4-25-2019

Fear and Freedom are at War - Privacy v. Security

Ryan Hennigan
rhennigan@cedarville.edu

“Fear and Freedom Are at War.”[1]

GSS 4900 – Senior Research

Ryan Hennigan

11 April 2019

[1] “President Bush Addresses the Nation.” *The Washington Post*, WP Company, 20 Sept. 2001

Table of Contents

Abstract

This paper deals with the seemingly unending balancing act of privacy versus security. To highlight this issue, the topic of discussion is the USA PATRIOT Act and the 9/11 background leading to its passage. Also, covered in the introduction is the state and apparatus of the U.S. intelligence community pre-9/11. As for the specifics of the law, this paper explores Section 213, dealing with the nature of warrants and their changing use in the fight against terrorism, Section 214, regarding wiretaps, including everything from the purpose of the device to the use of warrants to employ them, and finally Section 215, which is arguably the most controversial section of the law that outlines how the U.S. intelligence community uses secret dragnet procedures and programs to spy on unsuspecting U.S. citizens in an effort to collect telecommunications metadata. After the discussion about these sections of the law, the paper highlights the current development of revisions made to the law through the passage of the USA FREEDOM Act, which heeds the call for privacy reform, but does not truly fix the problem. Lastly, this paper offers a Christian worldview interpretation of what the Bible has to say about proper governance and what John Locke, arguably the most influential mind that helped form America's founding, might have to say on the issue.

Introduction

September 11, 2001 is a date that has been burned into the memories of every American. The nature of our nation was changed in an instant the moment that four commercial airplanes were hijacked and used as missiles against American civilians and military personnel in New York, Virginia, and Pennsylvania. Nearly 3,000 Americans perished, and the Twin Towers of the World Trade Center in downtown Manhattan were toppled. That day there were at least these two questions on everyone's mind: who has done this, and how do we stop it from happening again?

Before 9/11, America had never known a mainland attack on civilians of that magnitude in history. The United States' intelligence community was still stuck in a Cold War mentality, meaning it was focused on state actors rather than rogue extremist groups.[2] The federal creation of FISA in 1978, standing for the Federal Intelligence Surveillance Act, was the legal groundwork for intelligence collection regarding foreign adversaries to the U.S. The Act itself gave intelligence agencies like the CIA and NSA tools to spy on, locate, and prosecute potential threats to the national security of the U.S. In the words of Senator Patrick Leahy (D-VT) from the Senate Committee on the Judiciary:

> This law set up a secret court to review government applications to conduct secret wiretaps and searches inside the United States for the purpose of collecting foreign intelligence information to help protect this nation's national security. FISA was originally enacted in the 1970s to curb widespread abuses by both Presidents and former FBI officials of bugging and wiretapping Americans without any judicial warrant--based

[2] Clapper, James R. "How 9/11 Transformed the Intelligence Community." *The Wall Street Journal*, Dow Jones & Company, 7 Sept. 2011

> on the Executive Branch's unilateral determination that national security justified that surveillance.[3]

While FISA was a good start and appeared to meet the needs of the U.S. from the 1970s into the 1990s, after the attacks, it became increasingly obvious that the U.S. government had failed in its role as promoter of the general welfare and protector of the peace.[4] Drastic changes were required to meet this catastrophe, and those changes had to start on American soil. It was deemed necessary that if the U.S. was ever going to right this evil and prevent something similar or worse from ever happening on U.S. soil again, it had to arm itself with intelligence to fight this new enemy.

The tools America agreed it needed were soon to be found in the USA PATRIOT Act. This law, which stands for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, was passed in October of 2001 and it was the justification America needed to give the intelligence community resources to expand its operations.[5] Once again, Senator Leahy said, "In the USA PATRIOT Act, we sought to make FISA a more effective tool to protect our national security…"[6] On the same Senate Committee on the Judiciary, Senator Hatch (R-UT) said,

> After last year's tragic attack on September 11th, the [Bush] administration and Congress worked together to enact the PATRIOT Act. This is a broad package of measures that provided law enforcement and the intelligence communities with the necessary tools to fight terrorism worldwide and, of course, protect our country. These reforms were critical

---

[3] "THE USA PATRIOT ACT IN PRACTICE: SHEDDING LIGHT ON THE FISA PROCESS." *Senate Judiciary Committee Hearing on FISA Oversight: September 10, 2002*

[4] U.S. Congress. National Commission of Terrorist Attacks Upon the United States. Cong.

[5] The United States Department of Justice.

[6] "THE USA PATRIOT ACT IN PRACTICE: SHEDDING LIGHT ON THE FISA PROCESS." *Senate Judiciary Committee Hearing on FISA Oversight: September 10, 2002*

> to enhance our government's ability to detect and prevent terrorist attacks from occurring again…One of the most significant issues addressed by the PATRIOT Act was the lack of effective coordination between intelligence and criminal investigations.

With the speedy passage of this law that vastly broadened the horizon of governmental investigative powers, some agencies, activist groups, and media outlets were worried about how the telecommunications privacy of Americans was being handled and protected.

This was a new age of warfare, one that did not have a defined battlefield, but that could pop up at any moment anywhere. Therefore, now everything had to be tracked: phone calls, emails, bank accounts, etc. all in an effort to catch suspected terrorists to prevent another national crisis like 9/11. However, due to the unpredictable nature of the new fight facing America, boundaries of privacy, once enshrined in American freedom and individualism, were being crossed. Fourth Amendment protections of searches and seizures with warrants were beginning to enter the crosshairs of the American intelligence community. The thought was that if potential enemies were tipped off that they were being investigated, or spied on, then their illegal operations might go underground and be all that much more difficult to investigate. To prevent such a tipoff, the intelligence community now had governmental provision and approval through the USA PATRIOT Act to increase its surveillance techniques in ways that degraded the right of every American to be left alone from its government, or in other words, to possess privacy.

As will be discussed later in this paper, the massive privacy overreaches that were made by the intelligence community and sanctioned for by the USA PATRIOT Act have come to be known to the American people from the release of classified information from an ex-CIA and ex-NSA agent named Edward Snowden. Once Snowden made known that the U.S. intelligence community was an apparatus of unimaginable proportions to the average citizen, the gates of

controversy over the USA PATRIOT Act that sparked privacy fears were flung open wide. Whether history shall deem Snowden a hero or a traitor, such a discussion is out of the scope of this paper. However, the fact of the matter is that the intelligence apparatus and the precedent for the implementation of it still exists no matter what legislation is passed or what political party is elected to power. Speaking to the scope of this paper, multiple books and articles have been written on this issue of privacy versus security, however, this work only covers a minute section of telecommunications privacy affected by the USA PATRIOT Act. Furthermore, due to the limits of this research, the Christian-worldview/ethical section of the paper offers merely a passing glance at deeper theological and governance issues. With that being said, the two main research questions that this paper addresses are: Do Sections 213-215 of the USA PATRIOT Act violate the privacy rights of U.S. citizens, and, if so, can those rights be regained? As the following case will be made, the USA PATRIOT Act did overstep and violate U.S. citizens' privacy rights, and once lawmakers decide that certain privacy rights and concerns must be surrendered by the American people in a time of a national emergency, it is extremely difficult, if not impossible, to reinstate the full institution of those privacy rights again.

Literature Review

As mentioned above, several non-government agencies, activist groups, and individuals have published their take on the seemingly perennial debate of privacy versus security, thus the literature is extensive. However, one aspect of such publications about 21st century privacy in America that appears to be consistent is the inclusion of the USA PATRIOT Act in the discussion. With the passage of this bill, the federal government extended its investigative powers in the hopes of defending the nation. Knowing that more security would make some

lawmakers and Americans nervous about the sovereignty of their rights, it was touted at the time that this act would be able to both provide for the needs of national security, while simultaneously protecting the privacy of American citizens.[7]

In recent years, much political and social turmoil has surrounded this conversation of privacy versus security, especially given the developments of NSA mass data cache collecting discovered from leaked documents from within the NSA by Edward Snowden, that will be addressed later in this paper.[8] As far as the literature goes on this topic, specifically narrowed to the USA PATRIOT Act, most of the media complex in America appears to be against the extended parameters of government surveillance sanctioned for by the Act. Two of the most important news giants, the New York Times and NBC, both were eager to broadcast publications about the fears and shortcomings of the law and actions taken by America's intelligence community in light of it. Specifically, in 2005, the New York Times put out an article blasting the George W. Bush Administration and revealing to the American people that the NSA was partaking in the mass data collecting of U.S. citizens' phone records without warrants or needed judicial review.[9] Following this release by the New York Times several years later, NBC broadcasted the reform of the USA PATRIOT Act when former U.S. President Barack Obama signed into law the USA FREEDOM Act, which will be addressed later in this paper.[10]

Aside from these two media giants flexing their influence as opponents of the USA PATRIOT Act, other agencies and collectives, political in nature, sounded their disapproval. One such agency is the ACLU (American Civil Liberties Union). This organization, classified as a nonprofit organization, famous for its litigation in the Supreme Court and its lobbying of U.S.

