfeits privacy to a third party, whether another individual, a private company, or the government, is important. When one forfeits some privacy by sharing information with another individual, he can still expect the information to remain between these two parties. This contextual integrity allows people to form different relationships with others, either socially or in regards to one's interaction with private companies and the government (Nissenbaum 1998, 584). Someone can choose to sacrifice his privacy by sharing personal information with a company, but that does not mean that he gives up that information for any outside viewer. Contextual integrity is important when looking at surveillance actions because the mere aggregation of personal communications information by the government, without sharing it with other actors, still has implications for privacy violations, as examined further when looking at the Bulk Telephony Metadata Collection Program in the third case study.

National Security

National Security for the United States covers a broad array of issues. From natural disasters to terrorist attacks, the threats facing the country take many different forms. Leaving aside the role of economic or environmental security, Sarkesian et al. (2013, 2) state "US national security is the ability of national institutions to prevent adversaries from using force to harm Americans or their national interests and the confidence of Americans in this capability." Allowing for the defense against both physical and psychological threats from adversaries creates a useful definition when looking at the ability of actors, whether foreign or domestic, to harm the United States, but it focuses heavily on the militarized aspect of security. Ullman (1983, 133) offers an alternate definition:

> A threat to national security is an action or a sequence of events that (1) threatens drastically and over a relatively brief span of time to degrade the quality of life for the inhabitants of a state, or (2) threatens significantly to narrow the range of policy choices available to the government of a state or to private, nongovernmental entities…within the state.

Not limiting security to just potential harm from nefarious actors, this definition encompasses the changing nature of security and how one must adjust defense capabilities to counter all issues facing American interests. Taking into account the ability of governmental and nongovernmental actors to counter these threats also focuses on a key point—an increasingly globalized world entails much more than the capabilities of just sovereign governments. Many more of the threats facing the United States come from loosely organized terrorist organizations or even rogue individuals.

Since the attacks on September 11, 2001, the Department of Homeland Security (DHS) and the U.S. intelligence have worked to adapt the national security apparatus to combat the changing nature of the threats facing the nation effectively. Focusing on harm coming from terrorist organizations and ill-meaning individuals, the government stressed

the importance of information gathering to mitigate the potential risk of attacks. President George W. Bush (2002, 30), in his National Security Paper following the September 11th attacks, emphasizes this need: "Intelligence—and how we use it—is our first line of defense against terrorists and the threat posed by hostile states." Wrapped up in this call for increased use of intelligence gathering, President Bush highlighted new methods and the need for a new framework to help secure the nation and its interests. Much of the work coming out of the Department of Homeland Security echoes President Bush's emphasis on intelligence gathering to better protect Americans. President Obama (2010; 3, 17) also stresses the ability of the US security apparatus to change in response to shifting global realities, adapting the infrastructure of the military and intelligence communities to manage the risks facing America.

With the need for a new way of thinking about national security, the Department of Homeland Security focuses on implementing a new risk management strategy to mitigate the potential harm from various threats facing the United States. Under this strategy, the Department of Homeland Security looks to implement a "systematic and analytical process to consider the likelihood that a threat will endanger an asset…and to identify actions that reduce the risk and mitigate the consequences of an attack" (Decker 2001, 3). In order to create an effective risk management strategy, the Department of considers a threat assessment of a potential attack, vulnerability measurements of potential targets, and the consequences of an attack (Decker 2001, 6; ASME 2006, 50; Masse et al. 2007, 9). These three variables combine to create the following equation when considering risk to national security and/or a specific national institution or installation:

Risk = Threat x Vulnerability x Consequences

In order to assess the level of risk facing America in different situations accurately, one must accurately assess all three variables on the right side of the equation.

The threat analysis remains the hardest to predict accurately and the most vital to preventing an assault on American interests, as it judges factors that the government cannot control. Quite simply, DHS defines a threat as "the likelihood of terrorist activity against a given asset" (Decker 2001, 8). The Department of Homeland Security's 2009 *Risk Analysis and Intelligence Communities Collaborative Framework* outlines the threat judgments needed for an effective risk assessment. The factors that play an important role in determining the seriousness of a threat are: the estimated likelihood of an attack, the type of attack, attacker type, frequency of the attacks, and the ability of the agents to work around the current security apparatus. While each situation merits its own examination of the five factors, no assessment can incorporate all information or prepare the United States or any installation for every plausible attack. With this uncertainty, it remains crucial to gather more information to create as accurate an estimate of a threat as possible. Even with these assessments, "threat is viewed as the most subjective component in the risk equation" (Baker et al. 2009, 21). Given the multiple threats facing American citizens and national infrastructure, this difficulty is understandable but calls for a greater need to scrutinize the individual factors contributing to an accurate overall assessment.

When looking at the Department of Homeland Security's threat assessment,[1] multiple variables play into a calculation of an attack against the United States. While

[1] See the Department of Homeland Security's 2009 *Risk Analysis and Intelligence Communities Collaborative Framework* (22) for the full table of factors contributing to threat assessments.

some of these factors may seem very specific to individual assets, many are worth highlighting in order to appreciate how one determines a threat to America. In regard to a likelihood of an attack, the time frame plays an important role, as immediacy raises the threat level. With different types of attacks, the target profile, particular domain/setting (land, air, sea, etc.) and technique used all play important roles—different assets require different prevention measures. For example, a suicide bombing is radically different from the use of a chemical agent. Looking at the attacker, a rogue individual poses a different threat from an organized terrorist network such as al-Qaeda. If attacks could happen more than once or right in succession, the frequency can raise the threat level above what a one-time attack may otherwise indicate. Lastly, looking at the ability of an individual to adapt to U.S. security measures raises greater concerns, as undermining the current security apparatus is hard to predict and leads to the need for further steps to be taken to protect American interests.

An alternative yet similar assessment of threats specific to terrorism looks at the weapons that could potentially be used in an attack, the nature of the adversary, and the vulnerable targets in order to create multiple scenarios that could threaten the security of the United States (Hall 2005, 5). Similar to the system used by DHS, this framework takes into account the type of attack (weapons), attacker type (adversary characterization), and the target type. However, this framework does not explicitly address the likelihood or frequency of an attack, rendering it not as useful as the one laid out by the Department of Homeland Security.

Examining the factors considered by the Department of Homeland Security and the other agencies responsible for creating accurate threat assessments displays the

necessity to combine a lot of qualitative information into an accurate and quantitative measure of risk facing the United States. Many distinctive fields of analysis exist within the United States government to deal with differing aspects of each threat assessment. A significant portion of the intelligence gathered comes in a qualitative form and multiple agencies work on the same project, but they do not always collaborate to create accurate analysis of specific threats as much as one might hope (Baker et al. 2009, 23-24). Combined with the institutional limitations of gathering information, no threat is the same as the next and adapting to each situation presents a great challenge, hence the need to bolster Homeland Security's ability to work with other agencies and streamline the threat assessment process (Baker et al. 2009, 26-27; Masse et al. 2007, 25).

Looking at the vulnerability of a possible attack, the focus shifts more to the prevention of terrorists' ability to damage U.S. infrastructure based on how susceptible various installations are to attack and what the cost of potential damage would be. A successful vulnerability calculation "identifies weaknesses in physical structures, personnel protection systems, processes, or other areas that may be exploited by terrorists and may suggest options to eliminate or mitigate those weaknesses" (Decker 2001, 10). The consequences of an attack align heavily with the vulnerability, but depend much more on the potential human, economic and symbolic costs of each threat.

Multiple variables play into both the vulnerability and potential consequence of a strike on U.S. targets: a population index, an economic index, and the level of infrastructure (Masse et al. 2007, 7-8). The population index includes the size of a population within a specific area as well as the population density and makeup—civilian or military personnel. Important economic indicators include the Gross Product of the

area in question, including how large it is and how importantly it plays into the country's GDP overall. Lastly, the level of infrastructure depends on how valuable the assets in question are, not only in a monetary sense but also in economic stability and symbolic terms. Unlike the threat assessment portion of the risk equation, measuring the vulnerability of an asset and potential consequences of a potential attack are much less subjective. Population size and existing infrastructure are tangible metrics that the Department of Homeland Security can obtain from the Census and other official government sources.

The seemingly simple yet quite complex equation dictating the risk management policy of the United States works for evaluating many different scenarios facing the nation, but some limitations to its implementation do exist by trying to quantify and multiply together the threat, vulnerability and potential consequences of an attack. As Cox (2008; 1754, 1759) points out, a threat is not always sufficiently defined and all three variables are at least partially subjective in nature, making it difficult to apply a standardized quantitative analysis across the board. In line with this conclusion, the framework does not necessarily work equally as well for all potential risks to national security. In fact, due to the threat assessment variable, the framework used by the Department of Homeland Security seems to work better for risk stemming from natural disaster than from terrorism (National Research Council 2010, 2-3). This difference in success may partly be due to the lack of situations to test the framework's effectiveness for terrorist attacks, whereas assessing the risk level of natural disasters (and other climate events that cannot be averted) is easier due to frequency and the inability of humans to prevent all natural disasters from occurring.

Overall, the Risk = Threat x Vulnerability x Consequence framework adopted by DHS allows for a way to measure the risk to national security. While some of the variables may rely on substantive judgments, an openly formulated and articulated system stands far above no agreed upon system at all. As the literature shows, assessing risk in any situation presents multiple difficulties, especially without a guarantee of perfect intelligence.

II. National Security vs. Privacy Framework

In order to examine the three case studies effectively, the following framework looks to combine and operationalize both national security and privacy to determine if and when the government violated privacy in the name of national security. To do this effectively, one first must look at the way the United States seeks information on individuals seen as potential threats to national security, starting with reasons for and the policy implications of the Foreign Intelligence Surveillance Act of 1978.

Foreign Intelligence Surveillance Act of 1978 (FISA)

Congress passed FISA in 1978 as a means to regulate executive authority in regards to surveillance of individuals for national security purposes. Prior to the passage of the Act, the use of warrantless wiretapping and surveillance to gather intelligence information in the name of protecting the United States started under President Franklin D. Roosevelt (Jaeger et al. 2003, 296). Citing the Constitution's empowerment of the executive and the oath of office to "defend the Constitution of the United States," presidents following FDR continued to expand the surveillance programs and capabilities

of the United States (US Const., art. II, sec. 1; Jaeger et al. 2003, 296; Blum 2009, 275). Moving past World War II, the FBI extended the surveillance program to monitor civil rights leaders, members of the Communist Party and other leftist organizations as the Cold War stoked insecurity at home. These expanded efforts, put in place under the mandate of protecting national security, most famously included surveillance of Martin Luther King Jr. and some of his supporters (Garrow et al. 2002, 80).

With the escalation of the Cold War and the increased use of surveillance techniques to gather larger amounts of information, Congress drafted and passed the Foreign Intelligence Surveillance Act of 1978 as a way to add structure and limitations to the actions of the FBI and other government agencies. Congress intended for the legislation to act as a "firewall between foreign and domestic intelligence gathering" (Osher 2002, 532). In this role, FISA looked to allow for the collection of foreign intelligence while still protecting the rights of American citizens outlined under the Fourth Amendment. Adding a framework for collection of data on potential threats, Congress relaxed the threshold of probable cause in regards to criminal activity seen in regular law enforcement purposes. To start surveillance on a US citizen or a person reasonably believed to reside within the physical borders of the country, "the government only needs to establish probable cause that the target is a member of a foreign terrorist group or an agent of a foreign power" (Blum 2009, 276). FISA created different thresholds for determining probable cause when law enforcement agents looked at criminal cases versus when intelligence officials only sought to gather information on potential foreign threats.

Despite the lower standard for establishing probable cause, the 1978 act protects the rights and privacy of US citizens by mandating that a request from an executive official to obtain a warrant under FISA must still meet certain requirements. First, the official must suspect the potential target as an agent of a foreign power, and if the target also lives in the United States or is a US citizen, "there must also be probable cause to believe that the person is 'knowingly' engaged in activities that 'involve or may involve a violation of the criminal statutes of the United States'" (Blum 2009, 276). Second, a warrant requires probable cause that the target in question uses or plans to use the means of communication that the government intends monitor (FISA 1978, Sec. 1804). Third, an intelligence agent or agency looking to conduct the surveillance must minimize the capture, collection and spread of information pertaining to US citizens that does not relate to foreign-intelligence (FISA 1978, Sec. 1805). Lastly, the Attorney General and a senior intelligence officer must approve the significance of the surveillance to national security and confirm that no other normal techniques of information gathering could reveal the same level of detail needed to protect Americans (Blum 2009, 277).

