A Comparative Analysis of the USA PATRIOT Act of 2001 to the USA FREEDOM ACT of 2015: Balancing Security with Liberty

2015

Richard L. Russo
University of Central Florida

A COMPARATIVE ANALYSIS OF THE USA PATRIOT ACT OF 2001 TO THE USA FREEDOM ACT OF 2015: BALANCING SECURITY WITH LIBERTY

by

RICHARD L. RUSSO

A thesis submitted in partial fulfillment of the requirements
for the Honors in the Major Program in Legal Studies
in the College of Health and Public Affairs
and in The Burnett Honors College
at the University of Central Florida
Orlando, Florida

Fall Term 2015

Thesis Chair: David Slaughter, J.D.

ABSTRACT

Freedom and safety are two ideals that American citizens value greatly; however, the balance between privacy and security determines whether or not both can be achieved in a reasonable manner. Security and privacy are not mutually exclusive; however, they tend to exhibit an inverse correlation with regards to maintaining individual liberties. Security and privacy are highly beneficial, but when one is given too much weight, the other most often suffers. When the United States citizens are given too much privacy through regulations, the citizens risk their well-being by not allowing the government the ability to prevent dangerous activities being done by criminals. Citizens are unable to defend themselves against foreign and domestic threats of terrorism that affect large amounts of people such as bombings in public settings; however, the federal government can help to prevent such attacks in public settings through surveillance of public areas and monitoring of internet and intracellular communications. When the United States federal government is given too much discretion in security powers through legislation, citizens are at risk of losing their civil rights granted in the Bill of Rights and in Supreme Court cases. The United States of America has had a dangerous imbalance of power in favor of national security since the adoption of the USA PATRIOT Act in 2001, and the imbalance has continued to the present even after the passage of the USA FREEDOM Act in 2015.

This thesis will be a comparative analysis of the USA PATRIOT Act of 2001 to the USA FREEDOM Act of 2015. This thesis will show what specific powers are granted through provisions of the acts, whether or not the provisions are unconstitutional, how the privacy and security of American citizens will change due to the provisions in the USA FREEDOM Act, and

suggestions for how the United States federal government can continue to tilt the balance between security and liberty to ensure more protection for civil liberties and a decrease in national security powers. The suggestions will include three options for gaining the protection of civil liberties and the elimination of certain national security powers and the options are through Supreme Court cases on national security laws pertaining to individual cases or states, Congress passing concurring minor bills with the proposed plan to fully repeal granted national security powers without disturbing congressional alliances on other measures, and Congress passing a single act called the State Surveillance Repeal Act in order to fully repeal the USA PATRIOT Act provisions that would still be in effect after the passage of the USA FREEDOM Act.

DEDICATION

This thesis is dedicated to the United States citizens who had their civil rights violated because of the provisions of the USA PATRIOT Act.

ACKNOWLEDGEMENTS

Immense appreciation and sincere gratitude is owed to the following professionals who contributed in many ways to the production of this thesis.

Prof. David Slaughter J.D., Thesis Committee Chair, for his constant support, time, and guidance.

Dr. Barry Edwards J.D., Ph.D., Committee Member, for his advice and wisdom.

Prof. Timothy Ravich J.D., Committee Member, for his suggestions and knowledge.

Dr. Paul Reich Ph.D., Thesis Format Reviewer, for his time and help with formatting.

Prof. James A. Beckman J.D., LL.M., Department Chair, for his approval and suggestions.

Director Denise Crisafi M.A., HIM Director, for her guidelines and support.

Director Kelly Astro M. Ed., Director of Research and Civic Engagement, for her advice and support.