---

[7] McNeill, Jena Baker. "The PATRIOT Act and the Constitution: Five Key Points." The Heritage Foundation.
[8] Gallagher, Ryan. "NSA Collecting Phone Records for Millions of U.S. Verizon Customers." Slate Magazine.
[9] Lichtblau, James Risen and Eric. "Bush Lets U.S. Spy on Callers Without Courts." The New York Times.
[10] Thorp, Frank, V. "Barack Obama Signs 'USA Freedom Act' to Reform NSA Surveillance." NBCNews.com.

lawmakers, stood adamantly opposed to the passage of the USA PATRIOT Act because in its view, the law minimized the effectiveness of the Fourth Amendment to the U.S. Constitution, and it violated the basic right of privacy for every American by allowing the federal government unprecedented access to individuals' records, from emails to bank statements to phone calls, all without a warrant or at least a legitimate one.[11] Even though the ACLU arguably is one of the most vocal opponents to the Act, it by no means stands alone. Also standing opposed to the passage and implementation of the Act is the Electronic Privacy Information Center (EPIC), an issue-based lobbying group, responsible for authoring *amicus curiae* briefs and lobbying agendas all relating to privacy. According to EPIC, the USA PATRIOT Act's claims of adequate government oversight and checks and balances are not nearly effective enough to protect American citizens' right to privacy.[12]

With all of these high-profile critics taking their arguments, viewpoints, and findings to the people through mass publication, at first glance it might seem like there is little to no support for the USA PATRIOT Act, which was predicated on the need for looking out for the safety and security of the American people. However, the Act is not without its supporters. The most obvious supporters of the Act were/are government entities, such as the Department of Justice, Congress, and the State Department. All of these institutions saw the Act as necessary given the scope and destruction of the 9/11 terrorist attacks. In their eyes, this attack ushered in a new wave of warfare; this attack was no Pearl Harbor, which targeted military installations. Rather, this attack was performed against soft targets, meaning civilians and non-military personnel and infrastructure, in the hopes that it would inspire fear in the masses. Even President George W. Bush, in his September 20th address to a joint session of Congress, admitted that this enemy was

---

[11] "Surveillance Under the USA/PATRIOT Act." American Civil Liberties Union.
[12] "EPIC - USA Patriot Act." Electronic Privacy Information Center.

not a contemporary one for the United States; the men who created and executed these attacks, and the terrorist network who supported them, were the rumblings of an enemy who does not fight like modern armies, does not differentiate between civilians and military, and does not present conduct worthy to be called honorable. Admittedly, this fight, the War on Terror as it would come to be called, would be a long, costly, and arduous one.[13]

To fight this unconventional enemy required unconventional tactics. Thus, when the USA PATRIOT Act was drafted in 2001 to expand the surveillance tactics of the U.S. intelligence community, it was backed by lawmakers with the bill passing in favor in the House of Representatives by 357 votes to 66 and in the Senate 98 to 1.[14] Security became the highest commodity. Coming from a place of recognized failure on the part of the federal government to protect American citizens on that fateful September day, the government supported the expansionist agenda of the Act.[15] Aside from governmental support, the Act was also favored by the popular conservative-leaning think tank Heritage Foundation. The Heritage Foundation defended the Act upon its creation and on the arrival of its renewal dates. Heritage argued that the Act had internal and external safeguards that provided for security and individual protection of privacy, but most of all, that the Act was needed to protect national security.[16]

Of course, given the polarizing issue of privacy versus security, there were some institutions dedicated to attempting to solely present the facts of the Act and the stance of each side, both for and against the Act. These types of publications centered mostly around higher education sources or issue-based research institutions. For instance, the University of

---

[13] Selected Speeches of President George W. Bush: 2001-2008.
[14] "H.R. 3162 (107th): Uniting and Strengthening America by Providing Appropriate ... -- Senate Vote #313 -- Oct 25, 2001." GovTrack.us.
[15] The United States Department of Justice.
[16] McNeill, Jena Baker. "The PATRIOT Act and the Constitution: Five Key Points." The Heritage Foundation.

Connecticut's publication *UConn Today* published an article from its law school division entitled *Privacy, Security, and The Legacy of 9/11*. In this article, the author attempts to address the privacy concerns of legislation passed in retrospect of the 9/11 terrorist attack. Due to its question and answer format, the publication takes the stance of merely informing its readers, not taking a side.[17] Joining this middle-of-the-road stance, attempting to stay mostly objective solely by presenting facts is a research institution called the Center for Strategic and International Studies. This source published an article discussing the controversy of Section 215 of the USA PATRIOT, which will be discussed later in this paper. It references the issue some Americans have with the collection of telephony metadata, and then presents factual statistics to allow for the reader to decide for themselves if the law is truly a breach of privacy or not.[18]

As mentioned above, this issue of the balance between privacy versus security appears to present itself in increasing measure throughout the history of the United States. One can look back at the invention of wiretaps in the 1920s and 30s, anti-communist suspicions throughout the 50s and into the 80s, and now the authorization of metadata collecting through the internet and phone services due to 9/11 and they can see that at punctuated times, the scales of privacy and security have tipped to one extreme or the other. Arguably, all of these times, including the time of the passage of the USA PATRIOT Act, have been in times of national emergencies. However, as admitted to by President Bush, this national emergency of terrorist aggression and threats, is a long and strenuous one. However, is the United States truly still in danger of terrorist cells that have collectively declared death to America? The United States is coming up on the 18th anniversary of 9/11, and there are still military troops in Afghanistan. This War on

[17] Klau, Daniel. "Privacy, Security, and the Legacy of 9/11." UConn Today.
[18] Mann, Scott F. "Fact Sheet: Section 215 of the USA PATRIOT Act." Nuclear Stability in a Post-Arms Control World | Center for Strategic and International Studies.

Terror has been America's longest fight to date. Are we safe? Are our rights safe? The U.S. government was created in part to help protect its citizens, both from foreign and domestic enemies. But, who will protect Americans from their government? Has the government overstepped the safeguards all in the name of national security? When does security bow to privacy, and has the USA PATRIOT Act made privacy in this version of 21st century warfare a myth? Some might argue that this conclusion is a bit far fetched. However, if it is okay to surrender certain rights or the extent of some liberties in the time of a national crisis, when and how do we decide that it is time for those suspended rights to return in full measure? Can those suspended rights come back?

I am arguing that no matter which source you look at, either those that are in favor of the USA PATRIOT Act or those against it, the one thing that they all have in common is the realization that in the aftermath of the terrorist attacks committed on 9/11, the nature of privacy looks different then it did before. I argue in this paper that the idea and extent of the right to privacy possessed by American citizens was irreversibly changed through the creation and passage of the USA PATRIOT Act; the American people will never again know a government who will not try to argue the need to push the bounds of privacy intrusion for the sake of national security.

If it is true, that this ideal of privacy, that many organizations in the higher spheres of influence in American culture have argued has been tainted through the passage of the USA PATRIOT Act, is truly irredeemable, then it is arguable that the very definition of what the American Dream means has changed. To be the beacon of democracy, economic thriving, freedom and justice that America has claimed to be for nearly three centuries now, Americans must come to grips with the fact that they live in a different state now; a state that trusts no one.