Under FISA, granted that the government official's request meets all of the above requirements, the Foreign Intelligence Surveillance Court (FISC) approves the warrant. If the surveillance targets a US citizen, the plan to monitor the communication of the targeted individual needs to include a "minimization plan to ensure that reasonable steps were taken to only intercept information related to the investigation" (Jaeger et al. 2003, 297). Thus, Congress sought to protect the rights of American citizens and prevent the unchecked wiretapping seen under previous administrations.

In addition to spelling out the procedural details of obtaining a foreign intelligence warrant, the legislation mentioned emergency surveillance options and the types of information gathering that does not require a FISA warrant. While the Act did seek to protect the rights of American citizens, "FISA never intended to require a warrant to capture overseas communications between two foreign nationals who do not have Fourth Amendment rights" (Blum 2009, 278). The original act also sought to distinguish between wireless communication and the use of fiber optic cable, complicating the process of intelligence gathering and making "arbitrary distinctions, based on technology, that are divorced from any privacy or reasonableness concerns of the Fourth Amendment" (Blum 2009, 279). So while the original FISA legislation of 1978 helped create a distinction between what the executive branch could and could not do in regards to surveillance of individuals both inside and outside of the United States, it did not create a perfect framework. As seen with the distinction between wireless and fiber optic communication, parts of the legislation created somewhat confusing standards for intelligence agencies to follow when targeting individuals.

Given the scope of the new regulations and the seemingly stringent requirements of FISC approval to obtain a FISA warrant, one might expect a tough approval process for surveillance targets. However, the opposite is true: "From its commencement in 1978 through 1999, the FISC has granted more than 11,883 warrants and denied none" (Bradley 2002, 479). Even after the passage of the Patriot Act (discussed below) and the increase in the number of applications for FISA warrants, up through 2006, the Foreign Intelligence Surveillance Court "had approved all but five out of over 17,000 requests" for a warrant (Blum 2009, 306). While this overwhelming approval of requests for

warrants may reflect increased pre-screening by executive officials, such high approval numbers points to the insignificance of the FISC (Blum 2009, 307). The Court relies on the information presented to it by the government and with this reliance, it cannot verify or deny the claims of a government agent until after the fact. Additionally, the FISC seemed too willing to provide for the necessary warrants even before the passage of the Patriot Act, which increased the government's ability to conduct foreign intelligence gathering.

The Framework

Given the historical background of intelligence gathering on individuals either inside or outside the United States, the tradeoff between national security and privacy becomes clearer. The table below illustrates four situations that can potentially occur when balancing national security and privacy. The three case studies presented will fall into the orange boxes below, falling into the categories: threat to security, violation of privacy; threat to security, no violation of privacy; no threat to security, violation of privacy. The last outcome: no threat to national security, no violation of privacy, is not a viable case study because, while government surveillance is certainly possible in such a situation, it would serve no purpose and it is hard to document that such an event ever occurred. Overall, a case where no threat to national security and no violation of privacy exist is not important to the overall study of balancing national security and privacy.

Framework		Imminent Threat to U.S. National Security	
		Yes	No
Data collection violates citizens' privacy	Yes	**Y, Y**	**Y, N**
	No	**N, Y**	N, N

In terms of national security, the threat assessment aspect of the risk management formula offers the crucial element to answer the question if government surveillance occurred when an imminent threat to American security existed. Using the Department of Homeland Security's framework laid out above, the estimated likelihood of an attack, the type of attack, attacker type, frequency of the attacks, and the ability of the agents to work around the current security apparatus all play into determining the threat to national security.

While the vulnerability and potential consequences of an attack are important for the overall level of risk, the threat factor determines the necessary prevention measures taken by the Department of Homeland Security and other government agencies in regard to intelligence gathering, thus forming the impetus for more surveillance. Because of the high variability and subjective nature of many threat assessments, the coverage of the following case studies will look to determine the level of the threat on a broad scale and balance it with the government's actions that may or may not have violated the privacy of one or more United States citizens.

Establishing an accurate and useful quantifiable threat assessment for each case study is impractical given the lack of information available to an individual researcher. Furthermore, since much of the stated governmental purpose for more surveillance deals with a larger scope than just one particular asset, the Risk = Threat x Vulnerability x Consequence formula remains unwieldy and obtuse. Vulnerability and Consequence assessments may provide some supporting evidence, but given the internal and easily quantifiable nature of the variables contributing to these parts of the equation, i.e. the government does not need to increase surveillance to determine a population size or

nature of the nation's infrastructure, the examination of the following case studies will not directly focus on them.

While the literature on privacy does not offer an agreed upon, explicitly defined right to privacy, the definitions offered do provide an effective way to measure whether an action violates an individual's privacy. Using Moor's (1990, 76) definition that "an individual or group has privacy in a situation if and only if in that situation the individual or group or information related to the individual or group is protected from intrusion, observation, and surveillance by others," the following examination of three case studies will measure when and to what degree acts of surveillance violate one's privacy. The concept of zones of privacy allow for a notion of when one can protect personal information from outside intrusion, deciding what one wishes to disclose. In terms of governmental surveillance, the Fourth Amendment protects Americans from "unwarranted search and seizure," and while this does not constitute an expressed legal right to privacy, it bolsters the philosophical principle that violating privacy is not justified unless the good coming from it outweighs the harm caused (Moor 1997, 32). The strength of using the notion of zones of privacy to determine if a violation occurs is the ability to take public opinion into account, as an assessment of the harm caused depends largely on how a specific culture defines privacy (Moor 1990, 77).

The framework outlined above relies upon a binary assessment of both national security and privacy when in reality a gray area may exist when looking at what one constitutes as private or what the security apparatus might classify as a threat. However, in order to test my hypothesis that the balance between national security and privacy fundamentally shifted towards security while unduly infringing upon the privacy of

individual citizens effectively, the binary classification is necessary. Even with the definitive yes or no classification for each variable, the framework can shed some light on the shifting calculus of the national security agencies and the implications for the safety and privacy of American citizens.

Case Studies

Applying the above framework, the next three sections examine different case studies to showcase the intelligence efforts of the United States government in its recent history. The studies outlined seek to display the three grids of the boxes laid out in the framework: National security interest, no privacy invasion; no national security interest, privacy invasion; national security interest, privacy invasion. First, the case of Zacarias Moussaoui, a French national detained weeks before the attacks on September 11, 2001, provides an example when there was a credible threat to national security but no privacy intrusion. The unwarranted eavesdropping under the Terrorist Surveillance Program authorized by President Bush in 2002 fulfills the no national security interest and privacy invasion case study. Lastly, the NSA programs—namely Prism and the Bulk Telephony Metadata Collection Program—first revealed by Edward Snowden in May 2013, present evidence of a case where a potential national security interest and threat existed but privacy was also invaded. Given the recent press surrounding it and the dilemma that it causes as it raises the issue of possibly rebalancing security and civil liberties in the 21st century, the information shared by Edward Snowden requires greater examination.

III. National Security Interest, No Invasion of Privacy: The Case of Zacarias Moussaoui

Background

Zacarias Moussaoui, a French national, entered the United States on a 90-day Visa early in 2001. He paid $6,300 for flight lessons, enrolling in a Pan Am flight school in Minnesota (Mueller 2001). However, once in school, Moussaoui expressed interest in only learning how to fly large commercial jets, despite limited experience with a single engine aircraft. His interest in learning to fly a plane without bothering with training on how to take off and land caused instructors and staff of the flight school to suspect something was amiss. The flight school alerted the FBI, with the instructor going as far to say, "Do you realize that a 747 loaded with fuel can be used as a bomb?" (qtd. in Shenon 2001). The agency opened an investigation of the French national, suspecting him as a possible international terrorist. Subsequently, the INS arrested Moussaoui on August 16, 2001 due to his expired Visa, with the Minneapolis FBI field office playing a key role in ensuring his capture because of the concerns expressed by the flight instructors (Rowley 2002). Following the arrest of Moussaoui, French intelligence officials alerted U.S. intelligence services with further information linking Moussaoui to known terrorists in Europe and the Middle East (BBC News 2006).

While in custody, Moussaoui refused to allow authorities to search his personal belongings, and the FBI Minneapolis field office as well as FBI headquarters did not feel that enough evidence existed to obtain either the proper criminal or FISA warrant to gain access to Moussaoui's computer and other possessions (9/11 Report: Joint Congressional Inquiry 2003, 22). The FBI decided not to push for a criminal warrant because the agency headquarters felt the case lacked strong enough probable cause to search Moussaoui's

possessions. Hours after the terrorist attacks on September 11th, officials obtained such a warrant without even including the French intelligence reports. Agent Rowley, a legal officer at the Minneapolis office, felt frustrated with the hesitancy of her superiors to pursue a warrant before the attacks, stating:

> To say then, as has been iterated numerous times, that probable cause did not exist until after the disasterous [*sic*] event occurred, is really to acknowledge that the missing piece of probable cause was only the FBI's (FBIHQ's) failure to appreciate that such an event could occur (Rowley 2002).

After a complete investigation of Moussaoui and his subsequent indictment in December of 2001, a distinct pattern emerged between his actions and those of the 19 terrorists who hijacked the flights on 9/11. Robert Mueller, the director of the FBI, issued a press release following the indictment of Moussaoui outlining the similarities between the French national and one or more of the known hijackers. Researching the use of GPS equipment, crop dusting and purchasing videos of the flight deck from a store in Ohio all linked Moussaoui to known hijackers (Rowley 2002; Mueller 2001).

In addition to the concerns of the flight school instructors, the French intelligence and suspicions by the Minneapolis field agents, the Phoenix divisional branch of the FBI alerted headquarters on June 10th, specifically the Radical Fundamentalism Unit, of the possibility of Al-Qaeda to try and train terrorists in U.S. flight schools for future terrorist operations (9/11 Report: Joint Congressional Inquiry 2003, 20). The Radical Fundamentalism Unit oversaw the Moussaoui operation as well, but no information reached the Minneapolis agents regarding the Phoenix communication, despite their voiced concerns about Moussaoui (Rowley 2002). In addition, the Radical Fundamentalism Unit overlooked the signs from the information gained in the Phoenix Communication and French intelligence that might have provided even more of a reason

to press for a warrant against Moussaoui. As an individual, he fit the profile outlined in the concerns mentioned by the Phoenix office as well as having known connections to terrorists.

Thus an opportunity to do more in order to protect national security existed. While Robert Mueller remained skeptical after the attacks if any information gained before 9/11 could have prevented them from occurring, Agent Rowley emphatically disputes this sentiment from the FBI Director: "It's very doubtful that the full scope of the tragedy could have been prevented; it's at least possible we could have gotten lucky and uncovered one or two more of the terrorists in flight training prior to September 11th," (Rowley 2002). While all the questions regarding what might have occurred if the FBI aggressively pursued the Phoenix Communication and searched Moussaoui's computer for contacts and other valuable information remain speculative, a chance exists that the agency's actions might have helped to lessen the damage and destruction wrought on September 11, 2001. That said, a further analysis of the national security and privacy implications of the handling of the Moussaoui case allows for a deeper understanding of how the United States' security and intelligence agencies operated in the weeks leading up to the worst terrorist attack experienced in the country's history.

National Security

A clear national security interest existed leading up to the attacks on September 11, 2001. Despite the tragedy experienced due to the terrorist attacks, the relevant question remains whether or not Zacarias Moussaoui presented a compelling threat to the nation to merit further investigation or if the agency handled his case correctly, treating him just as an individual who overstayed a temporary visa? Given the FBI's level of

information before the attacks, Moussaoui constituted a legitimate threat to the United States worth further investigation.

Of the five elements mentioned by the Department of Homeland Security that factor into a threat assessment (the estimated likelihood of an attack, the type of attack, attacker type, frequency of the attacks and the ability of the agents to work around the current security apparatus), the ability of the agents to work around the security mechanisms of the United States presents the most glaring problem, as the attacks occurred, in part, because of intelligence failures. However, even without the gift of hindsight, enough of a threat existed for increased investigation into Moussaoui and other leads related to potential terrorist threats against the United States.

The likelihood of the attack due to Moussaoui and information revealed by the Phoenix Communication remained low given the intelligence of the United States in the summer of 2001. Moussaoui sat in a jail cell at the time of the attacks and did not present an imminent threat to the United States. FBI headquarters viewed him as an individual to deport, not one that acted as an international terrorist (Rowley 2002).