TABLE OF CONTENTS

Chapter 1: Introduction

The USA PATRIOT Act of 2001 was highly controversial and arguably contrary to the United States Constitution, specifically with respect to the federal right of privacy. While some of the powers granted to the United States federal government in the sections of the USA PATRIOT Act were necessary to cope with foreign terrorist threats after the September 11th World Trade Center attacks, the United States Congress drastically expanded the government's powers in an attempt to prevent another attack. Many of the sections of the USA PATRIOT Act were inconsistent with the ideals of American history; the sections were more suitable for a totalitarian government. Court cases such as *Doe v. Gonzales*, 546 U.S. 1301 (2005) and *Mayfield v. United States*, 504 F. Supp. 2d 1023 (2007), as well as whistle blowers such as Edward Snowden were instrumental in exposing the abuses of power by the National Security Administration under the USA PATRIOT Act. The highly controversial provisions will be explored in Chapter 2 in order to show the need for the USA FREEDOM Act and how the societal and governmental effects of the USA PATRIOT Act differ from the USA FREEDOM Act with regards to the privacy of United States residents. The USA FREEDOM Act of 2015 was created as a means of extending many of the national security powers granted in the USA PATRIOT Act of 2001, while making modifications to deal with public demands for increased transparency and protection of civil liberties. The adjustments were allegedly designed to allow for greater compliance with the United States Constitution; however, whether or not that is true remains to be discussed in the following chapters.

Brief Overview: The Right to Privacy

The inconsistencies between the USA PATRIOT Act's provisions and the United States Constitution's guarantee of the right to privacy are one of the chief concerns of this thesis. The right to privacy is largely considered to have been granted to United States citizens via Supreme Court Justice William O. Douglas' majority opinion in *Griswold v. Connecticut*, 381 U.S. 479 (1965):

> The Warren Court's most famous privacy case, *Griswold v. Connecticut (1965),* is often cited as the case in which the Court 'established' the right to privacy. The case involved a challenge to the constitutionality of a Connecticut law that made it a crime to provide married persons with information on how to prevent conception. 'We deal,' wrote Justice Douglas, 'with a right of privacy older than then Bill of Rights---older than our political parties, older than our school system… Various amendments to the Constitution, Douglas said, 'have penumbras formed by emanations from those guarantees that help give them life and substance.' He then offered a quick catalog: the First Amendment protects the freedom of association; the Third Amendment prohibits the quartering of troops in one's home; the Fourth Amendment protects from unreasonable searches and seizures; the Fifth Amendment prevents government intrusion by granting a privilege against self-incrimination; and the Ninth Amendment provides that the enumeration of certain rights is not intended 'to deny or disparage others retained by the people' (Lane, 2009, p.156)[1].

While this opinion was the first formal expression of the right to privacy in a Supreme Court Case, the right to privacy had long been seen as a civil right inherent in American values since the inception of the United States federal government, "The official birthdate of the 'right to privacy' in the United States, then, is December 15, 1791, the day on which the eleventh of thirteen states--- Virginia--- ratified the Bill of Rights. But its conception was decades earlier, when the British government began ignoring the basic rights and privileges of its citizens. The

[1] Lane, F. S. (2009). *American Privacy: The 400-Year History of Our Most Contested Right.* Boston, MA, USA: Beacon Press.

founding of the American republic gave the former British colonists an opportunity to reaffirm basic human rights, including privacy…" (Lane, 2009, p.17).

Chapter 2: Summary of USA PATRIOT Act

While some of the powers granted to the United States federal government in the USA PATRIOT Act's sections were necessary to deal with foreign terrorist threats after the September 11th World Trade Center attacks, this thesis will be focusing on problematic sections of the USA PATRIOT Act in order to demonstrate how the USA FREEDOM Act has repaired some of the problems that were created by the USA PATRIOT Act. The United States Congress had an opportunity to address the inherent problems with the passing of the USA PATRIOT Improvement and Reauthorization Act of 2005; however, Congress failed to do so by reauthorizing 14 of the 16 "sunsetted" USA PATRIOT Act provisions and by placing four-year sunsets on the other two, which were the authority to conduct roving surveillance (Section 206) and the authority to request production of business records (Section 215). "Sunsetted" provisions are simply measures within a statute that state that the law shall cease to have effect after a specific date, unless further legislative action is taken to extend the law.

The controversial provisions that are not in compliance with the United States Constitution and that cause detrimental effects to American society are sections 203(b) and (d), 206, 215, 213, and 505. These sections will be analyzed to show how their texts specifically grant enormous amounts of power to the national security agencies and how they severely infringe on the civil liberties of Americans.