Americans must realize that not only does freedom come at a cost, but so does peace. In the famous movie *Enemy of the State*, which entertains viewers with thoughts of government conspiracies over intrastate spying and assassination cover-up, one of the main characters has a quote that characterizes the government that directs the America that exists today: "Now we are fighting the peace, and it is much more volatile."[19] One could argue that if this peace which requires enhanced governmental intrusion is the end result of what it means to have security in the world, then has the terrorist won? If the goal of the terrorist is to inspire fear that leads to inaction, is it not in their best interest to have a people's own government perpetuate this fear through spying and killing the boldness that is needed to have the freedom of privacy? We shall see.

The Controversy Begins – Section 213

"A person has the right to determine what sort of information about them is collected and how that information is used." – Tim Sharp[20]

The USA PATRIOT Act was obviously seen as necessary for the U.S. to defend the homeland against terrorism, in both foreign and domestic forms. However, virtually from the outset of its passage, the law had its dissenters. The dissensions arose mostly around concerns of privacy, namely those dealing with property and telecommunications data. There are four main sections of the law that appeared to violate the sanctity of privacy, which Merriam Webster defines as, "the quality or state of being apart from company or observation."[21] The first section of the Act that the enemies of the law zeroed in on was Section 213.

---

[19] Bruckheimer, J (Producer), & Scott, T. (Director). (1998). *Enemy of the State* [Motion Picture]. United States: Touchstone Pictures.-

[20] Sharp, Tim. "Right to Privacy: Constitutional Rights & Privacy Laws." *LiveScience*, Purch, 12 June 2013

[21] *Merriam-Webster*

Section 213 of the USA PATRIOT Act, also known as the "Sneak and Peek" section, mostly handles the topic of search warrants for investigations related to potential acts of terrorism.[22] The ACLU interprets the section as such:

> "[This section] would allow law enforcement agencies to delay giving notice when they conduct a search. This means that the government could enter a house, apartment or office with a search warrant when the occupant was away, search through [a person's] property and take photographs, and in some cases seize physical property and electronic communications, and not tell [that person] until later. This provision would mark a [drastic] change in the way search warrants are executed in the United States."[23]

The basics of this section of the law are targeted toward the idea mentioned earlier that U.S. intelligence service agencies, in investigating potential terrorist threats, did not want to tip off those they were investigating for fear that they would take their illegal operations underground and be all the more difficult to find and potentially stop. The problem with these delayed warrants, is that, unlike typical warrants, they are detached from a third party that looks over the limits and provisions of the warrant in order to issue them, i.e. a magistrate. These delayed warrants are only approved by such a magistrate after they are served and thus, the searching authorities have greater license to expand the items and area being searched and potentially seized.

Aside from the broad nature of these delayed warrants, some argue that they also defy the Fourth Amendment of the U.S. Constitution. This Amendment protects U.S. citizens from unreasonable searches and seizures conducted without warrants. Also, this Amendment was

---

[22] DeRosa, Mary, et al. "Patriot Debates." - *Section 213*

[23] ACLU. "How the USA-Patriot Act Expands Law Enforcement 'Sneak and Peek' Warrants."

included in the list of Amendments that Supreme Court Justice William Douglas ruled as relating to the right to privacy.[24] The Supreme Court ruled that prior notice to the addressee of a warrant was a cornerstone of the Fourth Amendment.[25] Even though this has been the ruling of the highest Court in the nation, the Executive Branch still must enforce such a ruling, and at times throughout the glory years of the USA PATRIOT Act, it has not. Realistically, it is more practical to have intelligence agencies ask for forgiveness rather than to have them ask for permission. Because the USA PATRIOT Act was the law of the land, these intelligence agencies had both permission and forgiveness. One nuance that did set this "Sneak and Peek" Section apart from the other sections of the Act is that it was a permanent fixture in the law and did not contain a sunset provision, meaning it did not have to been individually renewed upon a certain expiration date set forth by the law upon its passage.[26]

However, the government argues for the constitutionality of the use of the tactic of delayed warrants. It argues that the notification of the service of the warrant still exists, but it is given after the search and/or seizure is complete. Furthermore, the government defends its use of delayed warrants by resorting to a historical argument, saying that these types of warrants have been used successfully in the past to catch those participating in child pornography, organized crime, and drug cases.[27] Where the government makes a compelling argument that there are safety –nets built into the law for these very reasons, its arguments do not seem to concern the threat of governmental overreach when the Fourth Amendment's original context is applied to the jurisprudence of issues involving warrants and searches.

---

[24] Oyez. "Griswold v. Connecticut."
[25] ACLU. "How the USA-Patriot Act Expands Law Enforcement 'Sneak and Peek' Warrants."
[26] ACLU. "How the USA-Patriot Act Expands Law Enforcement 'Sneak and Peek' Warrants."
[27] "USA Patriot Act Myth vs Reality ." *Preserving Life & Liberty Dispelling the Myths*

With this precedent in place, the integrity of the Fourth Amendment comes into question. This is just one instance within the spotlight of the USA PATRIOT Act where the lawmakers have empowered the government to decide when the right to privacy, such as in the case of not being notified of the service of a warrant, needs to be surrendered for the preservation of national security. This blatant disregard for the supremacy of the Constitution blazes a dangerous path for future lawmakers to suspend the founding principles of American identity that Americans hold so dear. Is security purchased at the price of the loss of privacy and individualism worth having in the first place? Should the American people accept that their Constitution and the actions of their government do not coincide? I would argue that where it is absolutely imperative to provide for national defense for the protection of the American people, it should not mean demeaning our values and the cornerstones of our identity. If the intelligence agencies are nervous about losing track of their suspects because their asking for a warrant may tip off the suspects and cause them to make their dealings more covert, then I believe that the duty is on the American government to adapt to meet the challenge, not settle for the sacrificing of American citizens' privacy.

The government took ownership when it failed to prevent 9/11, but now it is punishing the people by surrendering parts of their freedoms all to perform its own job of providing security. If the United States truly is the land of the free and home of the brave and the best country in the world as its leaders claim, then it cannot continue to bend its convictions to offer mediocre versions of the rights and freedoms that it touts and attempts to spread around the world. If America is the exceptional pacesetter it has been made out to be, then the lawmakers need to harness that American ingenuity to rise and meet the challenge of providing safety while

simultaneously vigorously defending in full measure the liberties and freedoms its people are entitled to.

Trap and Trace – Section 214

If the right to privacy means anything, it is the right of the individual, married or single, to be free from unwarranted governmental intrusion." - William J. Brennan[28]

Section 214 of the Act, otherwise known as the "Trap and Trace" Section, mostly regards the use of wiretaps. It has long been known that with the introduction of new technology, laws and procedures for collecting evidence have had to change to accommodate such new societal norms. Wiretapping is one such phenomenon. There have been several Supreme Court cases regarding the constitutional use and procedures of wiretapping in criminal investigations, but this section of the USA PATRIOT Act made the complexity of wiretapping a broader, more national and popular issue.

This section amends the FISA Act in relation to what are called pen registers and trap and trace devices. When looking at the United States Code, Cornell Law School defines a pen register as such: "[A] device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication…"[29] In layman terms, these devices are able to track the numbers dialed on a phone and the addressing information, or the location of a call. Since the beginning of wiretapping procedures, there has been a distinction between spying on the location and origin of a call, and the content of a phone conversation. Pen registers and trap and trace

---

[28] "William J. Brennan Quote." *Right to Privacy Quotes,* AZ Quotes,

[29] "18 U.S. Code § 3121 - General Prohibition on Pen Register and Trap and Trace Device Use; Exception." *Legal Information Institute*

devices are said to only locate a call and the number dialed, not be used to disclose the content of conversations.