The Phoenix Electronic Communication, sent to members of the Radical Fundamentalist Unit, the Osama Bin Laden Unit and the International Terrorism Unit in New York, outlined a theory highlighting the potential for increased al-Qaeda use of flight schools in the United States as training grounds for future terrorist operations in the aviation industry. Ken Williamson, the agent who authored the report, marked it as "routine," the lowest priority level in FBI communications, since he felt the increase in possible al-Qaeda connected individuals enrolling in flight schools in Arizona and potentially around the United States deserved further examination, but he lacked the tools

to conduct the necessary analysis (U.S. Dept. of Justice 2004). By marking it at as a routine communication, Williamson did not specify an imminent threat to United States security. Thus, based solely on the Phoenix electronic communication, the likelihood of an attack, given the known information, remained low. However, combined with the suspicions of Moussaoui's intentions in enrolling in flight school, the potential existed for greater harm against the United States. This assertion does not mean that perfect communication would have or even could have prevented the attacks, but it does mean that by linking pieces together, the FBI could have identified a greater threat to national security in the summer of 2001. Forging greater security connections between field offices and headquarters as well as with other intelligence agencies increased the potential capture or prevention of one or more of the other terrorists involved on September 11th. As Rowley (2002) notes, even if the whole attack could not have been prevented, detaining a couple more of the terrorists or heightening security levels at airports could have saved lives.

In the case of Moussaoui, the attack type and profile of potential attackers involved much of what actually occurred on September 11th. He possessed known connections to radical elements in London and other locations; he paid cash for flight lessons; he expressed interest in flying a commercial plane without bothering to learn how to take off or land the plane; he took martial arts classes, and he even stated after the attacks that he was part of a "plot to fly a Boeing 747 into the White House" (BBC News 2006). While evidence in hindsight cannot prove the threat level of an individual, the FBI possessed enough information about Moussaoui as an individual and about the potential

threat of terrorists looking to enroll into aviation schools for future operations to delve deeper into his case and certainly to search Moussaoui's possessions.

Similarly, as seen with the other threat indicators, the lack of effective communication between different branches of the FBI and with other intelligence agencies prevented an accurate understanding of the threat facing the aviation industry as a whole. In some respects, this lack of communication and cooperation within and between intelligence agencies represents the September 11th attackers' ability to work around the current security apparatus of the United States. However, this line of reasoning does not mean that terrorists explicitly intended to exploit the deficiencies of the United States. Instead, they benefited from the lapses in communication present in the U.S. surveillance system, changing the approach for the FBI and other national agencies moving forward into the 21st century.

Privacy

Looking at privacy in this case presents a straightforward narrative. The United States government did not violate Zacarias Moussaoui's privacy. The FBI refrained from searching any of his possessions before a Federal judge granted a warrant after the 9/11 attacks occurred. Not only do the actions of the FBI comply with a legal justification to privacy as seen in the 4th Amendment, the FBI does not violate Moussaoui's theoretical right to privacy. Relying on Moor's (1990, 76) definition that "an individual or group has privacy in a situation if and only if in that situation the individual or group or information related to the individual or group is protected from intrusion, observation, and surveillance by others," Moussaoui retains his privacy, even after his capture, since the FBI did not search any of his personal belongings (Moor 1990, 76). While Rowley felt

that probable cause for a criminal and/or a FISA warrant existed, FBI headquarters disagreed with her assessment, ending the possibility of searching Moussaoui's belongings until agents obtained a warrant after the terrorist attacks (Rowley 2002). If the FBI had obtained a warrant before 9/11, that document would have justified an invasion of Moussaoui's privacy not only because of the legal authority to do so but also because the moral benefit outweighs the harm caused by the searching of Moussaoui's belongings.

Discussion

The case of Zacarias Moussaoui details a failure on the part of the U.S. intelligence to communicate effectively within and between agencies as well as a lack of detailed analysis of terrorist activity within the United States. The agency needed more aggressive means of dealing with Moussaoui and the information uncovered by the Phoenix Communication. The links Moussaoui had to other terrorists and the implications of the Phoenix communication presented a threat to the United States. Even though he sat in a jail cell, the French national represented only a small part of a much larger effort to attack the United States. In fact, public sentiment felt that he was the 20th hijacker after the attack, even though Khalid Sheikh Mohammed, the man credited with planning the attacks, says that Moussaoui was not part of the 9/11 plot at all but rather a second wave of attacks against other U.S. targets to occur after the strike on the World Trade Centers (BBC News 2006).

While the FBI identified Moussaoui as a potential threat to the United States, they refused to pursue his connections and failed to link together the threats to the aviation industry and the United States as a whole. It is impossible to say specifically what

searching Moussaoui's possessions might have turned up in regards to preventing 9/11, but infringing on his privacy was justified and necessary in this particular case. Disparities between the official 9/11 commission report and the account given by Agent Rowley in the Minneapolis Field Office show that, at the very least, a lack of communication and clear direction led to a gross oversight in intelligence operations. Given Moussaoui's particular background and the level of attention given to his actions, the FBI failed by not investigating further or reaching out to other security agencies to try and contextualize the threat as part of a larger issue for the safety of American citizens. The fragmented coordination between FBI headquarters, the agencies' field offices and other intelligence services suggests large gaps in American surveillance. Many of the changes implemented post-9/11 looked to counter this deficiency and manage surveillance in a more expansive way, shifting the calculus surrounding the way the American government approached national security.

IV. No National Security Threat, Invasion of Privacy: Bush's Terrorist Surveillance Program (TSP)

Background

Following the attacks of September 11th, the Federal government reprioritized the way it approached intelligence collection in attempt to prevent anything on the magnitude of the terrorist attacks from ever happening again. The passage of the USA Patriot Act in 2002 marked the major legislative initiative to give the executive branch and intelligence agencies greater power to conduct surveillance on potential foreign terrorist threats by significantly altering the Foreign Intelligence Surveillance Act of 1978.

Despite the increased surveillance abilities that Congress granted to the Oval Office, President Bush issued an executive order authorizing the NSA to proceed with more domestic surveillance, marking a shift from solely collecting foreign intelligence data to targeting more communications within the United States. The program sought to increase the power of the NSA to monitor connections between Americans and foreigners, a turn from the agency's previous commitment to avoid the collection of data on American citizens (Risen and Lichtblau 2005). The *New York Times* broke the story, asserting:

> The eavesdropping program grew out of concerns after the Sept. 11 attacks that the nation's intelligence agencies were not poised to deal effectively with the new threat of Al Qaeda and that they were handcuffed by legal and bureaucratic restrictions better suited to peacetime than war, according to officials. In response, President Bush significantly eased limits on American intelligence and law enforcement agencies and the military (Risen and Lichtblau 2005).

The administration argued for greater freedom from FISC oversight, asserting that the current system limited the ability to act in a timely manner to respond to threats against the U.S. (Sanger 2005). To fully comprehend the extent of the administration's decision to act outside of the parameters outlined in FISA, an examination of the national security implications and privacy implications of the President's actions will follow a brief overview of the law and the subsequent amendments under the Patriot Act.

USA Patriot Act

Following the attacks of September 11, 2001, Congress sought to further empower intelligence agencies and the Executive Branch overall to combat the threat of terrorism. Formally known as the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (from here on referred to as the Patriot Act), the seminal bill passed in the aftermath of the attacks

expands the FISA framework to help facilitate easier surveillance of threats to the United States. These reforms include extending the period of emergency surveillance before requiring a warrant from 24 to 72 hours, increasing the number of judges on the Foreign Intelligence Surveillance Court from seven to eleven, providing for the authorization of roving wiretaps, allowing the surveillance period to increase from 90 to 120 days and explicitly empowering officials collect the content of voicemails and emails (Blum 2009, 280; Jaeger et al. 2003, 298-301; Bradley 2002, 485-491). While the act included many other subsequent procedural alterations of the original FISA text to address weaknesses in the surveillance structure in the United States, the two main changes came in the new level of requirements for surveillance approval and the intelligence relationship founded on secrecy between the government and the private sector.

As previously discussed, the purpose of surveillance up until the passage of the Patriot Act was to gather foreign intelligence on agents of foreign powers (FISA 1978, Sec. 1804). The Patriot Act changed the standard, stating that gathering foreign intelligence only needed to be a "significant purpose" of the surveillance (USA Patriot Act 2001, Sec. 218). This change lowered the threshold of the intelligence operations of the United States' agencies and allowed for greater leeway when deciding whom to target. While higher standards remained in place for monitoring the communications of American citizens, the change in language opened the door for looser regulations for intercepting communications. The wording and thus the interpretation of FISA, became much more vague for executive officials. The Act allows for more FISC approval of warrant requests as the "change erases much of the distinction between the standards necessary to receive a court order for wiretaps or searches for FISA and for criminal

investigations, allowing many FISA investigations to occur that simply would have been disallowed prior to the Patriot Act" (Jaeger et al. 2003, 299). The overwhelming number of cases approved by the FISC both prior to and following the passage of the Patriot Act shows how obtaining court approval was not originally tough and continued to be fairly easy. Whether the overwhelming approval of applicants was due to extensive preparation and precaution by the executive branch or the relative ease of the FISC process, the Patriot Act made the process for obtaining a FISA warrant that much easier.

The second major change presented by the Patriot Act revolved around the way the government requested information from private companies regarding the subscribers' electronic communications. Section 215 of the Patriot Act dictates that once the FBI or any other federal agency requests information from an individual or organization, that person or organization cannot reveal to anyone else the purpose of the investigation or even its existence (USA Patriot Act 2001, Sec. 215). While seemingly innocuous, this mandate plays an important role in the relationship fostered between surveillance agencies and private communications companies regarding the phone records of millions of clients. The case of the NSA and Verizon revealed in the spring of 2013 (to be discussed in my third case study) acts as a prime example of such a relationship.

Given all of this expansion of the abilities of executive agencies to collect information on foreigners and increasingly on American citizens, the Patriot Act presented the American public with a big step towards more executive authority in conducting surveillance on foreigners as well as American citizens. However, President Bush decided to go even further, disregarding FISA and the Patriot Act all together.

Terrorist Surveillance Program (TSP) and Subsequent Legislation

Despite the expanded powers under the Patriot Act, the Bush administration chose to conduct warrantless surveillance programs through an executive order. The president tasked the NSA with intercepting communications going into or out of the country when a possibility existed that at least one of the parties had ties to al-Qaeda (Risen and Lichtblau 2005; Blum 2009, 283). President Bush decided to avoid the FISA process by relying on the NSA program to circumvent the warrant approval process presented by the FISC. In admitting to the existence of the secret surveillance program, President Bush cited the Authorization for Use of Military Force Against Terrorists (AUMF) as empowering him "consistent with U.S. law and the Constitution, to intercept the international communications of people with known links to Al Qaeda and related terrorist organizations" (qtd. in Sanger 2005). However, as Levy (2006, 38) points out, "In voting for the AUMF, members of Congress surely did not intend to make compliance with FISA optional." Authorizing military force against terrorists does not equate to disobeying surveillance laws regarding American citizens.

When the *New York Times* first broke the story on the Terrorist Surveillance Program, the NSA monitored the communications of up to 500 US citizens as well as a couple of thousand foreign at one time (Risen and Lichtblau 2005). However, while the program circumvented the legal framework to prevent attacks against Americans in place under FISA, the effectiveness of the top-secret program remains up for debate. Administration officials interviewed at the time cited the case of Iyman Faris, a trucker with connections to al-Qaeda who was involved in a plot to bring down the Brooklyn Bridge with blowtorches, as evidence of the success of the warrantless program (Risen

and Lichtblau 2005). In addition, General Michael Hayden, the Director of the National Security Agency at the time, stated: "I can say unequivocally that we have gotten information through this program that would not otherwise have been available" (qtd. in Bergman et al. 2006). Yet, multiple sources call into question the actual role that the secret NSA program played in the capture of Faris, stating that many other avenues of surveillance and investigation played larger parts in stopping what never amounted to much of a threat to begin with (Bergman et al. 2006; Howe 2006; Kalven 2006).

In addition, while General Hayden issued a firm backing of TSP, the FBI did not share the same unequivocal support of the program as providing useful information that led to successful actions taken against potential threats. Robert Mueller, the director of the FBI at the time, stated his reservations regarding the legality and practicality of the program given the FISA provisions and Patriot Act (Bergman et al. 2006). Other FBI sources who worked closely with the NSA on the surveillance program displayed frustration at the ineffectiveness of the program and the burden placed on the Bureau to chase a lot dead end searches; one FBI source stated, “After you get a thousand [telephone] numbers and not one is turning up anything, you get some frustration” (qtd. in Bergman et al. 2006). The two disparate viewpoints on the effectiveness of the warrantless program from two major American intelligence agencies call into question the useful of the program. While someone who lacks security clearance—and knowledge of all of the pertinent information regarding the individuals targeted—cannot speak to all of the evidence presented by the Terrorist Surveillance Program, the frustration of Director Mueller at the questionable legality of the program and the inefficient and

ineffective nature of the administration's warrantless surveillance efforts speaks to the overall uncertainty surrounding President Bush's decision to bypass FISA.