Sec. 203(b) and (d)

Section 203 deals with the federal government's authority to share electronic, wire, and oral interceptions between intelligence agencies and other parts of the federal government. Section 203(b) and (d) were highly controversial since their adoption because they drastically changed the way criminal and intelligence investigations had been handled prior to 2001. The United States Congress proposed that the bill was necessary to break down barriers between criminal and intelligence investigations; however, most of the powers granted by this section were already specifically given to law enforcement officials, such as sharing grand jury information between foreign intelligence and criminal justice agencies. The following are the main parts of Section 203(b) and 203(d):

> Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information (USA PATRIOT Act, 2001, Section 203(b))…Notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)) or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information (USA PATRIOT Act, Pub. L. 107-56, 2001, Section 203(d)).

The main problem with Section 203(b) and (d)'s text is that their vagueness allows for unlimited sharing among intelligence and criminal justice agencies without any probable cause and for any type of crime. The potential dangers of this freedom of sharing information are vast and clearly against the Fourth Amendment's guarantee of freedom from unreasonable searches (U.S. Const. Amend. IV). Section 203(b) would allow for agencies such as the National Security Administration to conduct unreasonable searches by monitoring innocent people's online actions through local criminal justice agencies without any probable cause. The National Security Administration would legally be allowed to conduct such searches by simply claiming that there was a potential for terrorist activity without using any factual information to back up the claims.

Sec. 206

Section 206 is one of the shortest sections of the entire act due to it solely being an adjustment to the Foreign Intelligence Surveillance Act of 1978, yet it has raised more issues than almost any other section. Section 206 deals with roving surveillance authority for national security agencies and is as follows: "Section 105(c) (2) (B) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(c) (2) (B)) is amended by inserting, 'or in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons,' after 'specified person'" (USA PATRIOT Act, Pub. L. 107-56, 2001, Section 206).

Although Section 206 seems very limited, its effects are considerable on the ability to gather information on citizens. This section destroys barriers that were put in place in 1978 to prevent national security agencies from infringing on citizens' right to privacy guaranteed by the

Bill of Rights. Section 206 would make gathering information much easier for national security agents by allowing one wiretap authorization to cover multiple devices, eliminating the requirement for separate court authorizations for a suspect's different devices, such as for their iPhone, laptop, and tablet. The even larger problem with Section 206 is that it would put innocent people that had accidentally communicated with a criminal at risk of being monitored unknowingly. The problem with innocent citizens being monitored by national security agents is that it makes private conversations public and makes citizens feel that they have to restrict their speech out of fear of saying something that can be interpreted the wrong way to get them into trouble with the law. For example, if someone were to contact his/her employer via email and not know that the employer was breaking laws, the National Security Agency would have justified cause to search through their entire email database to check if he/she were associated with the employer's actions. The National Security Agency could then search the emails of the innocent employees to see if they have been involved in any other illegal activity and send that information to state and federal prosecutors to charge them. The gathering of evidence by national security agents through third-person accounts would make the entire criminal trial system completely unfair for defendants and would violate many amendments such as the Sixth Amendment by not allowing defendants to confront their witnesses. State and federal prosecutors would be able to use incriminating information from national security agents' metadata, while presenting their source of information as anonymous.

The harmful and reprehensible effects of this act were exposed in *Mayfield v. United States* in 2007. A Portland attorney named Brandon Mayfield was wrongly suspected of involvement in the Madrid train bombing case in 2004, due to illegally obtained information by

the federal government's intelligence agencies. Mayfield challenged the National Security Administration's secret surveillance of his home and law office arguing that the USA PATRIOT Act's Section 206 violated his Fourth Amendment right against unreasonable searches and seizures and won at the district level. Unfortunately, Mayfield never got his case to be heard at the appellate level due to a monetary compensation agreement he had reached with the federal government.

Advocates of Section 206 complain that without the breaking of the barriers established in 1978, the jobs of security agents would be too difficult and the process of gathering information would take too long. The typical argument is presented as follows:

> A roving or multi-point wiretap is tied to individuals and enables intelligence officials to obtain a single order that covers any communications device used by the target of the surveillance. In the absence of such authority, government officials would be required to seek a new court order every time a change in the location, phone, or computer occurred (Lungren, 2012, p.436)[2].