Section 214 of the USA PATRIOT Act expands the limits and rationales of the use of obtaining pen register/trap and trace warrants, setting a dangerous precedent of excessive governmental overreach into the protection of privacy. In the past, under FISA, to apply for these types of warrant, intelligence agencies had to prove that its intent was to surveil for the purpose of foreign intelligence, and that any information that they gathered was not intended to be used to bring someone to trial.[30] However, the USA PATRIOT Act expanded this justification for the issuance of these types of warrants; rather than being required to prove such wiretaps were to be used for the collection of foreign intelligence, now intelligence agencies must only demonstrate that there is a "significant purpose" for their use, thus lowering the bar and broadening the ability to receive such a warrant.[31]

On top of this broadening of justification for pen registers and trap and trace (PR/TT) wiretaps, the nature of the warrants themselves has changed. Under the provisions of the USA PATRIOT Act, the PR/TT warrants issued by magistrates are valid nationwide, and not just within that specific magistrate's jurisdiction.[32] This broad expansion of the warrants has effectively diminished the specificity of issuing and executing a warrant as interpreted by the Fourth Amendment. By narrowing the oversight of the judiciary, lawmakers have granted the intelligence community a larger geographic scope to conduct intelligence gathering operations while simultaneously lowering the bar to obtain the warrants in the first place.

---

[30] ACLU. "Surveillance Under the USA/PATRIOT Act."
[31] ACLU. "Surveillance Under the USA/PATRIOT Act."
[32] ACLU. "Surveillance Under the USA/PATRIOT Act."

A second way in which the USA PATRIOT Act has changed and broadened the nature of the warrants themselves is by now making PR/TT devices applicable to internet searches. As mentioned above, the PR/TT wiretaps are only meant to disclose the addressing information of whatever device it is attached to. So now that these wiretaps are being used by the intelligence community on websites, such agencies are able to read email headers, search histories, and preferred searches.[33] The privacy argument against such practices is that these characteristics of internet uses are much more than just addressing information. Personalized searches are relevant to specific people and say more about the user than simple locations could. The same is true with email headers. Such headers not only include to whom the email is being sent, but it also includes the subject line, which is a summary or the theme of the body context below. Naturally, these loosened justifications and procedures are cause for concern. The judiciary has virtually removed itself from the process of issuing PR/TT wiretap warrants and the process of reviewing the extent to which those warrants apply to American citizens, who may have no idea that they are being surveilled by the federal government.

When looking at the arguments in favor of the provisions for PR/TT wiretaps and warrants that issue them embedded in the USA PATRIOT Act, the government claims that such intelligence procedures are specifically not directed toward those actions taken by Americans that are protected under the First Amendment.[34] However, there is no discussion within the law itself as to what actions in the telecommunications sphere, such as sending emails and searching the internet, are considered protected under the First Amendment. Therefore, the intelligence agencies are able to draw weak and broad connections to the need for surveillance and what they

[33] ACLU. "Surveillance Under the USA/PATRIOT Act."
[34] "USA Patriot Act Myth vs Reality ." *Preserving Life & Liberty Dispelling the Myths*

are actually surveilling using PR/TT wiretaps. Furthermore, the government uses the argument that in the Supreme Court case *Smith v. Maryland* (1979), the Court ruled that,

> "The use of pen registers does not constitute a 'search' within the meaning of the Fourth Amendment. As such, the Constitution does not require that law enforcement obtain court approval before installing a pen register. This is so because 'a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties…'"[35]

Granted this support for the government's case is more compelling than some of its other supports. However, when reviewing this reference, one must keep in mind that this case was decided before the internet was used in mass by Americans. Therefore, as discussed above with the expansion of uses for the PR/TT wiretaps, intelligence agencies and investigation entities have been given more access to Americans' personal lives in the present age of the internet than was previously envisioned when this Court case was decided. Perhaps now that many Americans do their shopping, banking, communicating, and researching online, the Court would see the need to shore up this broad use of PR/TT wiretaps and warrants. Sadly, such a call to revisit the issue was overshadowed by the need for security given the events of 9/11.

However, once again, the American people are forced to choose between the two fundamental rights of life (security) and liberty (privacy). With this precedent of a distanced judiciary and expansive wiretapping practices by law enforcement and federal intelligence agencies, it is hard to image any practical reversion to internet privacy. Because the standard for what information is considered relevant in the investigation of illegal activities, including terrorism, has been lowered due to Section 214 of the USA PATRIOT Act, then Americans must now live with the understanding that their actions on the internet could very well be being

---

[35] "USA Patriot Act Myth vs Reality ." *Preserving Life & Liberty Dispelling the Myths*

monitored by authorities. The internet is a staple in most American lives nowadays. How should Americans feel about their privacy being invaded when they use this tool? Should the protections of the Fourth Amendment not include those actions that we spend a large amount of our time on, such as sending and receiving emails, searching the internet, and making phone calls? The use of the internet is necessary in the globalized world we currently live in, so knowing that our privacy is potentially at risk by our own government should give us pause because we are bending the values of our right to privacy in a way that degrades the intent of it. Just because the world-wide web exists, should we surrender our fundamental right to privacy? Regardless of how one answers that question, the fact is that it has already been done because of the passage of this law. Never has this fact been more real than when Section 215 of the USA PATRIOT ACT became law, and the floodgates of domestic surveillance secrets were blown open wide.

Telephony Metadata Collection – Section 215

"I can't in good conscience allow the U.S. government to destroy privacy, internet freedom and basic liberties for people around the world with this massive surveillance machine they're secretly building…Even if you're not doing anything wrong, you are being watched and recorded." – Edward Snowden[36]

Arguably, the most controversial section included in the USA PATRIOT Act is Section 215. Section 215, or the "Business Records" section of the law, was an amendment to Section 501 of the FISA Act, where the federal government was given license to collect tangible items, including business records, that may be linked to an investigation involving foreign intelligence.[37] Under this Section, it is prohibited to collect such information to gather intelligence regarding U.S. citizens, unless such action can be linked to the broader need for

[36]"Edward Snowden Quotes." *BrainyQuote*, Xplore
[37] Mann, Scott F. "Fact Sheet: Section 215 of the USA PATRIOT Act."

national security. However, the controversy comes in with the National Security Agency's (NSA) programs of telecommunication metadata collecting.

Telephony metadata is defined by the Center for Strategic and International Studies as, "The mass collection of basic call-log information, from telecommunications companies. This includes the date, time, and duration of calls to and from all phone numbers."[38] Critics of this process have raised the alarm bells because they view this action as a virtual dragnet upon the phone and internet information of U.S. citizens due to what can be considered incidental spying.

The way it works is that as the NSA begins an operation to collect intelligence of a foreign nature, such intelligence can lead back to citizens of the U.S., either intentionally or unintentionally. The trail works itself out because as a U.S. intelligence agency like the NSA conducts wiretapping procedures and acquires phone records or internet search histories of foreign persons of interest, they can use any other outside contacts that that person of interest might have had as another potential informant. So, what started as the investigation of one person of interest grows at an exponential rate to other people the NSA investigates. Eventually, this constant action of delving into peoples' records to potentially gather intelligence makes its way to including U.S. citizens in the mix. This fact came out in full swing in late 2005 and early 2006 when *The New York Times* published an article detailing how then-President Bush allowed the NSA to collect phone data on U.S. citizens without warrants: "Since 2002, the agency has been conducting some warrantless eavesdropping on people in the United States who are linked, even if indirectly, to suspected terrorists through the chain of phone numbers and e-mail addresses, according to several officials who know of the operation."[39] Furthermore, in the middle of 2013, *The Guardian* obtained a copy of an Obama Administration order that showed

[38] Mann, Scott F. "Fact Sheet: Section 215 of the USA PATRIOT Act."
[39] Lichtblau, James Risen and Eric. "Bush Lets U.S. Spy on Callers Without Courts."

how the collection of U.S. citizens' phone data had been increased and continued under the Obama presidency: "The document shows for the first time that under the Obama administration the communication records of millions of US citizens are being collected indiscriminately and in bulk – regardless of whether they are suspected of any wrongdoing."[40]

The situation of privacy of the American people only got worse when in June 2013, an ex-CIA and ex-NSA agent named Edward Snowden illegally released government secrets of how the U.S. intelligence community was gathering information on both foreign and domestic entities. Several of the programs were fraught with privacy violations. Snowden was the agent who truly showed the American public and the world how the gathering and use of telephony metadata was being accomplished. He disclosed programs such as PRISM, which according to *The Washington Post* is a, "system the NSA uses to gain access to the private communications of users of nine popular Internet services…"[41] Snowden also disclosed a Bush-era surveillance program called Stellar Wind which, according to *Business Insider*, allows for the vast collection of Americans' email and internet metadata.[42] However, possibly his most impactful disclosure to date was the release of a governmental surveillance program called Boundless Informant, which is the telecommunications dragnet process that creates a spying network as explained above. Furthermore, this program uses a global heat-map to show the NSA where their intelligence coverage is coming from.[43] According to *The Guardian*, to create this massive spying network of metadata, the NSA was allowed to spy within three groups: the friends of the individual person of interest, then to the friends of those friends, and finally to the friends of