Following the *New York Times* uncovering the warrantless surveillance program in 2005, Congress passed the Protect America Act of 2007 and the FISA Amendments Act of 2008 as a way to amend the legal framework in place for intelligence collection further. The impetus for the subsequent legislation came from some of the concerns that the Bush administration raised when justifying its circumvention of FISA after 9/11 (Blum 2009, 295). The Protect America Act expanded further on the Patriot Act, effectively legalizing the warrantless wiretapping program for a six-month period by empowering the Attorney General and Director of National Intelligence to authorize communication between a foreigner outside of the country and a citizen within U.S. borders if the individual in focus is "reasonably believed" to be outside of the country (Risen 2007). In addition, the expansion allowed the warrantless collection of foreign-to-foreign communication that runs through the United States while traveling between two individuals (Protect America Act 2007, Sec. 105B). While the procedures remained subject to review by the Foreign Intelligence Surveillance Court after the fact, the expanded powers of executive branch officials allowed for much more leniency in the government's effort to collect foreign intelligence data.

Additionally, the FISA Amendments Act of 2008 cements a lot of the changes first enacted in 2007 by providing for even more executive branch authority in the surveillance of individuals both domestically and internationally. Section 702 of the act gives the Attorney General and Director of National Intelligence the ability to authorize surveillance on individual outside the country for up to one year in order to gather foreign

intelligence if the purpose of the surveillance is not reverse targeting[2] of US citizens, if both officials certify the necessity of the surveillance for foreign intelligence purposes, if the Attorney General outlines a set of guidelines to ensure proper surveillance of individuals, and lastly if Congress and the FISC review the procedural guidelines and certifications of the executive officials periodically (FISA Amendments Act 2008, Sec. 702, 1861). These amendments to the original 1978 law allow for greater freedom for executive officials to monitor the electronic surveillance of various targets but also places more emphasis on Congressional and FISC review of the Attorney General's certification and the procedural process of the NSA in its surveillance of individuals. Removing the warrant requirement for searches when the target is not a U.S. citizen or reasonably believed to be in the country helps smooth out the collection process as "the warrant is a poorly designed means for balancing the security and liberty interests involved in counterterrorist surveillance" (Posner 2008, 255). Even if a warrant does make adapting in time to counterterrorist threats harder, the implications that the Terrorist Surveillance Program and the subsequent legislation have for the balance between national security and privacy require greater examination.

National Security

Assessing one specific threat to national security emerging from the warrantless surveillance under the Bush administration presents a formidable task, not because of a large number of threats but because of the broad scope of actions taken by the administration to gather information. Fundamentally, the shift in intelligence embodied

[2] Reverse Targeting refers to the surveillance of an individual reasonably believed to be outside of the US in order to gather more information on a person that is within the country's borders (see FISA Amendments Act of 2008 Section 1808 on Congressional oversight for the procedures in place to prevent NSA overstep).

by both the Patriot Act and the Terrorist Surveillance Program seeks to prevent many more threats than just responding to them. With September 11th catching the intelligence agencies off-guard, the security apparatus of the United States sought much more data to anticipate the likelihood of an attack, the attack type, attacker profile, frequency of attacks and the ability of potential threats to work around the existing security structures of the country. In effect, US agencies sought greater information to prevent acts of terrorism from occurring again at any level.

Since the largely unanticipated tragedy on September 11, 2001, the American government saw the likelihood of an attack as something hard to predict and something much more preventable with more information coming in about the threat that individuals, whether part of an international terrorist organization or acting as a rogue agents, presented. The declaration of a War on Terror by President Bush and the Authorization for Use of Military Force Against Terrorists enacted by Congress shows a shift in the way the Federal government viewed the likelihood of attacks against the United States. Given the surprise nature of the terrorist attacks, the likelihood of a further attack was unknown, but the administration did not want to find itself facing another attack with the same devastating effects. Thus, the chance of an attack right after September 11, 2001 remained unknown, but given the sophistication and planning that went into hijacking three planes, the administration saw the uncertainty as unnerving and something that required as much information as possible (Sanger 2005). In addition, the President stated his actions were legal, given the authorization of the AUMF by Congress, even though many saw the authorization of force not allowing for the unwarranted spying on United States citizens (Levy 2006, 38).

The specific attack type for a threat assessment also remains hazy given the lack of specificity surrounding the surveillance program. Trying to prevent all future attacks provides an extremely broad scope for assessing the threat to the United States at the time. Certainly the vulnerability exposed by the hijackers put the Federal government on higher alert, but the desire to stop all possible attacks does not provide a credible threat type or signify a specific type of attack that a security agency can effectively protect against without severely infringing upon the rights of American citizens. The profile of the attacks on the World Trade Centers does not automatically translate to other potential future attacks, though one could argue that they did allow insight into the types of individuals that might try and harm the United States.

When looking at the profile of possible attackers, the government tried to combat the enemy embodied by the terrorist attacks on September 11, 2001. President Bush explicitly said the program aimed to monitor those individuals with links to al-Qaeda (Sanger 2005; Risen and Lichtblau 2005). Individuals whom the NSA suspected to form connections with al-Qaeda were the explicit targets of the surveillance, but any individual who communicated internationally could fall under government surveillance. Thus the profile of possible attackers extended to those persons with potential links to terrorists overseas, something that the decentralization of terrorist networks after the attacks helped to facilitate (O'Brien 2011). The NSA suspected those targeted of maintaining links to al-Qaeda, but given the lack of evidence to support the claims, the FBI came up empty-handed when following through with the requests for information submitted by the NSA (Bergman et al. 2006). Even with the profile of the attacker known as an individual with at least loose affiliations to al-Qaeda who sought to hurt Americans either inside or

outside of the country, the targeting of individuals that actually occurred did not match these profiles, with thousands of searches not uncovering information regarding potential threats against the United States.

The frequency of attacks and the ability to work around the security infrastructure of the United States remained vague with the Terrorist Surveillance Program, but in the wake of a national tragedy, the administration feared more attacks that the security agencies could not foresee. Some officials worried that the 9/11 attacks marked the beginning of increased targeting of American citizens as a "new global jihadist movement" emerged in the opening years of the 21st century, allowing for the decentralization and growth of terrorist networks globally (O'Brien 2011). The lack of concrete evidence did not dissuade officials from this position, as the memory of September 11th only served as a reminder that terrorists possessed the capability to work around the security structures in place in the United States. Even if exact profiles of potential attackers or the exact type of attack remained unknown, terrorists clearly thought about the current security structures and the vulnerabilities in those systems when looking at potential ways to attack the United States.

Overall, despite the successful terrorist attempts on September 11th, the uncertainty of the threats facing the United States after the attacks caused the Bush administration to take drastic steps to ensure that terrorists could not catch the country off guard again. The broad collection of the content of communications from American citizens to suspected terrorists overseas sought to shift the balance of knowledge regarding terrorism to allow for more security. However, the warrantless targeting of individuals based solely on some communication patterns did not uncover any additional

information from intelligence obtained through other means, such as prisoner interrogation or FISA-backed surveillance.

The NSA touted the arrest of Iyman Faris as a success story of the warrantless surveillance program, neutralizing a terrorist threat against the United States; yet further examination of the threat shows that not only did other sources besides TSP help uncover the plot against the Brooklyn Bridge, the threat to the bridge never amounted to much to begin with. Faris, a naturalized citizen and truck driver from Ohio, attended an al-Qaeda training camp in 2000, scouted targets for the terrorist organization, and admitted to plotting to attack the Brooklyn Bridge by attempting to cut the suspension cables that maintained the integrity of the structure (U.S. Dept. of Justice 2003). However, Faris ultimately concluded that the plot to disable the bridge required too much risk and did not seem likely to succeed, given the security surrounding the bridge and the difficulty of obtaining the tools required to follow through with the plot (Howe 2006). In addition, the evidence used against Faris did not require information gathered by the Terrorist Surveillance Program, as U.S. intelligence already knew about the potential threat from other sources such as interrogations (Bergman et al. 2006). Multiple FBI sources confirm the lack of evidence that Faris presented a serious threat to the U.S. or that the Terrorist Surveillance Program revealed any imminent threats facing the country. One official, when asked about TSP, stated that “there were no imminent plots - not inside the United States” that the unwarranted surveillance uncovered, and when the FBI did find small amounts of information, other sources had already produced the same information (Bergman et al. 2006).

So the threat level, both uncovered by the larger surveillance program and the one determined specifically for Iyman Faris, did not show an imminent threat to the United States. Despite the comments of President Bush and General Hayden praising the effectiveness of the Terrorist Surveillance Program, the threats actually revealed by warrantless monitoring of the international communications of up to a thousand Americans did not produce any substantial or new information to better the security of the country. However the program did raise questions regarding the privacy of Americans when communicating with each other and foreigners.

Privacy

The secrecy of the Bush Administration in expanding the surveillance capabilities of the United States raises many privacy concerns, especially given the timing of the Patriot Act and the potential the administration had to support even more changes in the legislation to allow for the surveillance officials desired without breaking the law. Leaving the legal aspect aside and only looking at the privacy of American citizens, the conduct of the Bush Administration makes it hard to say that a reasonable, innocent American would not view her privacy violated if the Terrorist Surveillance Program happened to target her. One's private communications falls into a zone of privacy, allowing one to expect that no one else besides the intended recipient will receive, hear or read that communication. While electronic surveillance in general intrudes into this zone of privacy, the administration's decision to conduct the monitoring of communication without the proper clearance from the FISC further undermines trust in presidential authority.

Looking at Moor's (1990, 76) definition, one sees that the unwarranted surveillance violates the condition of privacy as described as "an individual or group has privacy in a situation if and only if in that situation the individual or group or information related to the individual or group is protected from intrusion, observation, and surveillance by others." Any American citizen who communicated with someone abroad exposed himself to unwarranted surveillance and potential intrusion from the NSA and the FBI under the Terrorist Surveillance Program. While the President and General Hayden both cited the use of the program to monitor potentially dangerous individuals, the frustration expressed by the FBI officials conducting the surveillance gives insight into the lack of true threats and the intrusion into the private communications of American citizens. With multiple dead ends and a lot of searches leading nowhere, the surveillance of some individuals seemed unnecessary and unrelated to the security of the United States (Bergman et al. 2006). Without using a warrant, the Bush administration undercut the legislative expansion of FISA. Beyond the legal justification, the way in which one acquires information is just as important as the information gathered (DeCew 1986, 152; Moor 1990, 76). Disregarding the framework set in place, the Bush administration deceived Congress and the American people, both who thought that the Patriot Act expanded FISA to the necessary point for effective U.S. surveillance.

Even though the Terrorist Surveillance Program did not come up with strong evidence of terrorist activity in the United States or reveal any imminent threats against Americans, a retrospective view of the program makes it much easier to state that the program was unnecessarily intrusive. Looking at Moor's definition, privacy encompasses a lot of an individual's actions and an invasion of privacy may be needed at some points

to protect the welfare of others. Moor (1990, 32) states this ethical argument in his Justification of Exceptions Principle: "A breach of a private situation is justified if and only if there is a great likelihood that the harm caused by the disclosure will be so much less than the harm prevented that an impartial person would permit breach in this and in morally similar situations." Bush justified the intrusion into the private spheres of people's lives in order to prevent future harm against other U.S. citizens.

Given the lack of evidence revealed by the program and the recent expansion of the Patriot Act to allow for greater flexibility when conducting foreign and domestic surveillance, the justification for the breach in the privacy of Americans remains fairly weak. Furthermore, as mentioned briefly above, the use of unwarranted searches on U.S. citizens undermined public trust in executive authority, as most citizens opposed the program once it was revealed (Diamond and Jackson 2006). Without the legal support or public support, the justification for the Terrorist Surveillance Program did not outweigh the harm to the civil liberties of Americans.

Discussion

The Bush administration argued that unwarranted surveillance provided the most efficient and timely way to ensure the protection of American interests. However, in doing so, the administration overreacted and unduly sacrificed the privacy of thousands of Americans in order to pursue more information that marginally increased the security of the United States. The desire to gain more information about potential enemies was well intended, but the vague threat level did not merit the circumvention of the FISA framework and the already expanded surveillance capabilities under the Patriot Act. The Patriot Act allowed for emergency surveillance options, granting the Bush

Administration the ability to conduct the searches needed in order to pursue information about those who wished to harm the United States. Furthermore, the record of FISA warrants approval shows the low threshold that government officials needed to reach in order to conduct surveillance (Bradley 2002, 479). While Bush argued strictly for efficiency and the unnecessary regulations accompanying FISA, at least by requiring a warrant, the legislation forced government officials to do the proper due diligence in the authorization process and examine the facts on hand before blindly conducting surveillance operations against American citizens and other potential targets.