This argument for the increased national security powers in searching for possible terrorist threats is reasonable in that it Section 206 does make searching for evidence much easier for national security agents; however, it does not take into account the possible ramifications of being able to access information on a roving wiretap basis. The allowance of roving wiretaps on suspects completely ignores Supreme Court precedent and Fourth Amendment requirements of having specific warrants for each search. The ability of an agent to search multiple sources with a single roving wiretap approved by court order essentially invalidates the entire point of having a warrant, which is to ensure that people are searched in reasonable ways for specific purposes.

[2] Lungren, D. E. (2012). Congressional Perspective on the Patriot Act Extenders, *A. Notre Dame JL Ethics & Pub. Pol'y*, *26*, 427.

Roving wiretaps allow for multiple parties and pieces of information that were not originally sought in the warrant to be included in an umbrella of searching procedures that are very inclusive and general to the point where they would not be considered reasonable evidence finders in a federal criminal court of law.

Sec.215

Section 215 is dangerous because of its use of vague terminology to expand the ability of federal agencies to access records. The main text of Section 215 is as follows:

> The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution (USA PATRIOT Act, Pub. L. 107-56, 2001, Section 215).

The problem with Section 215 is that it permits the FBI Director to force a citizen to produce “any tangible things” without complying with the Fourth Amendment. The statement “any tangible things” vaguely gives the FBI unconstitutional power to conduct unreasonable searches and seizures of citizens’ records.

Section 215’s secretive measures were exposed by one of the most infamous leaks of national security information in United States history. Edward Snowden, a Central Intelligence Agency employee, leaked information on the National Security Administration’s abuse of Section 215 in its metadata and telecommunication record gathering tactics. The National

Security Administration had clearly been violating the Fourth Amendment and using Section 215's vague language as cover:

> Critics of the program point to the presumptively relevant definition from section 215. This includes records relating to an agent of a foreign power and individuals in contact with a suspected agent of a foreign power. It is clear that nearly all of the records obtained from Verizon and other phone service providers will not meet these criteria. Critics therefore believe that the FBI bears the burden of showing why those records are in fact relevant and should be included in the orders. Opponents further argue that 'everything' nullifies the relevance limitation in the statute. Essentially, they contend that if law enforcement always has access to all records, they can inevitably identify a subset of records as 'relevant'—yet that renders the term 'relevant' essentially meaningless. In construing a statute, courts are supposed to give meaning to every word that Congress used, but by defining bulk collection as relevant, they would in effect be ignoring that term. Furthermore, the government has acknowledged that the vast majority of the data collected under the orders is not relevant to any investigation. Allowing the NSA to determine what is relevant once the data is in their possession violates the plain meaning of the statute. In essence, critics contend that the NSA is applying the prerequisite for collecting records retroactively. The statute requires that there be grounds to believe the data is relevant prior to collection, but that determination cannot be made until the records are actually in the NSA's possession and undergoing analysis (McGowan, 2013, p.2426-2427)[3].

Sec. 213

Section 213 deals with the federal agencies' authority to delay the notice of the execution of a warrant and has commonly been referred to as the "sneak and peak warrant" section. The main text of Section 213 is stated as follows:

> Delay.--With respect to the issuance of any warrant or court order under this section, or any other rule of law, to search for and seize any property or material that constitutes evidence of a criminal offense in violation of the laws of the United States, any notice required, or that may be required, to be given may be delayed if-- ``(1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705); ``(2) the warrant prohibits the seizure of any tangible property, any wire or electronic communication (as

[3] McGowan, C. J. (2013). Relevance of Relevance: Section 215 of the USA PATRIOT Act and the NSA Metadata Collection Program, *The. Fordham L. Rev., 82*, 2399.

> defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and ``(3) the warrant provides for the giving of such notice within a reasonable period of its execution, which period may thereafter be extended by the court for good cause shown (USA PATRIOT Act, Pub. L. 107-56, 2001, Section 213).