[40] Greenwald, Glenn. "NSA Collecting Phone Records of Millions of Verizon Customers Daily."
[41] Lee, Timothy B. "Here's Everything We Know about PRISM to Date."
[42] Szoldra, Paul. "This Is Everything Edward Snowden Revealed in One Year of Unprecedented Top-Secret Leaks."
[43] Szoldra, Paul. "This Is Everything Edward Snowden Revealed in One Year of Unprecedented Top-Secret Leaks."

those friends.[44] To accomplish this task, the NSA would search phone records, emails, and social media posts of all three of these levels; say the person of interest had just a single friend on Facebook, by the time the NSA gets to the third tear, they will be investigating 26,634 people, some of whom are U.S. citizens.[45] Again from *The* Guardian, "The Boundless Informant documents show the [NSA] collecting almost 3 billion pieces of intelligence from US computer networks over a 30-day period ending in March 2013."[46]

This massive apparatus of the U.S. intelligence community's programs for the collection of telecommunications data, both of a foreign and domestic nature, was sanctioned for by the passing of the USA PATRIOT Act in October 2001. It was this law, which set the precedent for intrusive surveillance at the expense of privacy, that brought America into the current security versus privacy debate that it is in now. Once the existence of programs like PRISM, Stellar Wind, and Boundless Informant were made known to the worldwide public, the U.S. went on the defensive. U.S. citizens knew immediately that their government had not be forthright with them, and the idea of privacy that they had believed they possessed, was shattered in an instant. To help restore confidence in their government, the Obama Administration acted to respond to the cries for reform. Rather than attempt to defend Section 215 of the USA PATRIOT Act, the Obama Administration decided it was best to start fresh with a new law called the USA FREEDOM Act. The question that remains yet to be answered is, are the Obama-era revisions enough to truly restore the sanctity of privacy once endeared by millions of Americans?

---

[44]MacAskill, Ewen, et al. "NSA Files Decoded: Edward Snowden's Surveillance Revelations Explained."
[45]MacAskill, Ewen, et al. "NSA Files Decoded: Edward Snowden's Surveillance Revelations Explained."
[46]Greenwald, Glenn, and Ewen MacAskill. "Boundless Informant: the NSA's Secret Tool to Track Global Surveillance Data."

End of the Controversy? – USA FREEDOM Act

"…I have called for reforms that better safeguard the privacy and civil liberties of the American people while ensuring our national security…" – Barack Obama[47]

When Edward Snowden released government secrets as to how the U.S. intelligence community was spying on people, including citizens of the United States, there were immediate calls to have the U.S. government step up to the plate, admit its use of these invasive and unprecedented tactics, and reform its ways. Calls for the reinstatement of privacy were coming both from within the U.S. and from allies without. In fact, "in 2015 the United States of Appeals for the Second Circuit found [that] Section 215 of the Patriot Act could not be used to validate the bulk collection of Americans' phone records."[48] The Obama Administration heeded these demands but amending the USA PATRIOT Act.

On June 2, 2015, Barack Obama signed into law the USA FREEDOM Act, standing for Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act.[49] This law sought to amend the more controversial provisions of the USA PATRIOT Act, specifically Section 215. For all intents and purposes, this law banned the bulk collection of data (metadata) through programs like PRISM, it narrowed the government's ability to collect only data that is, "to the greatest extent reasonably practical," it limited the tripartite circles of interest for spying from three hops to two (friends of friends), it allows for private companies to disclose FISA orders it receives, it declassifies important FISA Court opinions, it puts an *amicus curiae* panel on the FISA Court, and it extends the expiration of some of the other less controversial USA PATRIOT Act provisions to December 2019.[50]

---

[47] Office of the Press Secretary. "Statement by the President on the USA FREEDOM Act."
[48] Editors, History.com. "Patriot Act."
[49] "The USA Freedom Act: What Is It and How Does It Affect Your Online Activities."
[50] The Washington Post. "US Freedom Act: What's in, What's Out."

Arguably, this is a step in the right direction for those who champion the rights of telecommunications privacy. At the time of the passage of this law, the Obama Administration touted the Act's ability to truly equip the U.S. intelligence community with the tools it needs to keep America safe, while simultaneously defending American's right to privacy like the USA PATRIOT Act claimed it would in 2001. However, some critics still think that the federal government passed up on an opportunity to take decisive action and stand up for the privacy rights of Americans by choosing a form of a middle ground that made mediocre attempts at righting the past privacy wrongs allowed for by the USA PATRIOT Act. In fact, History.com says, "Despite the act's efforts to protect civil liberties, its critics believe it doesn't go far enough. The benefits of the Patriot Act and the USA Freedom Act to national security will undoubtedly continue to be weighed against the potential intrusion on Americans' privacy and their civil rights."[51]

If the process of the passage of the USA FREEDOM Act is any indication, it seems that no matter what government revisions are made in the context of security and privacy in the realm of telecommunications, America will never again know the privacy of a pre-9/11 world. It does seem that this Obama Administration law is a step toward restoring this privacy, but even with its revisionist efforts, the makers of the law admitted through what they kept in the law that such a pre-9/11 privacy will never exist again. For instance, even the USA FREEDOM Act allows for the, "limited use of bulk data collecting under Section 215 [of the USA PATRIOT Act] in an emergency."[52] The danger in this dormant provision is that who is to say what constitutes an emergency? It is this ingrained fear in Americans caused by 9/11 that will almost ensure that telecommunications privacy will never be the full, robust liberty that it once was. Whether that

[51] Editors, History.com. "Patriot Act."
[52] Editors, History.com. "Patriot Act."

is cause for concern, is up to the reader of this paper. However, the point of this paper is to show that the intelligence apparatus of the U.S. government and the precedent of surrendering privacy for the sake of security in efforts such as telephony metadata collecting, have been created under the institution of the USA PATRIOT Act, and as such, the death of telecommunications privacy has been ushered into the United States.

Biblical and Ethical Arguments

Obviously, this issue of the loss of telecommunications privacy due to warrantless searches and invasive secret government programs ushered in by the USA PATRIOT Act is fraught with political arguments for each side. Some say that in this new age of technology and warfare, a lessening of privacy rights should be expected, and if it is a sacrifice that must be made in order to prevent another terrorist attack like 9/11, then it is worth that sacrifice. Others, like the position of this paper, argue that they know the balance of privacy and security will always favor one side over the other in particular circumstances. However, they recognize that when America's needs for immediate security due to a national emergency have run their course, then the balance should once again favor privacy, since it has been enshrined as a fundamental right in our Constitution.

The fact is, that with the passage of the USA PATRIOT Act security was much more heavily favored at the expense of privacy. Even with the revision of the USA FREEDOM Act, that perpetual balance was not restored because the intelligence and legal precedent has been set and is still present in the new law. This brings up an ethical question about how we are to be governed, and how, from a Christian worldview, are citizens to relate to their government when they know full well that their government could be/has been spying on them. To answer this

question I will be looking at the two Bible verses Romans 13:1-5 and 1 Peter 2:13-17, as well as the basics of John Locke's Social Contract Theory.