The evidence that FBI agents did not find new and useful information regarding potential threats to the United States from the NSA requests for unwarranted monitoring and collection of content data on American citizens communicating with individuals abroad suggests the ineffectiveness and unnecessary nature of the Terrorist Surveillance Program. As the Iyman Faris case demonstrates, the threats to the United States did not require the executive action outside the scope of FISA. Granted, while the above discussion on the threat level to national security relies upon the lack of evidence stemming from the FBI searches of NSA leads, that is not to say that a true threat might not exist that could call for surveillance. However, the emergency procedures built into FISA and the Patriot Act allowed for the legal approach to address this new threat.

Thus not only did the Terrorist Surveillance Program invade the privacy of American citizens, it did not serve a legitimate national security purpose in terms of its ability to identify and address potential threats against the country. This analysis does not downplay the possibility of a threat to the United States, but it does suggest an overstep by the Bush Administration in its attempts to protect American security. However, as

seen with the Protect American Act of 2007 and the FISA Amendments Act of 2008, legislative actions sought to cement the increased executive surveillance powers permanently by bringing them under FISA control and allowing for more unwarranted presidential action. Despite the secrecy on the part of the administration, Congress allowed the unwarranted infringement in privacy to become more normal in the security actions of the United States. One sees elements of this trend with the revelations surrounding other secret activities of the NSA, namely the Bulk Telephony Metadata Collection Program and Prism programs.

V. National Security Threat, Invasion of Privacy: Bulk Telephony Metadata Collection and PRISM

Background

The insights into NSA actions presented by Edward Snowden's release of information to *The Guardian* in May of 2013 allowed a glimpse into the many national security programs enacted since the Terrorist Surveillance Program that further placed privacy on the line when looking to defend the national security of the United States. As a former employee of the CIA and a private contractor for the NSA, Snowden felt that the U.S. government sacrificed the rights of American citizens with the mass collection and analysis of telephone and electronic metadata (Greenwald and Poitras 2013). While Snowden released documents about various surveillance programs run in the United States and continues to reveal other information about the NSA, this case study focuses on the NSA's Bulk Telephony Metadata Collection Program and the PRISM program, highlighting two of Snowden's revelations and narrowing the focus of the analysis to two of the programs that deal the most with balancing individual privacy and national

security.[3] Two court cases, *Klayman v. Obama*, No. 13-0851 WL 6571596 (D.D.C. Dec. 16, 2013) and *ACLU v. Clapper*, Civ. No. 13-3994 WHP (S.D.N.Y. Dec. 27, 2013), grapple with the constitutionality of metadata collection—the former approving an injunction to stop the collection of the plaintiff's metadata, while the latter declares the collection of metadata constitutional. These cases help guide the discussion in regards to balancing national security and privacy with the Bulk Telephony Metadata and PRISM programs.

These surveillance programs go much farther than prior surveillance activities, both in the scope and depth of the collection and analysis of American data. The Bulk Telephony Metadata Collection Program expands upon the framework laid out by the Terrorist Surveillance Program, the Protect America Act of 2007, and the FISA Amendments Act of 2008. With the collection of metadata, the NSA relies upon Section 702 of the 2008 legislation and Section 215 of the Patriot Act in order to request information from private telephone companies to access subscriber metadata, aggregate this data in one place, and conduct targeted searches to analyze potential terrorist threats (Greenwald 2013). The surveillance program looks to detect possible terrorist numbers contacting individuals within the United States, communications from people within America to suspected terrorist organizations abroad and communications within the borders of the U.S. While the NSA does not collect the content of telephone calls, "the numbers of both parties on a call are handed over, as is location data, call duration, unique identifiers, and the time and duration of all calls" (Greenwald 2013). With the

[3] See Al Jazeera's Timeline (http://america.aljazeera.com/topics/topic/organization/nsa.html) on Snowden's release of information for details and pertinent news articles on all the government surveillance programs, including "upstream" data collection from fiber-optic cables, searches of online chat rooms, the NSA's pressure on companies to reveal encryption codes, estimates of the amount of metadata collected and surveillance of foreign leaders, to mention a few.

collection and analysis of this data, dubbed “business records,” as consistent with Section 215 of the Patriot Act, on the subscribers to Verizon and other large service providers, the NSA created a “counterterrorism program” to link communications between suspected terrorists and other potentially dangerous individuals (13-0851 D.D.C. 15). The ability to gather the large swaths of metadata on American citizens allows for the retroactive analysis (up to five years) of potential threats to the security of the United States.

However, government officials cannot sift blindly through the metadata of American citizens. In order to search the collected metadata without a warrant, NSA agents must only intend on using the results for counterterrorism purposes and utilize certain “identifiers,” such as a number of a suspected terrorist, that contain "reasonable, articulable suspicion" that they are connected to a terrorist organization (Bradbury 2013, 2-3). With each identifier, the NSA can then search three connections or “hops” away from this initial query, with the first “hop” being the identifiers that come up as a result of the initial query, the second “hop” consisting of the identifiers linked to any of the connections made by the first “hop” and so on (Bradbury 2013, 3; No. 13-0851 D.D.C. 18). Given the expansive nature of the searches, with the potential for an exponential number of identifiers related to the first query, a lot of telephone numbers can be covered by these searches. Only 300 identifiers were approved for use in 2012, yet once these searches are made for the whole database, the NSA can look to connect different pieces of information to determine communication patterns by further searching the results with queries that do not strictly follow the “reasonable, articulable suspicion” threshold (No. 13-0851 D.D.C. 18). The retroactive ability of the NSA to search metadata records from up to five years ago further enhances the agency’s ability to detect such patterns.

Since Edward Snowden first revealed the government's request for information from Verizon Wireless and other telephone companies, a Washington D.C. Circuit Judge and a New York Circuit Judge split in their decisions regarding the Bulk Telephony Metadata Collection Program within two weeks of each other. The first case, *Klayman v. Obama*, granted an injunction for the plaintiffs, individual subscribers to Verizon's services, against the metadata collection on the grounds that the privacy concerns of American citizens outweighs the governmental interest. District Judge Richard J. Leon, in deciding the case, quite effectively lays out the question of privacy as:

> whether [the] plaintiffs have a reasonable expectation of privacy that is violated when the Government indiscriminately collects their telephony metadata along with the metadata of hundreds of millions of other citizens without any particularized suspicion of wrongdoing, retains all of that metadata for five years, and then queries, analyzes, and investigates that data without prior judicial approval of the investigative targets (No. 13-0851 D.D.C. 43).

Framing the issue in this way allows one to see the debate on privacy revolving around two separate areas: the collection of the metadata and the separate analysis of the information once gathered.

In *ACLU v. Clapper*, New York District Judge William H. Pauley III does not approve an injunction for the ACLU, relying on a past Supreme Court case dealing with the collection of data and the security responsibilities of the U.S government. By issuing this ruling, the judge finds that individuals cannot claim a reasonable expectation of privacy when using telephone service providers. *Klayman* uses the same evidence to argue for the opposite conclusion, forcing a side-by-side comparison of the two decisions in order to fully comprehend the privacy and national security issues at stake.

Both decisions look at *Smith v. Maryland, 442 U.S. 735 (1979)* to decide on what an individual can reasonably expect in terms of privacy when he uses a private telephone

provider. In the case, the Court rules that an individual cannot reasonably expect privacy when submitting information to a telephone company because he already forfeits his privacy to the telephone company when using its services. *ACLU v. Clapper* relies upon *Smith v. Maryland* as guidance for metadata collection, stating that the clients of Verizon and other telephone companies cannot expect privacy because, using the service to dial another number, individuals already waive any reasonable standard of privacy by giving a third party access to their telephone metadata. *Klayman v. Obama* acknowledges the precedent set by the *Smith v. Maryland* decision but ultimately concludes that the two instances of privacy are not synonymous. In *Smith v. Maryland,* the individual in question is a potential thief, and law enforcement officers placed a short-term pen register on his phone in order to help with a criminal investigation. The forfeiture of privacy only occurred once police officers installed the pen register, whereas the bulk collection of metadata allows for continued aggregation and retroactive analysis for data of all telephone users for up to five years. *Klayman v. Obama* veers from the *Smith v. Maryland* decision due to collection of data for up to five years and the catchall nature of the surveillance program, as compared to the pen register targeted at one individual. The reason and relationship between the government and private companies differs completely for each circumstance. Furthermore, the massive expansion seen in the use of mobile phone technology and the type and amount of information gleaned from the metadata of individuals since the Court ruled in *Smith v. Maryland* make the cases almost completely separate. One came in a criminal investigation from law enforcement personnel while the other came from a national security agency in a systematic effort to connect suspected terrorist organizations to other potential threats to the United States.

Judge Pauley addresses three concerns mentioned by the ACLU in its request for an injunction from the New York District Court: the vast collection of metadata, the analysis of metadata through individual queries, and the possibility of these two actions of having a "chilling effect" on future communications (Civ. No. 13-3994 S.D.N.Y 14). Given the precedent set in *Smith v. Maryland*, the aggregation of metadata does not infringe on an individual's rights because individuals do not own their metadata when choosing to use the services of communications companies. On a statutory level, the case claims that only Verizon or other service providers maintain the right to challenge the government's collection practices under Section 215. In terms of individual privacy, the Bulk Telephony Metadata Program employs various minimization procedures in order to limit the exposure of a particular individual to governmental intrusion. No names or financial information goes into the database, the querying of metadata requires preapproved identifiers, and the NSA only concentrates on connections three "hops" away from the initial search. In addition, Pauley argues that the fear of the collection and analysis of this data as infringing on the associational rights of the ACLU lacks standing due to its speculative nature and failure to present sufficient evidence that the program imposed substantial burdens on the Plaintiff's First Amendment rights.[4]

To wrap up his decision on the bulk collection of telephone metadata, Judge Pauley cites the efficacy of metadata collection in preventing terrorist attacks on the United States. The decision mentions the NSA thwarting multiple potential terrorist threats against the United States since the initial implementation of the program in 2006.

[4] See *Clapper v. Amnesty International,* 133 S.Ct. 1138 (2013) for further discussion of the insufficient evidence against individuals' First Amendment rights in regards to the NSA's collection of metadata. However, the Supreme Court heard this case before Edward Snowden released documentation on the Bulk Telephony Metadata Collection Program.

The court opinion places the metadata collection as one tool available to the government in seeking to stop terrorist plots. Combined with other investigations and surveillance programs, the metadata helped to establish connections made by al-Qaeda to other potential threats against the U.S., the nation's interests, and the safety of its allies. Namely, the decision lists the early workings of a plan to bomb the New York Stock Exchange, a request for help making explosives for another potential bomb threat in New York, and a plot to attack a Danish Newspaper responsible for publishing the image of Mohammed (Civ. No. 13-3994 S.D.N.Y 48-49). Given the release of information on these terrorist connections, the lack of any evidence suggesting that the NSA used the database for anything besides counterterrorism operations, and the reminder of the tragedies of September 11th, the New York District Court finds the program lawful in advancing a genuine governmental interest.

Judge Leon's treatment of the same issues arrives at the opposite conclusion in *Klayman v. Obama*, though this opinion focuses mostly on the first two concerns mentioned in the *ACLU* case—the aggregation of data and retroactive analysis by NSA agents—not addressing the potential "chilling" effects of a large data collection program. First, unlike the Supreme Court's claim in *Clapper v. Amnesty International,* 133 S.Ct. 1138 (2013), the collection of metadata is not speculative. The explicit goal of the program is to aggregate metadata to conduct counterterrorism operations in the United States. Without the large compilation of data on the contacts between those with reasonable ties to a terrorist organization, the NSA could not safely assert that it assessed all possible avenues of risk facing the United States in regards to foreign terrorist attacks. In effect, the program integrally depends on amassing everything before conducting

searches. If the scope of the data collection did not extend to the levels that it did, the subsequent queries of the data would not produce a reliable result.

While both *Klayman v. Obama* and *ACLU v. Clapper* both acknowledge the initial intent of the program, the decision in *Klayman v. Obama* states that individuals do possess the constitutional ability to challenge the collection of their metadata records by the NSA. In his decision, Judge Leon states that the government contradicts itself in its push to dismiss the call for an injunction. The stated purpose of the Bulk Telephony Metadata Collection Program is to amass all of the records to create a searchable database for surveillance purposes, but the government tries to suggest that the collection of data may be incomplete so that no certainty exists to say that the NSA collected the metadata of the plaintiff (13-0851 D.D.C. 38). More importantly, the query of the metadata also presents privacy problems, as the government must search through every number in the database for connections to the initial query. In addition, the surveillance program continually updates the information about the metadata from service providers, adding daily new information for analysis. While the information gathered from a search of a individual's metadata in 1979, when *Smith v. Maryland* was decided, provided a small glimpse of one's communication patterns, the information gathering now provides "a vibrant and constantly updating picture of the person's life" (13-0851 D.D.C. 54). Not only does this changing nature of communication allow for the decision to deviate from previous views of metadata, it lays the foundation for an argument demonstrating the NSA searches are unreasonable intrusions upon individuals' privacy.