The powers granted in Section 213 go against many Supreme Court rulings over the last century with regards to searches and seizures. The section allows for the search and seizure of any property or material that constitutes evidence of any criminal offense, even a misdemeanor, without a warrant. The home has always been regarded as a safe haven by the United States Supreme Court and this clause would clearly make that no longer the case. The abuses by federal agencies against noncitizens living in the United States by using Section 213 can be explained as follows:

> The first major piece of legislation to respond to apparent weaknesses in U.S. national security, the statute expanded the range of aliens who could be excluded or deported from the United States on terrorism-related grounds, while reducing the procedural protections available to them. Under the new law, immigrants "certified" as threats to national security must be held in government custody without bond pending deportation proceedings and removal from the country. Detention could become indefinite for those aliens found to be deportable but whom other countries decline to accept. As the USA PATRIOT Act went into effect, several hundred immigrants remained in government detention under a separate emergency order allowing them to be held without charge for an extended period. The lengthy detention of so many aliens, few of whom were suspected of involvement in the terrorist attacks, generated concern that efforts to protect national security in the wake of September 11 had infringed on the constitutional rights of noncitizens (Sinnar, 2003, p. 1419)[4].

Sec.505

[4] Sinnar, S. (2003). Patriotic or unconstitutional? The mandatory detention of aliens under the USA PATRIOT Act. *Stanford Law Review*, 1419-1456.

Section 505 dealt with the detainment of citizens suspected of committing terrorist activities, imposed due process limitations on suspects of terrorism and authorized the power to issue National Security Letters to organizations for communications compliance. The following excerpt from the section shows how the federal government was able to accomplish all of the above in a concise manner:

> TELEPHONE TOLL AND TRANSACTIONAL RECORDS.—Section 2709(b) of title 18, United States Code, is amended— (1) in the matter preceding paragraph (1), by inserting ‘‘at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director’’ after ‘‘Assistant Director’’; (2) in paragraph (1)— (A) by striking ‘‘in a position not lower than Deputy Assistant Director’’; and (B) by striking ‘‘made that’’ and all that follows and inserting the following: ‘‘made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States; and’’; and (3) in paragraph (2)— (A) by striking ‘‘in a position not lower than Deputy Assistant Director’’; and (B) by striking ‘‘made that’’ and all that follows and inserting the following: ‘‘made that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution of the United States (USA PATRIOT Act, Pub. L. 107-56, 2001, Sec. 505).

Section 505 made National Security Letters apply to electronic communications service provider records, credit reports, and financial records. The National Security Letters were not subject to court approval, they did not require national security agencies to prove that there was any connection between the orders and the suspected foreign terrorists, and recipients of the letters were legally barred from telling anyone that they had received the orders. The recipients of National Security Letters were forced to comply with the intelligence gathering measures and were not legally entitled to challenge the demands. The forced secrecy and compliance caused

many problems for falsely accused citizens, as was eventually discovered in many court cases such as in *Mayfield v. United States*, 504 F. Supp. 2d 1023 (2007). In *Mayfield vs. United States*, Brandon Mayfield, a law-abiding citizen from Oregon, was linked by substandard FBI lab work to the 2004 Madrid train bombings, lost his freedom for two weeks by being jailed, harassed, and held as a primary suspect for treason, a crime punishable by death. After being falsely accused due to information gathered from the Federal Bureau of Investigation wiretapping his home, he was jailed in the United States until Spanish authorities captured the real terrorists.

Chapter 3: Summary of USA FREEDOM Act

The USA FREEDOM Act was signed into law on June 2, 2015 by President Barack Obama. Although The USA FREEDOM Act is not perfect, it is about as good as practically possible of a compromise that could have been achieved during the Congressional gridlock. The United States Congress was heavily divided on the issue of whether or not to limit the national security powers of the USA PATRIOT Act upon the expiration of many of its provisions. Many Representatives and Senators were against any limitation of national security powers but in the end the USA FREEDOM Act was compromised and thus allowed for a decrease of national security power that were highly unlikely to pass through both houses of the United States Congress. The USA FREEDOM Act enacts extensive reforms to surveillance programs by ending bulk collection of all records, preventing government overreach, allowing challenges to national security letter gag orders, creating a panel of experts at the FISA court, and mandating transparency. The USA FREEDOM Act provides for all of these drastic changes in favor of civil liberties while still preserving and adding necessary security powers to deal with foreign terrorist threats. The USA FREEDOM Act is able to provide all of these changes while still preserving necessary security powers by still allowing amended types of data collection, invoking counter-terrorist forces inherent in international treaties, and still allowing many of the processes created by the USA PATRIOT Act only on a more transparent and controlled level. An example of a process created under the USA PATRIOT Act that will be continued under the USA FREEDOM Act to ensure necessary security powers is the issue of national security letter gag orders to corporations and individuals only with the added requirement of allowing narrower search terms and the ability of corporations to challenge such letter gag orders in federal courts. Some of the