Romans 13:1-5 says,

> "Let everyone be subject to the governing authorities, for there is no authority except that which God has established. The authorities that exist have been established by God. **2** Consequently, whoever rebels against the authority is rebelling against what God has instituted, and those who do so will bring judgment on themselves. **3** For rulers hold no terror for those who do right, but for those who do wrong. Do you want to be free from fear of the one in authority? Then do what is right and you will be commended. **4** For the one in authority is God's servant for your good. But if you do wrong, be afraid, for rulers do not bear the sword for no reason. They are God's servants, agents of wrath to bring punishment on the wrongdoer. **5** Therefore, it is necessary to submit to the authorities, not only because of possible punishment but also as a matter of conscience." [53]

The author of this verse is Paul, and he is addressing these comments to Christians living in Rome in the early part of the new A.D. timeline. However, these words still have significance for Christians today because Christians believe the God's Word (the Bible) is active in the world to reveal truth about God. With that being said, to put it in the modern context for the evangelical living in the U.S., we are clearly called to obey those in power over us (the government) because, as Paul makes clear, God has chosen them to inhabit these seats of power for His purposes. However, as is made clear in other parts of Scripture, when man's law and God's Word collide, Christians are called to follow God's law. Although, when God's law and

---

[53] "BibleGateway." *Romans 13 NIV - - Bible Gateway*

man's law coincide, then Paul calls all people, especially Christians, to obey the law. Those who rebel in such a circumstance are also rebelling against the Lord, and should fear punishment.

In the context of the government surveillance and privacy discussion of this paper, in this verse Paul makes it clear that those who rebel, or break the law, from those in power should expect punishment. Therefore, the U.S. government should be able to properly execute surveillance of known suspects in regards to national security in order to build a case against enemies to ensure punishment and justice. It is when such surveillance is performed against law-abiding U.S. citizens that separate courses of action need to be taken, since U.S. citizenship comes with rights and freedoms. Such courses of action might include making the warrants public and involving the judiciary more.

The reason there should be a difference between surveillance tactics of legitimate terrorist suspects and law-abiding U.S. citizens, from a Christian perspective, is because Paul goes on to say that if we as Christians obey the governing authorities when we should (when not in contradiction to God's Word), then we should have no fear of punishment and be secure in our freedom. Interpreted broadly, this should mean that U.S. citizens, if they are law abiding, should have no fear of invasive government programs that violate our privacy and store up metadata about our lives. That means the NSA's programs like Boundless Informant and the like that cause fear of government brings up the ethical dilemma of correct, biblical governance.

Moving on the 1 Peter 2:13-17, which says,

> "Submit yourselves for the Lord's sake to every human authority: whether to the emperor, as the supreme authority, **14** or to governors, who are sent by him to punish those who do wrong and to commend those who do right. **15** For it is God's will that by doing good you should silence the ignorant talk of foolish people.**16** Live as free people, but do

not use your freedom as a cover-up for evil; live as God's slaves. **17** Show proper respect to everyone, love the family of believers, fear God, honor the emperor."[54]

From a Christian perspective, this verse once again highlights the need for Christians to submit the governing authorities, and to the bureaucracies they create (interpreted from verse 14). However, what is also equally clear is that God created mankind to live as free people. Yes, the main emphasis of this freedom is of a spiritual nature, but it is also true that here on earth it is within a free society and governance structure that the God-given image of man and his creative capacity and free will, in whatever measure he may possess it, can express itself, often times for the betterment of his fellow man. We were made to be free. This is incredibly difficult when the fear of undisclosed government surveillance is taking place, often times targeting its own citizens. Our rights and freedoms, which engender a sense of security in and of themselves, are being swept away without the people's' consent. The government should not be using the guise of the protection of freedom to cover up its invasive procedures without the trust and acknowledgment of the people.

Speaking of consent, trust, and acknowledgement of the people, we now turn to John Locke's Social Contract Theory in our ethical discussion. This theory, though pioneered by Thomas Hobbes, is more famously espoused in Locke's *Second Treatise of Government*, in which he tells his audience how government first formed in the world and why. The main point Locke harps on is that before government, man lived in the state of nature, where it was often kill or be killed. Due to the acquisition of property and the chaos that ensued from this state of nature, Locke argues man began to perceive the need for a civilized society, with boundaries (laws) to stop, control, and prevent the violence of mankind. This civilized society would take

[54] "BibleGateway." *Romans 13 NIV - - Bible Gateway*

on the form of government that operated with authority. Locke points out that in order to form this type of structure, two things needed to happen: 1.) the people under the authority of the government had to consent to that government 2.) consent meant to surrender some rights in favor of security. If and when the government overstepped its original purpose and lost the consent of the people, then the people had the right to overthrow the government and begin again, hence the term contract to describe his theory.[55]

At the time of the founding of America, Lockean principles helped to define the American War for Independence and why it was being fought. Later, due to the outcome of that war, those principles were enshrined in the founding and governing documents of the United States, such as the Constitution. Bringing this theory in the argument of the balance between privacy and security, Locke's theory makes clear that protection of citizens is one of government's most important functions, and to accomplish this, some liberties must be surrendered for the sake of security. However, his theory also makes clear that in this contract setting, the citizens of said government are to know what liberties they are surrendering when, to whom, and why. This is where the debate begins. How can U.S. citizens knowingly surrender their right to privacy in favor of security if they are not made aware that their privacy could be in danger from secret government surveillance in the first place? The answer is that they cannot and therefore they do not because they are not informed of the other half of the contract. This is where the U.S. intelligence agencies and government begins to lose the trust of the people when their secret operations are made public due to illegal leaks. This fact is why Barack Obama signed into law the USA FREEDOM Act, which sought to make the dealings of FISA Court

[55] Bennett, Johnathan. *Second Treatise of Government*.

warrants and hearings more public and to scale back the Boundless Informant program, although arguably not far enough.

In summation, the Bible tells Christians to obey governing authorities, as they are used by God to carry out good intended purposes of rewarding good and punishing evil. However, this obedience is presupposed on the principle of the government being straightforward: if you break the law, you will be punished, but if you keep it there is no need to fear. From a more philosophical side, the Lockean Social Contract Theory, which runs deep in American history, makes it clear that the American people have a right to know when their rights are being surrendered, even if it is on their behalf by representatives. The passage of the USA PATRIOT Act, and its revised version the USA FREEDOM Act violate these presuppositions and philosophical theories by still making provision for secret invasive government abuse of U.S. citizens' privacy rights.

Conclusion

In reality, the balance between privacy and security will continue to shift based on world events for the rest of the existence of Western democracy. The passage of the USA PATRIOT Act ushered in the death of true, lasting telecommunications privacy in a way that violates the very fundamental and foundational identity of what it means to be American. Privacy and personal choice has been enshrined in American democracy from day one, but now it is being eroded, with the inability to fully recover, at least in the realm of telecommunications. The laws may have changed and procedures may have shaken up, but the intelligence infrastructure and legal precedent of Sections 213's warrants, 214's wiretaps, and 215's metadata dragnetting of the

USA PATRIOT Act still breathe life. It only takes another 9/11 and these anti-privacy monstrosities will be back to rear their ugly heads, all in the name of national security.

Annotated Bibliography

Kean, T. H., Ben-Veniste, R., Fielding, F. F., Gorelick, J. S., Gorton, S., Hamilton, L. H., . . . Thompson, J. R. (2004, July 22). The 9/11 Commission Report. Retrieved January 24, 2019, from https://www.9-11commission.gov/report/911Report.pdf

This is the 9/11 Commission Report produced to provide the U.S. Government and the American people with answers as to the prelude, happenings, and aftermath of the terrorist attack on the World Trade Center and the Pentagon on September 11, 2001. The Commission's report is comprised of 13 different sections, spanning over 400 pages. This report was intended to lay the groundwork of the coming War on Terror, both domestically and abroad. Its purpose was to illustrate to the American people the lack of government security in preventing the attacks, and the necessary steps needed to be taken to have the government fulfill its role as gatekeeper to the protection of American citizens.

N. (n.d.). Government Efforts Before and After the September 11 Attacks. Retrieved January 25, 2019, from http://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Ch3.pdf

This document is chapter 3 of a publication from the National Commission on Terrorist Attacks Upon the United States. It is a part of the broader publication from the U.S. Government entitled the Terrorist Financing Staff Monograph. This document looks at the lack of government accountability in relation to the 9/11 terrorist attacks. Specifically, it takes a chronological approach to the intelligence community's lack of resources and involvement in surveilling terrorist networks domestically and abroad. It categorizes the FBI's lack of incriminating data to stop the 9/11 attack before it happened and cites the shortcomings of FISA and the Department of Justice. It proceeds to cover domestic law enforcement shortcomings and the ways that it needs to be buffed up in the future for the protection of Americans.