In determining the legality of the Bulk Telephony Metadata Collection Program, Judge Leon finds that, based on the burden of proof needed in determining the

government's interest to violate privacy without a warrant and the record of efficacy, the program is not constitutional. Past cases dealing with the government conducting surveillance without a warrant focus on certain situations that constitute a government "special need" for the surveillance, while "daily searches of virtually every American citizen without any particularized suspicion" suggests an overly broad intrusion on an individual's privacy (13-0851 D.D.C. 58). Additionally, the intended purpose of the specific program is not just the identification of potential terrorist threats but instead the identification of such threats faster than other tools at the disposal of the NSA and other governmental agencies. NSA officials stress the need of the metadata program to quickly pinpoint and thwart terrorist plots against Americans, but no evidence of this urgency or expedited process shows in examples presented to Congress or the American public (13-0851 D.D.C. 61). For each of the cases listed as evidence of the successful surveillance operations in *ACLU v. Clapper,* the use of metadata plays either a complementary role to other surveillance practices in identifying potential threats and/or reveals activities that, while linked to known terrorist organizations, do not present imminent threats to the security of the United States.[5] Thus the decision finds that the "special needs" threshold for warrantless searches does not outweigh the infringement on citizens' reasonable expectations of privacy.

In addition to shedding light on the Bulk Telephony Metadata Collection Program, Edward Snowden detailed the NSA use of Section 702 of the FISA Amendments Act of 2008 to authorize the implementation and use of PRISM, a

[5] See *Klayman v. Obama*, No. 13-0851 WL 6571596 (D.D.C. Dec. 16, 2013) for further discussion on the government's intended surveillance purposes regarding the Bulk Telephony Metadata Collection Program. Even with the opportunity to "present additional, potentially classified evidence *in camera,*" the Government chose not to (62). The reliance on other surveillance methods and lack of urgency challenges the stated efficacy of the metadata program.

surveillance program which looks to access information on the electronic communications of individual subscribers to U.S. Internet companies. PRISM involves NSA "collection directly from the servers of…U.S. Service Providers" (Ball 2013). This collection under PRISM remains separate from the "upstream" gathering of electronic metadata from fiber-optic cables and other data infrastructures (Ball 2013; Washington Post 2013). The PRISM program acts much the same for electronic metadata as the bulk collection of telephone metadata does with major telephone service providers except that it allows for the collection of certain content in electronic communications, such as email, chat rooms, cloud stored files, etc. (Sottek and Kopstein 2013). The collection of data extends to nine major Internet service providers, including Microsoft, Google, Yahoo, and Facebook (Lee 2013). Under Section 702, the Director of National Intelligence and the Attorney General can approve the targeted surveillance of an individual for up to a year as long as the individual is reasonably believed to be outside of the United States. In order to conduct the surveillance in line with the FISA Amendments Act of 2008, the NSA must use "identifiers" approved by officials and cannot intentionally target United States citizens, purely domestic communications or any individual believed to be located in the United States, though the agency may collect information on Americans as long as foreign intelligence remains the primary purpose of surveillance and not reverse targeting of Americans (Bradbury 2013, 10). With the sufficient query of approved identifiers, the NSA can request metadata and content information from the Internet service providers, who must then turn over the requested data.

The technology companies implicated by the release of documents denied their involvement in giving the NSA unfettered access to their servers. Executives at Google,

Yahoo and Facebook all opposed the notion that the NSA possesses the ability to sift through its servers at will (Lee 2013, Sottek and Kopstein 2013). However, these companies do cooperate with NSA queries under Section 215 of the Patriot Act, which allows the agency to request business records for foreign intelligence purposes. Thus some ambiguity exists when leaked NSA documents detail "direct access" to the servers of these companies (Ball 2013). While the law requires companies to release the specified information, the exact nature of the relationship between the public and private sectors remains murky under the PRISM program as well as with the other clandestine surveillance programs of the NSA.

Following the revelations by Edward Snowden and the announcements of the decisions in *Klayman v. Obama* and *ACLU v. Clapper*, President Obama has altered the minimization procedures that the NSA must follow when conducting the aggregation and querying of telephony metadata. Instead of NSA-approved query identifiers, with an exception of a national emergency, a court must find "reasonable, articulable suspicion that the selection term is associated with an approved international terrorist organization" to enable the NSA to search the aggregation of metadata (Obama 2014; Clapper 2014). In addition, these searches only extend to identifiers two connections or "hops" away from the initial query (Obama 2014; Clapper 2014). President Obama, while still feeling the metadata program necessary, cut the ability of the NSA to search as much American information.

On March 27, 2014, President Obama took an additional step in proposing an end to the bulk collection of metadata by the NSA and outlined a plan for keeping American data strictly in the hands of service providers until requested by the government

following approval by the FISA Court (Ackerman 2014). If the FISC grants approval for a particular search, the mechanical query of data would work in much the same way as it does presently, the difference being that the government does not aggregate the metadata itself. The government identifies a target number with "reasonable articulable suspicion"—as determined by the FISA Court—and then telephone service providers would have to turn over data on that phone number and the numbers that are two hops away (Ackerman 2014). The proposal still needs Congressional approval, with differing versions pending in the House and Senate, but the announcement by the administration does show some progress towards a serious reevaluation of the way the NSA conducts its surveillance activities. However, since the programs are still in operation, along with other NSA surveillance operations, a review of the programs as they stand now begs two questions. How much of a difference will these alterations make in regards to national security if the approval of search terms demands judicial approval? Additionally, do these changes to the NSA's actions alter the privacy implications of the original program? Answering both of these questions does not prove to be a simple process but first relies upon an examination of the threat and privacy assessments for the Bulk Telephony Metadata Collection and PRISM programs.

National Security

The two court cases examined above lay out the fundamental national security interests of the NSA when looking to collect telephone and electronic metadata from American citizens and other subscribers to U.S. telephone and Internet companies, but applying the Department of Homeland Security's threat assessment framework allows for

a more explicit look at the national security interests at stake with the surveillance programs. As used to examine the two other case studies, the five factors playing into determining a threat to the United States are the estimated likelihood of an attack, the type of attack, attacker type, frequency of the attacks, and the ability of the agents to work around the current security apparatus (Baker 2009, 22). Similar to the analysis presented in the case study on the Terrorist Surveillance Program under President George W. Bush, identifying one specific threat or threat level to the security of the United States remains difficult given the large scope of the programs in their attempts to prevent any potential terrorist attacks. Even with the difficulties of applying the threat assessment criteria, the factors playing into the determination of a threat provide a way to categorize the surveillance activities to compare with the two previous case studies and other governmental actions.

The Bulk Telephony Metadata Collection Program and PRISM present an almost comprehensive approach to dealing with threats to the security of the United States, much more encompassing than the Terrorist Surveillance Program. The government states its intentions of aggregating all of the telephone metadata to ensure thorough analysis of all possible avenues to prevent known terrorist organizations from harming Americans (13-0851 D.D.C. 15). While the likelihood of one particular attack remains hard to state with any certainty when looking at such a vast collection of metadata, the scope of information, if utilized correctly, allows for a greater ability of the government to foresee attacks and prevent them. The intention of the surveillance programs is to counter any subsequent attack after September 11th, with the government placing even greater emphasis on national security.

The specific type of attack and frequency of attack remain sufficiently vague when looking at the impetus for increased surveillance, but the attacker profile is relatively clear, if not readily identifiable. The collection of metadata focuses on preventing the attacks of terrorist, with no discrimination between attack types, seeking to act quickly to stop threats against the U.S., yet both surveillance programs only target foreign individuals. The NSA may collect American metadata but only in hopes of gaining more information on foreign threats to national security. These targeting procedures do not restrict the NSA from responding to perceived threats from inside the United States or from an American citizen abroad, but they do require a FISA warrant to pursue further surveillance on an individual (Bradbury 2013, 3). The warrantless programs focus only on foreign threats with connections to identifiers related to known terrorist organizations. In this regard, the attacker profile contains the potential to present a decently high threat to the security of the United States. Moving beyond the initial query term, depending on where an individual number or identifier falls on the communication chain in relation to the suspected terrorist connection, a large range exists for the potential for an identifier to raise concern regarding the nation's security. A telephone number that exists one link (or hop) away in a communication chain presents a greater likelihood of a significant threat than one three hops away. However, even given the necessary minimization procedures in place to ensure the tailoring of query terms to items relevant for foreign intelligence, the ability of the NSA to access connections three hops (now two under Obama's new guidelines) exponentially increases the number of contacts linked to the initial search. Thus, while the NSA may be targeting foreign individuals with connections to known terrorist organizations, the metadata collection

also includes many other people as well, making it harder to distinguish with certainty between potential threats and innocent telephone and Internet users.

Despite the difficulties, the most noticeable aspect of determining the threat level facing the United States is the ability of government to prevent individuals from working around the security infrastructure already in place. Section 702 of the FISA Amendment Act sought to cut the possibility of increasing terrorist activity, a distinct possibility given not only the 9/11 attacks but also general fears of surveillance officials that the 21st century could bring an increased terrorist targeting of American citizens (O'Brien 2011). The collection of metadata from telephone and Internet service companies allows the NSA to aggregate data in a way not possible to that point, even under the Terrorist Surveillance program. By collecting and searching vast amounts of information, the NSA certainly cuts the possibility of terrorists working around the national security apparatus, at least in the agency's ability to identify communications between known terrorist organizations and other potential threats to the United States.

Evidence of specific threats to the United States mitigated due specifically to the vast aggregation of metadata and PRISM remains mixed given the many programs at the disposal of the NSA to detect threats to the national security and the lack of information open to the public. The Director of the NSA, General Keith Alexander, stated in a House Intelligence Committee hearing that surveillance operations thwarted "potential terrorist events over 50 times since 9/11" (qtd. in Savage 2013). While the specifics of such plots are not general information for the public, FBI Deputy Director Sean Joyce revealed a couple of cases for Congressional hearings, namely a thwarted plot against the New York Stock Exchange as well individuals transferring money to terrorists in Yemen (Savage

2013; Civ. No. 13-3994 S.D.N.Y 49). While Joyce stated the need for all current NSA activities to ensure national security, these examples do not show the level of urgency or imminent threat of attack that the agency relies upon as justification for their expansive nature (Savage 2013; 13-0851 D.D.C. 62). Not only did other sources provide much of the information in the discoveries of these threats, the threats themselves were not imminent or all that serious. In the case of the plot to bomb the New York Stock Exchange, the government found the participants guilty of sending money to al-Qaeda but did not charge them with any domestic crimes for the potential bombing (Savage 2013). Given that the government lists other examples but keeps them confidential, it remains impossible to examine each of the known situations, but the existing evidence shows that the national security threat posed by the uncovered plots was low and did not include imminent threats, the primary reason for such a expansive surveillance program to begin with.

Privacy

Even though two district judges came to different conclusions on the legal challenges to PRISM and the Bulk Telephony Metadata Collection Program, a more theoretical approach to privacy allows for a slightly adjusted method when looking at the programs revealed by Edward Snowden. Again, using Moor's (1990, 76) definition of the condition of privacy existing when "an individual or group has privacy in a situation if and only if in that situation the individual or group or information related to the individual or group is protected from intrusion, observation, and surveillance by others" one finds that both surveillance programs violate individuals' privacy. However, as mentioned in the discussion of the Terrorist Surveillance Program, situations do arise

when a breach of one's privacy is ethically permissible. Moor's (1997, 32) Justification Principle provides a nice foundation to view the collection of telephone and electronic metadata, as it takes into account what an average individual would see as a breach in privacy and if the harm mitigated by the violation of privacy outweighs its cost.

To measure the costs of the metadata and content collection and analysis fully, both via telephone and over the Internet, one must separate the collection of the data and the subsequent queries submitted by NSA agents. First, the NSA's collection of metadata or electronic content does violate a reasonable expectation of one's privacy. It is extreme for a person to expect privacy in a public sphere, but the contextual integrity of privacy matters, i.e. just because one chooses to share certain information with another person does not mean that she accepts that anyone may access that information (Nissenbaum 1998; 573, 584). An individual voluntarily giving a telephone service provider his metadata allows for a reasonable expectation that the release of that information will not stray outside of that relationship. While the government may (or may not) have the legal authority to aggregate individuals' metadata, it does intrude on the public's privacy. Contextual integrity holds so much importance when looking at privacy claims because the type and level of information that one decides to share with a certain party allows for a unique relationship with that person or organization (Introna 1997). A customer of Verizon or Google or any other telephone or Internet service provider, is not trying to form a unique social relationship with that firm, but he or she expects the information shared with the company to stay private.