added national security powers that will be covered in detail are the creation of a new call records program, additional time to track suspected foreign terrorists upon entry into the United States, and increasing the prison sentences for terrorist supporters. Even some of the issues caused by the USA PATRIOT Act that the USA FREEDOM Act doesn't cover were resolved recently such as the expiration ("sunset") of Section 215 of the USA PATRIOT Act on May 31, 2015.

Although the USA FREEDOM Act sufficiently deals with the problems it addresses, it fails to account for other civil liberty issues caused by the NSA's surveillance system such as allowing individuals to challenge NSA orders:

> Other issues that the FREEDOM Act does not address include creating a cause of action for individuals and entities actually harmed by NSA surveillance and the appearance of NSA meddling in NIST encryption creation and gaining unauthorized access to overseas servers. The first issue will likely not be resolved for a variety of reasons, including that this would potentially make the government liable for an untold number of alleged Fourth Amendment infringements, and the real world eventuality that such liability would create an undue burden on the courts from the thousands of individual claims or class action claims that could seek to draw millions of citizens into the class that would immediately commence. None of the proposed legislation addresses the issue of NSA/NIST collaboration in creating backdoors to encryption systems. Additional Congressional oversight could address the issue, but to address it at the outset and staunch the financial harm befalling the United States tech industry, the most readily available way to address the issue, would be the budgetary mechanism of defunding the SIGINT Enabling Project. This would limit the NSA's ability to strong-arm NIST and major telecoms and reinstill public trust in the tech industry (Ombres, 2015, p. 53)[5].

The above quote makes it clear why many parts of the USA PATRIOT Act are not addressed in the USA FREEDOM Act; the main reasons for not addressing certain problems are

[5] Ombres, D. (2015). NSA Domestic Surveillance from the Patriot Act to the Freedom Act: The Underlying History, Constitutional Basis, and the Efforts at Reform. *Seton Hall Legis. J., 39*, 27.

that in addressing the issues the Federal Government could be opening itself up to many civil rights law suits, addressing the issues would cause federal courts to be unduly burdened with thousands of individual claims and class action suits involving millions of people, and addressing the issues would require an admittance of wrongdoing from the federal administration that it would not be willing to acknowledge to the public. The admittance of wrongdoing could potentially cost congressmen and congresswomen their seats in their respective houses as well as foster resentment from the public, neither of which are desired consequences for the federal administration in power.

Specific sections of Titles I through VII of the USA FREEDOM Act will be discussed at length in the remainder of this thesis to show specifically how the act protects civil liberties and security powers without causing any potentially significant damaging consequences. Specific excerpts from the sections, focusing only on the most relevant language, will be used to show how adjustments were made to security laws to provide for greater privacy protection.

Sec. 101. Additional requirements for call detail records.

Section 101 deals directly with the roving surveillance issues created by Section 215 of the USA PATRIOT Act. The roving surveillance powers granted to national security agencies allowed for the formation of bulk call records requests. National security agencies would request thousands of call records from telephone companies that they thought could possibly lead to evidence of future terrorist activities. The National Security Agency program specifically designed for phone records compartmentalization gathered up bulk telephone records through telephone metadata and conducted searches on the data based on telephone numbers. Telephone

metadata that was allowed to be searched did not include the content of telephone conversations; however, other details such as the length of the call, the originating phone number and the number called were permitted. The problem with the bulk requests were that they allowed national security agencies to spy on innocent United States citizens' activities without any probable cause or warrants. The bulk spying was completely inconsistent with traditional democratic values by creating a sense of insecurity and paranoia among citizens. The sense of being presumed guilty until proven innocent if falsely suspected of committing a terrorist act was frightening and the possibility of being wiretapped without any knowledge of the fact was reprehensible. Citizens couldn't feel free to express their thoughts, especially with regards to the federal government, when they thought that they could be spied on by national security agencies at any time. Section 101 addresses the intrusive powers and provides for stricter regulations on the use of the telephone records requests:

> (i)there are reasonable grounds to believe that the call detail records sought to be produced based on the specific selection term required under subparagraph (A)are relevant to such investigation; and (ii) there is a reasonable, articulable suspicion that such specific selection term is associated with a foreign power engaged in international terrorism or activities in preparation therefor, or an agent of a foreign power engaged in international terrorism or activities in preparation therefor; and (i) authorize the production on a daily basis of call detail records for a period not to exceed 180 days;(ii) provide that an order for such production may be extended upon application under subsection (b) and the judicial finding under paragraph (1) of this subsection; (iii) provide that the Government may require the prompt production of a first set of call detail records using the specific selection term that satisfies the standard required under subsection (b)(2)(C)(ii); (iv) provide that the Government may require the prompt production of a second set of call detail records using session-identifying information or a telephone calling card number identified by the specific selection term used to produce call detail records under clause… (v) provide that, when produced, such records be in a form that will be useful to the Government; (vi) direct each person the Government directs to produce call detail records under the order to furnish the Government forth with all information, facilities, or technical assistance necessary to accomplish the production in such a manner as will protect the secrecy of the production and produce a minimum of

> interference with the services that such person is providing to each subject of the production; and (vii) direct the Government to (I) adopt minimization procedures that require the prompt destruction of all call detail records produced under the order that the Government determines are not foreign intelligence information; and (II) destroy all call detail records produced under the order as prescribed by such procedures (USA FREEDOM Act, Pub. L. 114-23, 2015, Sec. 101).

The specific quoted sections above from the USA FREEDOM Act mainly do two things to guarantee the protection of civil liberties: (1) prohibit bulk collecting of records and (2) prevent government abuses of terrorist prevention powers. The clauses help prohibit bulk collection of records by forcing national security agents to have a reasonable suspicion of terrorist activity before requesting call records. They help prevent government overreach and abuses by prohibiting large-scale, undiscerning collection, such as all records from a large geographic area like a city. The clauses specifically force governments to focus on narrower targets of call records because of the requirement of a reasonable suspicion. The proponents for the USA PATRIOT Act defend the unconstitutional powers by claiming that the bulk telephone records programs were necessary to prevent terrorist activities and that the USA FREEDOM Act's section I is detrimental to national security; however, research studies show that the claims are completely false. Recent research studies on the National Security Agency have been conclusive and consistent in their findings that the bulk telephone records programs were not necessary or even helpful in fighting terrorist threats as can be seen by the following studies' claims: "Surveillance of American phone metadata has had no discernible impact on preventing acts of terrorism and only the most marginal of impacts on preventing terrorist-related activity, such as fundraising for a terrorist group" (Bergen, 2006, p.6)[6]. The federal government's

[6] Bergen, P., Sterman, D., Schneider, E., & Cahall, B. (2014). Do NSA's Bulk Surveillance

insistence on the need to have these secretive surveillance powers to combat terrorist activities is analogous to the argument to have stricter gun control laws to prevent lone wolf attacks by insane American citizens. Although both measures sound appealing and reasonable, they in no substantial way would deter the criminal activities from occurring because neither proposition addresses the true causes of the horrible activities, those causes largely dealing with mental illnesses.

Sec. 103. Prohibition on bulk collection of tangible things.

Section 103 is a continuation of Section 101's dismantling of the unconstitutional powers granted to the National Security Agency under the USA PATRIOT Act. Section 103 requires national security agents to go through a more laborious process in identifying necessary call records to ensure that innocent citizens will not be monitored for criminal activity. Section 103 requires specific selection terms for requesting information:

> (A) a specific selection term to be used as the basis for the production of the tangible things sought; (b) ORDER.—Section 501(c) (50 U.S.C. 1861(c)) is amended (1) in paragraph (2)(A), by striking the semicolon and inserting, 'including each specific selection term to be used as the basis for the production;'; and(2) by adding at the end the following new paragraph: '(3) No order issued under this subsection may authorize the collection of tangible things without the use of a specific selection term that meets the requirements of subsection (b)(2)' (USA FREEDOM Act, Pub. L. 114-23, 2015, Sec. 103).