Crisis Management and Response Post-September 11. (n.d.). 150-170. Retrieved January 25, 2019, from http://govinfo.library.unt.edu/911/staff_statements/911_TerrTrav_Ch6.pdf

This document is a U.S. State Department staff statement report about the efficiency of the U.S. Government's response to the 9/11 attack. The statements focus mostly on immigration mandates, policies, and shortcomings that reach across the bureaucracy to INS, the State Department, and the CIA. Mostly, this report addresses the need for more intense screening and travel policy to prevent another 9/11-like attack. It also provides American citizens with a rundown of State Department and other bureaucratic agencies' programs and their successes and findings that have been implemented since 9/11.

McNeill, Jena Baker. "The PATRIOT Act and the Constitution: Five Key Points." *The Heritage Foundation*, 10 Feb. 2011, http://www.heritage.org/homeland-security/report/the-patriot-act-and-the-constitution-five-key-points.

This is a journal article covering specific hotly-debated aspects of the USA PATRIOT Act from the conservative-leaning Heritage Foundation. More specifically, the article covers five basic points on how the act is beneficial to the U.S. and still upholds Constitutional standards. The five aspects that the author of the article point to all relate to privacy, arguing that the act does not grant the government carte blanche to impose on a citizen's right to privacy. This factual defensive of the act provides a pro-establishment view as to the usefulness of the law.

Sensenbrenner, J. F., Jr. (2001, October 26). H.R.3162 - 107th Congress (2001-2002): Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. Retrieved January 24, 2019, from https://www.congress.gov/bill/107th-congress/house-bill/03162

This is the word for word legislation of the USA PATRIOT Act. It comes for the website of the U.S. Congress, and it is the detailed legislation about enhancing government measures and tactics within the bureaucracy to prevent terrorist attacks in the United States. It covers subjects ranging from the intelligence community, immigration services, rules and regulations on the banking industry, etc. It laid the groundwork for the functions of the government in its political fight against the War on Terrorism.

Selected Speeches of President George W. Bush: 2001-2008. (n.d.). Retrieved January 25, 2019, from https://georgewbush-whitehouse.archives.gov/infocus/bushrecord/documents/Selected_Speeches_George_W_Bush.pdf

This source is a collection of speeches by former President George W. Bush. I specifically choose his speech on September 20, 2001 to a joint session of Congress. This speech was given in the shadow of 9/11 as a form of a State of the Union in which Bush made demands on behalf of the U.S. government to the terrorist organization called Al-Qaeda that was being harbored by the Taliban in Afghanistan. In this speech, Bush prepared the country, including the military, for the War on Terror. Specifically, he told the people that this fight would be a long and hard one, and he also created the cabinet-level position of Department of Homeland Security. On top of this, this speech given by Bush was also used to outline the soon-to-be-formed coalition of Western powers that would invade Afghanistan.

Rosenzweig, P., Stimson, C., & Shedd, D. (2016, May 13). Maintaining America's Ability to Collect Foreign Intelligence: The Section 702 Program. Retrieved January 24, 2019, from https://www.heritage.org/defense/report/maintaining-americas-ability-collect-foreign-intelligence-the-section-702-program - _ftn2

This source is an online journal editorial published by the conservative think tank policy formulator called The Heritage Foundation. This article was written at the time that Section 702 of the FISA Act was up for a vote on re-installment. Heritage takes the pro-re-installment stance, arguing that the Act provides for the necessary tools needed by the intelligence community to protect the country from terrorist attacks. The article also addresses the pros and cons of the act, and it touches on the subject of Section 702 authorizing incidental spying on American citizens. Heritage argues that this is mostly conjecture and an ideological concern.

Mann, S. F. (2014, February 27). Fact Sheet: Section 215 of the USA PATRIOT Act. Retrieved January 25, 2019, from https://www.csis.org/analysis/fact-sheet-section-215-usa-patriot-act

This source is an article published by the Center for Strategic and International Studies. It addresses Section 215 of the USA PATRIOT Act, which allows the government to collect tangible items for the purpose of surveillance. This article mentions the controversy over the section, especially after the Edward Snowden leak of classified NSA information. Also, it assesses the legitimacy of bulk telephony metadata collection.

Gallagher, R. (2013, June 06). NSA Collecting Phone Records for Millions of U.S. Verizon Customers. Retrieved January 25, 2019, from https://slate.com/technology/2013/06/nsa-verizon-phone-records-national-security-agency-order-collects-metadata-from-millions-of-americans.html

This source is an article from Slate detailing how the NSA has used specific provisions from the USA PATRIOT Act that allowed it to collect phone data records from U.S. citizens. The article specifically refers to Verizon Wireless customers. It addresses how FISC court-ordered the handing over of data referring to phone calls, including duration. Most of the data collecting was done regarding Verizon business customers in America. The article also covers how the collecting of this metadata was ordered after the heightened terror situation of the Boston Marathon Bombing.

Risen, J., & LICHTBLAU, E. (2005, December 16). Bush Lets U.S. Spy on Callers Without Courts. Retrieved January 25, 2019, from https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html

This is a New York Times article that dives more in depth to the NSA telephony metadata collection and the concerns that citizens have about how the Bush Administration has potentially skirted their right to privacy. On top of this concern, the article also addresses the lack of needing warrants for specific government agencies to collect this intelligence. Finally, the New York Times article mentions how the Bush Administration thought this measure was necessary because of how the terrorist attack on 9/11 highlighted the level of unpreparedness of U.S. intelligence agencies.

Thorp, F., V. (2015, June 2). Barack Obama Signs 'USA Freedom Act' to Reform NSA Surveillance. Retrieved January 24, 2019, from https://www.nbcnews.com/storyline/nsa-snooping/senate-vote-measure-reform-nsa-surveillance-n368341

This source is an NBC News article that addresses former President Obama signing into law the USA FREEDOM Act. This law was intended to revise the NSA's telephony metadata collection strategy. Its purpose was to address the surveillance controversy that was unleashed by Edward Snowden, who was a former NSA worker. The article quotes Barack Obama as touting the law's ability to provide the country with protection from terrorism and protect citizens' right to privacy.

Clauson, Marc; Ferkaluk, Emily K; Lyons, Justin D; Rich, David; Sims, Kevin; Smith, Mark Caleb. (2019). Anti-Federalist Papers No. 2: We Have Been Told of Phantoms. *Rendering to God and Caesar: Critical Readings For American Government* (pg. 73). Salem, Wisconsin: Sheffield Publishing Company

This source is a political science book that contains influential political and historical thinkers throughout generations that address topics ranging from federalism to biblical perspectives of government enterprises. I chose to specifically single out an Anti-Federalist publication from an another with the pseudonym Brutus, written in 1787. This specific work capitalizes on the need for the protection of liberty from the government, and it champions certain rights. I believe the political theories ingrained in this work still echo loudly today in the American mind when addressing the right to privacy and the government's role in protecting its citizens.

Klau, Daniel. "Privacy, Security, and the Legacy of 9/11." *UConn Today*, UConn Today, 7 Dec. 2015, today.uconn.edu/2015/09/privacy-security-and-the-legacy-of-911/.

This source is a University of Connecticut publication, written from the department of UCONN Law. It was published 14 years after 9/11, and by utilizing a Q&A format, it addresses the questions of the right to privacy, the USA PATRIOT Act, and the NSA leaks of Edward Snowden. For the most part, the publication attempts to stray away from bias and stick to the facts.

NSA Surveillance. (n.d.). Retrieved January 25, 2019, from https://www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance

This source is a publication from the ACLU. It addresses, from a politically left-leaning perspective, the legality of the NSA's surveillance procedures on American citizens. It takes the stance that these tactics and strategies are unlawful and need to be fought against. On a more practical footing, this publication also defines the major bureaucratic agencies involved in the privacy vs. security debate centered around the terrorist attacks of 9/11. It introduces the reader to FISA, the NSA, and Executive Order 12,333. On top of this, the publication then moves on to list the lawsuits it has waged to right what it views as an infringement of American citizens' rights.