Second, once the government gathers the information, the subsequent query of the metadata further violates an individual's privacy. Even though the program does not

explicitly collect the names or financial information of the persons whose metadata falls into one of the categories created by the approved identifiers, the extent of metadata and rapid and continuous update of the information in the database allows intelligence officials to create "an entire mosaic—a vibrant…picture of the person's life" (13-0851 D.D.C. 54). Given that Americans heavily rely on mobile phones for so much today, a search of the metadata and content of telephone and electronic communications allows the government access to much more of an individual's live than he may think is reasonable. Furthermore, the search of information allows for up to a five-year retrospective analysis of information, allowing for the government a large swath of data to analyze. Certain minimization procedures dictate that the NSA may not specifically target a U.S. citizen, but that does not preclude it from collecting data on Americans at all. Any linkage with an identifier gives the NSA access. Until President Obama's reform of the program in January of 2014, the ability of the NSA to query data three connections away from an initial identifier allowed for a large collection of American metadata. The government has not released information on the amount of information collected on American citizens, information released by Edward Snowden shows that in the month prior to his leak of NSA surveillance information, the government compiled nearly three billion pieces of data on Americans (Greenwald and MacAskill 2013). While it remains difficult to show how much of the country that number covers, it is definitely large enough to show a collection of a non-insignificant amount of American metadata.

Weighing whether or not the benefit of breach of privacy by the government outweighs its costs remains particularly difficult given the lack of information on the plots that the programs detected. Given that no terrorist organization has attacked the

United States since September 11th, one can argue that the NSA and other surveillance agencies have done their job in ensuring the safety of American citizens. General Alexander claims that surveillance actions prevented more than 50 potential terrorist threats since 9/11, a statistic that suggests that the violation of Americans' privacy might be worth a guarantee of national safety (Savage 2013). However, judging the degree of the benefit of the surveillance programs in question remains difficult given other tools available to the NSA, ones that do not necessarily require the sacrifice of Americans' privacy. To discuss the justification of the surveillance programs, one needs a sense for the success of the Bulk Telephony Metadata Collection Program and PRISM. Yet, the opinions in *Klayman v. Obama* and *ACLU v. Clapper* differ on the overall success rate. Without showing a need for the two programs to move quickly to counter terrorist threats, the examples cited by the government show much more routine data collection. If the government does not use these programs to collect useful information faster than other methods available, then the invasion of Americans' privacy does not meet the requirements of the Justification Principle.

Discussion

Both PRISM and the Bulk Telephony Metadata Collection Program grew out of the memory of September 11th and continued to build upon the Terrorist Surveillance Program. Each program expands the ability of the NSA to monitor and track potential terrorist actions against the United States, but they also greatly encroach on Americans' reasonable expectations of privacy. A definitive analysis of the effectiveness of these two programs as compared to other surveillance actions conducted by the NSA remains difficult given the lack of concrete threat assessments. The government claims the

necessity for the large aggregation of data to allow for expediency in preventing terrorism, but the cases it cites as evidence of the effective prevention did not require fast action to respond to an imminent threat. The government does not provide convincing evidence that the gains from the bulk collection of American data outweigh the costs of the violation of privacy. Security agencies may hesitate to reveal all the information about their surveillance programs in order to more effectively counter potential terrorists. The element of surprise certainly helps the government stop the terrorists' ability to work around the existing surveillance infrastructure. However, given the sacrifice of U.S. citizens' privacy and the lack of any evidence to support the stated purpose of both the Bulk Telephony Metadata Collection Program and PRISM of allowing for much needed expediency to combat threats to national security, the government should be able to provide some tangible justification for these drastic actions.

Thus, without more information from the NSA on the 50 terrorist actions stopped by these dragnet programs, it remains hard to categorize the threat level facing the United States. Taking the government at its word when it declares the necessity of the surveillance programs allows one to conclude that credible threats exist that require greater government action to prevent them. However, whether or not these actions require the extensive violation of Americans' privacy remains impossible to tell without more information. If other NSA programs do indeed allow for the effective countering of the threats against the United States and no great need of urgency exists, then the dragnet programs are not justified. Much of this depends on the nature of the threats to the United States. These threats are largely uncertain, making it harder to say that credible and tangible threats against the United States existed every time the government claimed they

did. Instead of definitively saying an imminent threat to security definitely exists to warrant these dragnet surveillance programs, as originally hypothesized, the evidence shows that the threat level remains uncertain in this case. In itself, this fact implies that the actions of the United States may greatly sacrifice the privacy of American citizens for an unwarranted level of security.

VI. Conclusion

These three case studies display a trend in the last decade of American surveillance: less privacy in the name of ensuring more security. Clearly, the modifications to the Foreign Intelligence Surveillance Act of 1978 in the Patriot Act, the Protect America Act of 2007, and the FISA Amendments Act of 2008 all seek to give the government more legal authority to conduct surveillance on potential foreign threats to the United States. While these pieces of legislation outline a framework for more executive action, the case study of the Terrorist Surveillance Program shows that the government went even farther than the Patriot Act authorized. In their national security strategies, both President Bush (2002) and President Obama (2010) emphasized the need to gather more information about potential threats to the U.S. in the wake of September 11th. The Bulk Telephony Metadata Collection Program and PRISM, while only two of the many programs run by the NSA, represent the current trend in surveillance activities to prevent terrorist attacks. Uncertain threats facing the United States have led to gathering even more information in order to eliminate as many surprises facing the security of the country.

Starting with the case of Zacarias Moussaoui and working chronologically up to the present, the path taken by security agencies seems relatively obvious. September 11th

caught the U.S. off guard and exposed flaws in the nation's security apparatus. The government stated that the lack of information regarding terrorist threats provided justification for expanding the surveillance activities of the United States. The Terrorist Surveillance Program worked outside of the legal limitations to provide greater surveillance, and the Protect America Act of 2007 as well as the FISA Amendments Act of 2008 basically legalized the warrantless searches by the Bush Administration, providing for even greater surveillance operations. The Bulk Telephony Metadata Collection Program and PRISM are two of the outgrowths of this progression.

Edward Snowden's revealing of these programs to the world highlights the need for Americans to continue assessing the way in which we view our own privacy in regards to our national security. If Snowden had not revealed the extent to which the NSA aggregates and analyzes American telephone and electronic metadata, the populous still would not know the actions taken by the government in the name of protecting U.S. interests. If we did not know about these programs, would the government be committing unreasonable surveillance actions in the name of our security without our knowledge? That depends on the threat level facing Americans. No one disagrees that maintaining national security is one of the most important duties of the United States government. The problem arises when the government chooses to sacrifice the privacy of its citizens in such a comprehensive way to counter unknown threats. However, without knowing an exact threat level, one cannot state with certainty what an appropriate amount of surveillance actually entails or if the actions taken by the government help protect us from attack. Without certainty, the temptation exists to let more surveillance compensate for the knowledge gap to favor security over the privacy of American citizens.

President Obama's presidential bid and his actions in office illustrate the way in which the government since 9/11 errs on the side of caution when looking to implement national security policy. As a senator and then a candidate for the Oval Office, Obama criticized the surveillance activities of the Bush administration, stating that the warrantless Terrorist Surveillance Program presented a "false choice between the liberties we cherish and the security we provide" (Baker 2014). Yet, once in office, President Obama continued and even expanded the NSA programs started under Bush, demonstrating the fact that once in charge, he did not want to preside over the nation's security at the time of another terrorist attack, let alone one on the magnitude of September 11th. With the move from Senator to President, from legislator to administrator, Obama shed his ability to remain outside of policy implementation and inherited the responsibility to protect the nation from attack. With his new role, he did exactly what he criticized Bush for doing—choosing security over civil liberties. Assuming the role of commander in chief weighs more heavily on a leader than theoretical concepts of liberty, a mentality described by Professor William Marshall as "the not on my watch mentality" (Marshall 2014). The expansion of surveillance programs demonstrates the executive's propensity to favor issues of security over that of privacy.

This trend is concerning. Uncertainty cannot justify sacrificing everything in the name of national security. The government is not, and never should be, omniscient and omnipotent. A risk of terrorist attacks against Americans will always exist. For that matter, risk in general will always exist. No one wants to suffer from a terrorist attack, just as no one wishes to be the victim of violent crime, but that does not empower the

government unduly to sacrifice the rights of its citizens to minimize uncertainty. A comparison to an Orwellian "big brother" presence over-dramatizes the surveillance conducted by the government, but it acts as a fair warning that, in an age of digital expansion, we are losing some of our privacy in the name of national security, and that's just with the programs we know about.

If the executive acts in protecting our national security, it remains up the legislature and the judicial system to ensure the protection of American privacy, especially as technological expansions increase the surveillance capabilities of the United States. Legislation has been proposed to place greater limits on the NSA's ability to collect and analyze metadata, but, as seen with the Protect America Act of 2007 and the FISA Amendments Act of 2008, legislation in response to executive overreach can also allow security agencies the legal justification to expand surveillance operations. The judiciary lags even farther behind when it comes to addressing technological shifts and the role of surveillance in the lives of American citizens. The last Supreme Court case on government electronic surveillance, *City of Ontario v. Quon*, 558 U.S. 1090 (2010), dealt with the use of electronic pagers as the technological innovation requiring judicial review. As noted by Judge Leonie Brinkema, the almost archaic nature of electronic pagers illustrates the 20-year lag the Court experiences when dealing with issues of technological progress and surveillance (Marshall 2014). It is unreasonable to expect the Court or the legislature to predict all advancements in technology and the subsequent implications for government surveillance actions, but given the rapid development of this ability to access more information at such great ease, no counterweight exists to President's sense of responsibility to protect against the worst case scenario.

We cannot, in good faith, fully blame the President for trying to protect us from threats to our security, but we also cannot rely solely on him or her to weigh effectively abstract notions of privacy with the possibility of harm to American lives. If the judiciary continues to lag, public demands for change may provide the best way to counter the responsibility felt by the executive. A new balance must be struck. Polling data from the Pew Center highlights that public opinion has soured towards the bulk collection programs over the time since Snowden's revelation. In July 2013, just after Snowden initially released the documents on the activities of the NSA, 50 percent of Americans approved the collection and analysis of metadata by the NSA and 44 percent disapproved; these numbers have declined since then, with 40 percent approving the collection and 53 percent disapproving as of January 2014 (Pew Research 2014). Even with a significant decline in approval, the program retains a large amount of support from Americans. Yet, 85 percent of Americans seek to increase their online privacy or "mask their digital footprints" when using the Internet (Rainie 2013). Individuals recognize the normative values of privacy, even if they remain split on the role of the government in conducting surveillance activities.

Ultimately, the answer might not actually lie in deciding between more national security or more privacy. These two things are not necessarily mutually exclusive when it comes to policy implementation. As privacy advocate Ginger McCall notes, technology can allow for privacy protection while helping to curb potential threats to national security (Marshall 2014). New, less revealing body scanners employed by the Transportation Security Agency at airports provide an example of these changes and the role public protest can play in curbing invasions of privacy while still allowing for

effective surveillance. The balance sought comes from the need of Americans to re-evaluate the way they view privacy in the age of big data and cloud technology. With more transparency, the government can facilitate this conversation. President Obama took an important step with his proposal to end the metadata aggregation by the government, but more can be done. Instead of sacrificing privacy for greater national security, the American people can demand a re-evaluation of the government's role in protecting the security and rights of its citizenry.

Work Cited

Ackerman, Spencer. 2014. "Obama formally proposes end to NSA's collection of telephone data." *The Guardian*, March 27. Last accessed at: http://www.theguardian.com/world/2014/mar/27/obama-proposes-end-nsa-bulk-data-collection on April 13, 2014.

ACLU v. Clapper, Civ. No. 13-3994 WHP (S.D.N.Y. Dec. 27, 2013).

ASME Innovative Technologies Institute, LLC. 2006. *Risk Analysis and Management for Critical Asset Protection: The Framework* (2nd ed.) Washington, DC.

Baker, John, Meghan Wool, Adrian Smith, Jerome Kahan, Clarke Ansel, Philip Hammar, … and Rosemary Lark. 2009. "Risk Analysis and Intelligence Communities Collaborative Framework." *Homeland Security Institute*, last accessed at http://wikileaks.org/gifiles/attach/33/33666_Risk-Intel%20Collaboration%20Final%20Report.pdf on March 31, 2014.

Baker, Peter. 2014. "Obama's Path From Critic to Overseer of Spying." *New York Times*, January 15. Last accessed at: http://www.nytimes.com/2014/01/16/us/obamas-path-from-critic-to-defender-of-spying.html on April 14, 2014.

Ball, James. 2013. "NSA's Prism surveillance program: how it works and what it can do." *The Guardian*, June 8. Last accessed at http://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google on March 31, 2014.

BBC News. 2006. "Profile: Zacarias Moussaoui." *BBC News,* April 25. Last accessed at http://news.bbc.co.uk/2/hi/americas/4471245.stm on March 31, 2014.

Bergman, Lowell, Eric Lichtblau, Scott Shane, and Don Van Natta Jr. 2006. "Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends." *New York Times*, January 17. Last accessed at http://www.nytimes.com/2006/01/17/politics/17spy.html?pagewanted=all on March 31, 2014.

Blum, Stephanie C. 2009. "What Really is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Reform." *Boston University Public Interest Law Journal* 18: 269-314.

Bradbury, Steven G. 2013. "Understanding the NSA Programs: Bulk Acquisition of Telephone Metadata under Section 215 and Foreign-Targeted Collection Under Section 702." *Lawfare Research Paper Series*, September 1 (3): 1-18.

Bradley, Alison A. 2002. “Extremism in the Defense of Liberty?: The Foreign Intelligence Surveillance Act and the Significance of the USA PATRIOT ACT.” *Tulane Law Review* 77: 465-493.

Bush, George W. 2002. *The National Security Strategy of the United States of America*. White House. Washington, D.C., September. Last accessed at http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf on March 31, 2014.

City of Ontario v. Quon, 558 U.S. 1090 (2010).

Clapper, James R. “FISC Approves Government’s Request to Modify Telephony Metadata Program.” Office of the Director of National Intelligence, February 6. Last accessed at http://icontherecord.tumblr.com/post/75842023946/fisc-approves-governments-request-to-modify on March 31, 2014.

Clapper v. Amnesty International, 133 S.Ct. 1138 (2013).

Cox, Louis A., Jr. 2008. "Some Limitations of "Risk=Threat X Vulnerability X Consequence" for Risk Analysis of Terrorist Attacks." *Risk Analysis* 28 (6): 1749-1761.

DeCew, Judith W. 1986. "The Scope of Privacy in Law and Ethics." *Law and Philosophy* 5 (2): 145-173.

Decker, Raymond J. 2001. “Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts.” *S. Comm. On Governmental Affairs*, 107th Cong. Last accessed at: http://www.gao.gov/assets/110/109050.pdf on March 31, 2014.

Diamond, John. And David Jackson. 2006. “Surveillance program protects country, Bush says.” *USA Today,* January 23. Last accessed at http://usatoday30.usatoday.com/news/washington/2006-01-23-bush_x.htm?csp=24 on March 31, 2014.

Foreign Intelligence Surveillance Act of 1978. Pub. L. 95-11. 92 Stat. 1783. 25 Oct. 1978.

Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008. Pub. L. 110-261. Stat. 2474. 9 July 2008.

Garrow, David J. Edward Sorel. and Nancy C. Sorel. 2002. “The FBI and Martin Luther King.” *Atlantic Monthly,* July 2002: 80-88. Last accessed at http://www.theatlantic.com/magazine/archive/2002/07/the-fbi-and-martin-luther-king/302537/ on March 31, 2014.

Gorkin, Russell T. 2010. "The Constitutional Right to Informational Privacy: Nasa v. Nelson." *Duke Journal of Constitutional Law and Public Policy Sidebar* 6 (1): 1-22.

Greenwald, Glenn. 2013. "NSA collecting phone records of millions of Verizon customers daily." *The Guardian*, June 5. Last accessed at http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order on March 31, 2014.

Greenwald, Glenn. and Ewen MacAskill. "Boundless Informant: the NSA's secret tool to track global surveillance data." *The Guardian*, June 11. Last accessed at http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining on March 31, 2014.

Greenwald, Glenn. and Laura Poitras. 2013. "NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things' – video." *The Guardian*, June 9. Last accessed at http://www.theguardian.com/world/video/2013/jun/09/nsa- whistleblower-edward-snowden-interview-video on March 31, 2014.

Griswold v. Connecticut, 381 U.S. 479 (1965).

Hall, Randolph W. 2005. "Assessment Guidelines for Counter-Terrorism: CREATE Terrorism Modeling System (CTMS), a CREATE Report." *Center for Risk and Economic Analysis of Terrorism Events*, University of Southern California: rep. 05-017. Last accessed at http://www.usc.edu/dept/create/assets/001/50787.pdf on March 31, 2014.

Howe, Eva. 2006. "Angle Repeated Discredited Brooklyn Bridge Claim" *Media Matters*, February 6. Last accessed at http://mediamatters.org/research/2006/02/06/angle-repeated-discredited-brooklyn-bridge-clai/134795 on March 31, 2014.

Introna, Lucas D. 1997. "Privacy and the Computer: Why We Need Privacy in the Information Society." *Metaphilosophy* 28 (3): 259-75.

Jaeger, Paul T., John C. Bertot., Charles R. McClure. 2003. "The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act." *Government Information Quarterly* 20: 295-314.

Kalven, Josh. 2006. "Boot Repeated Dubious Claim that Secret NSA program led to Arrest of Iyman Faris." *Media Matters*, January 19. Last accessed at http://mediamatters.org/research/2006/01/19/boot-repeated-dubious-claim-that-secret-nsa-pro/134669 on March 31, 2014.

Klayman v. Obama, No. 13-0851 WL 6571596 (D.D.C. Dec. 16, 2013).

Lee, Timothy B. 2013. “Here’s everything we know about PRISM to date.” *Washington Post*, June 12. Last accessed at: http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/ on March 31, 2014.

Levy, Robert A. 2006. “Wartime Executive Power: Are Warrantless Wiretaps Legal?” *THE FREEMAN: Ideas on Liberty*, February 28. Last accessed at http://object.cato.org/sites/cato.org/files/articles/levy-fee-july2006_0.pdf on March 31, 2014.

Marshall, William P., Hon. Leonie M. Brinkema, J. Trevor Hughes, Ginger McCall. 2014. “Techno-Snooping: Privacy, Technology, and the Evolving Rule of Law.” *Colby College Brody Panel Discussion*, April 6. Last accessed at: http://www.colby.edu/news_events/c/b/040614/2773127/techno-snooping-privacy-technology-and-the-evolving-rule-of-law/ on April 14, 2014.

Masse, Todd., Siobhan O’Neil, and John Rollins. 2007. *The Department of Homeland Security’s Risk Assessment Methodology: Evolution, Issues, and Options for Congress*. Congressional Research Service, February 2. Last accessed at http://fpc.state.gov/documents/organization/80208.pdf on April 4, 2014.

Moor, James H. 1990. "The Ethics of Privacy Protection." *Library Trends* 39 (1-2): 69-82.

Moor, James H. 1997. "Towards a Theory of Privacy in the Information Age." *Computers and Society* 27 (3): 27-32.

Mueller, Robert. 2001. “Indictment of Zacarias Moussaoui.” FBI National Press Office, December 12. Last accessed at http://www.fbi.gov/news/pressrel/press-releases/indictment-of-zacarias-moussaoui-1 on March 31, 2014.

National Research Council. 2010. *Review of the Department of Homeland Security’s Approach to Risk Analysis.* Washington, DC: The National Academies Press. Last accessed at: http://www.nap.edu/openbook.php?record_id=12972 on March 31, 2014.

Nissenbaum, Helen. 1998. "Protecting Privacy in an Information Age: The Problem of Privacy in Public." *Law and Philosophy* 17: 559-96.

Obama, Barack. 2010 *National Security Strategy*. White House. Washington, D.C., May. Last accessed at http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf on March 31, 2014.

Obama, Barack. 2014. “Remarks by the President on Review of Signals Intelligence.”

White House, January 17. Last accessed at http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence on March 31, 2014.

O'Brien, Lauren B. 2011. "The Evolution of Terrorism Since 9/11." *FBI Law Enforcement Bulletin*. September. Last accessed at http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/september-2011/the-evolution-of-terrorism-since-9-11 on March 31, 2014.

Osher, Steven A. 2002. "Privacy, Computers and the Patriot Act: The Fourth Amendment Isn't Dead, but no one will Insure it." *Florida Law Review* 54: 521-542.

Parent, William A. 1984. "Recent Work on the Concept of Privacy." *American Philosophical Quarterly* 20 (4): 341-54.

Pew Research. 2014. "Obama's NSA Speech has Little Impact on Skeptical Public." *Pew Research Center for the People & the Press*, January 20. Last accessed at: http://www.people-press.org/2014/01/20/obamas-nsa-speech-has-little-impact-on-skeptical-public/ on April 14, 2014.

Posner, Richard A. 2008. "Privacy, Surveillance, and Law." *The University of Chicago Law Review* 75 (1): 245-260.

Protect America Act of 2007. Pub. L. 110-55.121 Stat. 552. 5 Aug. (2007).

Rainie, Lee, Sara Kiesler, Ruogu Kang and Mary Madden. 2013. "Anonymity, Privacy, and Security Online." *Pew Research Internet Project*, September 5. Last accessed at: http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/ on April 14, 2014.

Risen, James. 2007. "Bush Signs Law to Widen Reach for Wiretapping." *New York Times,* August 6. Last accessed at http://www.nytimes.com/2007/08/06/washington/06nsa.html?_r=0 on March 31, 2014.

Risen, James. and Eric Lichtblau. 2005. "Bush Lets U.S. Spy on Callers Without Courts." *New York Times*. December 16. Last accessed at http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all on March 31, 2014.

Roe v. Wade, 410 U.S. 113 (1973).

Rowley, Coleen M. 2002. "Memo to FBI Director Robert Mueller." *TIME Magazine,* May 21. 2002. Last accessed at http://globalresearch.ca/articles/ROW205A.html on March 31, 2014.

Sanger, David E. 2005. “Bush Says He Ordered Domestic Spying.” *New York Times*, December 18. Last accessed at: http://www.nytimes.com/2005/12/18/politics/18bush.html?pagewanted=all&_r=0 on April 2, 2014.

Sanger, David E. 2014. “Obama Lets N.S.A. Exploit Some Internet Flaws, Officials Say.” *New York Times*, April 12. Last accessed at: http://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html?emc=eta1&_r=0 on April 14, 2014.

Sarkesian, Sam C., John A. Williams, and Stephen J. Cimbala. 2013. *US National Security: Policymakers, Processes, and Politics*. Boulder, CO: Lynne Rienner Publishers.

Savage, Charlie. 2013. “N.S.A. Chief Says Surveillance has stopped Dozens of Plots.” *New York Times*, June 18. Last accessed at: http://www.nytimes.com/2013/06/19/us/politics/nsa-chief-says-surveillance-has-stopped-dozens-of-plots.html?pagewanted=all on April 1, 2014.

Schoeman, Ferdinand. 1984. "Privacy: Philosophical Dimensions." *American Philosophical Quarterly* 21 (3): 199-213.

Shenon, Philip. 2001. "A Nation Challenged: The Suspect; Flight School Warned F.B.I. of Suspicions." *The New York Times*, December 22. Last accessed at http://www.nytimes.com/2001/12/22/us/a-nation-challenged-the-suspect-flight-school-warned-fbi-of-suspicions.html on March 31, 2014.

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

Solove, Daniel J. 2002. "Conceptualizing Privacy." *California Law Review* 90 (4): 1087-155.

Sottek, T.C. and Josh Kopstein. 2013. “Everything you need to know about PRISM.” *The Verge*, July 17. Last accessed at http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet on March 31, 2014.

Tavani, Herman T. 2007. "Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy." *Metaphilosophy* 38 (1): 1-22.

Ullman, Richard H. 1983. "Redefining Security." *International Security* 8 (1): 129-53.

United States Cong. 2003. *9/11 Report: Joint Congressional Inquiry*. Washington: Congress, July 24. Last accessed at: http://news.findlaw.com/wsj/docs/911rpt/index.html on March 31, 2014.

United States Cong.: House Permanent Select Comm. on Intelligence and the S. Select Comm. on Intelligence. 2003. *9/11 Report: Joint Congressional Inquiry*, July 24. Last accessed at http://news.findlaw.com/wsj/docs/911rpt/index.html on March 31, 2014.

United States. Dept. of Justice. 2004. *A Review of the FBI's Handling of Intelligence Information Prior to the September 11 Attacks*. Natl. Office of the Inspector General, November. Last accessed at: http://www.justice.gov/oig/special/s0606/final.pdf on March 31, 2014.

United States Dept. of Justice. 2003. "Iyman Faris Sentenced for Providing Material Support to Al Qaeda." Washington: U.S. Dept of Justice, October. Last accessed at http://www.justice.gov/opa/pr/2003/October/03_crm_589.htm on March 31, 2014.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001. H.R. 3162, 107th Cong., 1st Sess. (2001).

Warren, Samuel D., and Louis D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4 (5): 193-220.

Washington Post. 2013. "NSA slides explain the PRISM data-collection program." *Washington Post*, June 6. Last accessed at http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ on March 31, 2014.