"President Bush Addresses the Nation." *The Washington Post*, WP Company, 20 Sept. 2001, www.washingtonpost.com/wp-srv/nation/specials/attacked/transcripts/bushaddress_092001.html.

This source is the written transcript of President George W. Bush's speech addressing a joint session of Congress on September 20, 2001. It was written and posted by the Washington Post.

Clapper, James R. "How 9/11 Transformed the Intelligence Community." *The Wall Street Journal*, Dow Jones & Company, 7 Sept. 2011, www.wsj.com/articles/SB10001424053111904537404576554430822300352.

This source is an excerpt from a Wall Street Journal article by James Clapper talking about the lack of the U.S. government in providing protection and security from terrorist attacks, such as the one from 9/11.

"THE USA PATRIOT ACT IN PRACTICE: SHEDDING LIGHT ON THE FISA PROCESS." *Senate Judiciary Committee Hearing on FISA Oversight: September 10, 2002*, fas.org/irp/congress/2002_hr/091002transcript.html.

This source is the excerpt from the Senate Judiciary Committee of 2002 discussing what the USA PATRIOT Act is and why it was created. Most of the script talks about how the USA PATRIOT Act amends the FISA Act.

Sharp, Tim. "Right to Privacy: Constitutional Rights & Privacy Laws." *LiveScience*, Purch, 12 June 2013, www.livescience.com/37398-right-to-privacy.html

This source is a publication by Tim Sharp posted in *Live Science* that discusses the Constitutional amendments that deal with privacy. This publication also offers a definition of privacy and depicts the balance of privacy and security. Sharp also discusses privacy jurisprudence cases and how they have led to the current status of privacy in America.

"Privacy." *Merriam-Webster*, Merriam-Webster, www.merriam-webster.com/dictionary/privacy.

This is a straight-forward dictionary definition of the term "privacy."

ACLU. "How the USA-Patriot Act Expands Law Enforcement 'Sneak and Peek' Warrants." *American Civil Liberties Union*, www.aclu.org/other/how-usa-patriot-act-expands-law-enforcement-sneak-and-peek-warrants.

This source is from the American Civil Liberties Union and discusses Section 213 of the USA PATRIOT Act. This publication has a biased anti-USA PATRIOT Act bent, discussing how this section of the law destroys the integrity of warrants and the Fourth Amendment to the Constitution.

DeRosa, Mary, et al. "Patriot Debates." - *Section 213*, apps.americanbar.org/natsecurity/patriotdebates/section-213.

This source is a publication written by three authors that seeks to interpret Section 213 of the USA PATRIOT Act. Each author provides their own section and interpretation of the section in relation to how it relates to the privacy versus security debate.

Oyez. "Griswold v. Connecticut." 11 Apr. 2019, www.oyez.org/cases/1964/496.

This source is from a database of Supreme Court cases website. Specifically, it is a case about the establishment and recognition of the right to privacy at the federal level with *Griswold v. Connecticut*. In this 1965 case, the Supreme Court uses the issue of contraceptives to establish the existence of the right to privacy.

"USA Patriot Act Myth vs Reality ." *Preserving Life & Liberty Dispelling the Myths*, Department of Justice, www.justice.gov/archive/ll/subs/add_myths.htm#s213.

This source is from the Department of Justice. It is an online government publication that seeks to provide facts and support for the existence of the USA PATRIOT Act. Specifically, this publication deals with Section 213 of the law, describing how its inclusion is essential to the War on Terror.

"William J. Brennan Quote." *Right to Privacy Quotes*, AZ Quotes, www.azquotes.com/quote/838215?ref=right-to-privacy.

This is a website that has a collection of famous quotes about privacy right said by influential people. This specific quote is from U.S. Supreme Court Justice Brennan, who helped to created the Court's jurisprudence on privacy rights.

"18 U.S. Code § 3121 - General Prohibition on Pen Register and Trap and Trace Device Use; Exception." *Legal Information Institute*, Cornell Law School, www.law.cornell.edu/uscode/text/18/3121.

This source is an explanation from Cornell Law School of the U.S. Legal Code with specific regard for how it affects Section 214 of the USA PATRIOT Act. This publication offers a definition for wiretaps, pen registers, and trap and trace devices.

ACLU. "Surveillance Under the USA/PATRIOT Act." *American Civil Liberties Union*, 2019, www.aclu.org/other/surveillance-under-usapatriot-act.

This publication is from the American Civil Liberties Union, which is against vast swaths of the USA PATRIOT Act. In this specific publication, the ACLU outlines its basic arguments as to how the USA PATRIOT Act violates the right to privacy and degrades the Fourth Amendment. More precisely, this article discusses why from the ACLU's perspective the Act was passed, and how Sections 213 through 215 in particular violate privacy rights.

"Edward Snowden Quotes." *BrainyQuote*, Xplore, www.brainyquote.com/authors/edward_snowden.

This is a quote database website. It's pretty self-explanatory.

Greenwald, Glenn. "NSA Collecting Phone Records of Millions of Verizon Customers Daily." *The Guardian*, Guardian News and Media, 6 June 2013, www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

This is a publication from *The Guardian* in 2013 that discusses how the Bush Administration allowed for the NSA to collect U.S. citizens telephone records, specifically from Verizon customers which is the largest telephone network in the United States.

Lee, Timothy B. “Here's Everything We Know about PRISM to Date.” *The Washington Post*, WP Company, 12 June 2013, www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/?utm_term=.8d67a5385f32.

This is a publication from *The Washington Post* that discusses the nature of the NSA’s PRISM program that was released from the ex-CIA official Edward Snowden. This program allows for the NSA to access internet history of users from nine different search engine sites.

Szoldra, Paul. “This Is Everything Edward Snowden Revealed in One Year of Unprecedented Top-Secret Leaks.” *Business Insider*, Business Insider, 16 Sept. 2016, www.businessinsider.com/snowden-leaks-timeline-2016-9.

This source is a publication from *Business Insider* that offers a timeline and explanation of the government secrets that Edward Snowden revealed.

MacAskill, Ewen, et al. “NSA Files Decoded: Edward Snowden's Surveillance Revelations Explained.” *The Guardian*, Guardian News and Media, 1 Nov. 2013, www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

This source is a publication from *The Guardian* that discusses in more detail the programs that Edward Snowden revealed, such as Boundless Informant, Heartbeat, and PRISM.

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

This source discusses the reaches of the Boundless Informant program that revealed how the U.S. intelligence community was dragnetting for metadata information. This source shows the three circles of influence the NSA was allowed by law to spy on.

Office of the Press Secretary. "Statement by the President on the USA FREEDOM Act." *National Archives and Records Administration*, National Archives and Records Administration, June 2015, obamawhitehouse.archives.gov/the-press-office/2015/06/02/statement-president-usa-freedom-act

This source is an official press release located in the National Archives. It is a statement from Obama about why the his administration signed the USA FREEDOM Act into law and how it is the reformed USA PATRIOT Act.

Editors, History.com. "Patriot Act." *History.com*, A&E Television Networks, 19 Dec. 2017, www.history.com/topics/21st-century/patriot-act.

This source is from *History* and it discusses in brief the purpose and controversy of the USA PATRIOT Act.

"The USA Freedom Act: What Is It and How Does It Affect Your Online Activities." *Pixel Privacy*, 2019, pixelprivacy.com/resources/freedom-act/.

This publication describes the new Obama-era law USA FREEDOM Act. It seeks to describe how the law differs and is similar to the USA PATRIOT Act.

The Washington Post. "US Freedom Act: What's in, What's Out." *The Washington Post*, WP Company, June 2015, www.washingtonpost.com/graphics/politics/usa-freedom-act/.

This source is about the USA FREEDOM Act and how it compares to the USA PATRIOT Act. This comes in the wake of the Snowden government leaks.

"BibleGateway." *Romans 13 NIV - - Bible Gateway*, Bible Gateway, www.biblegateway.com/passage/?search=Romans%2B13&version=NIV.

This is a Bible verse from an online Bible publication service called Bible Gateway.

Bennett, Johnathan. *Second Treatise of Government*. Jan. 2005, www.earlymoderntexts.com/assets/pdfs/locke1689a.pdf.

This publication is a book from John Locke that describes a theory of government called the Social Contract Theory.