USA PATRIOT Act supporters claim that the language inherent in these provisions is unnecessarily restrictive on national security agencies and that the swiftness of bulk records request programs was the key to their effectiveness. These defensive claims are completely

---

Programs Stop Terrorists? *New American Foundation*, 13.

unwarranted as well. Research studies and court cases have shown that the ability of national security agents to request and receive massive amounts of telephone metadata very quickly had absolutely no effect on terrorism prevention. Federal Courts have recognized the illegitimacy of arguments made in favor of the NSA's limitless surveillance program:

> Similarly, U.S. District Judge Richard Leon, who presided over a Federal Court case challenging the constitutionality of the bulk collection program, and who read the government's affidavits regarding the necessity of the program for national security, ruled in favor of an injunction against the NSA programs on December 16, 2013. He noted that the plaintiffs have a 'substantial likelihood' of showing their privacy interests outweigh the Government's interest in the NSA's bulk collection of American telephone metadata, and therefore the NSA's New America Foundation Page 7 bulk collection program constitutes an unreasonable search under the Fourth Amendment. He said in his opinion that given the 'utter lack of evidence that a terrorist attack has ever been prevented because searching the NSA database was faster than other investigative tactics,' he had 'serious doubts about the efficacy of the metadata collection program as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism (Bergen, 2006, Sec. 103).

Judge Leon made a set of very critical statements in his court ruling to show his disapproval of the NSA's surveillance programs:

> I cannot imagine a more 'indiscriminate' and 'arbitrary invasion' than this systematic and high-tech collection and retention of personal data on virtually every citizen [...] the almost-Orwellian technology [...] Records that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic – a vibrant constantly updating picture of a person's life. [...] No court has ever recognized a special need sufficient to justify continuous, daily searches of virtually every American citizen without any particularized suspicion. The Government urges me to be the first non-FISC judge to sanction such a dragnet. [...] The Government does not cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack [...] Because of the utter lack of evidence that a terrorist act has ever been prevented because searching the NSA database was faster than other investigative tactics – I have serious doubts about the efficacy of the metadata collection program [...] I have little doubt that the author of our Constitution, James Madison [...] would be aghast (*Klayman v. Obama*, 957 F. Supp. 2d 1, 59 Comm. Reg. (P & F) 825 (2013)).

Sec. 108. Inspector General Reports on Business Records Orders

Section 108 is the first section in the USA FREEDOM Act that deals with increased transparency requirements for national security agencies. After former Central Intelligence Agency contractor Edward Snowden leaked information in 2013 pertaining to national security abuses of power under the USA PATRIOT Act, transparency became a vital issue for the United States Congress to address in the USA FREEDOM Act revisions. Section 108 shows that the USA FREEDOM Act is an attempt by the Legislative Branch to gain more oversight over the Executive Branch's security measures; the section along with the further elaboration of the transparency concept in Title VI of the USA FREEDOM Act prove that the constitutional theory of checks and balances between branches of government is necessary to prevent further government abuses of power. Section 108 takes the first step in addressing transparency problems by forcing Inspector General Reports to the United States Congress to include many items of information that were formerly considered classified such as how terrorist activity information was obtained and from what sources. Section 108 provides:

> ..the importance of the information acquired under title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) to the activities of the intelligence community; (B) the manner in which that information was collected, retained, analyzed, and disseminated by the intelligence community; (C) the minimization procedures used by elements of the intelligence community under such title and whether the minimization procedures adequately protect the constitutional rights of United States persons; and (D) any minimization procedures proposed by an element of the intelligence community under such title that were modified or denied by the court established under section 103(a) of such Act (50 U.S.C. 1803(a)) (USA FREEDOM Act, Pub. L. 114-23, 2015, Sec. 108).

Sec. 202. Privacy procedures.

Section 202 is a broad privacy measure that encompasses the reasoning behind Title II of the USA FREEDOM ACT. One of the issues brought about by the USA PATRIOT ACT was the inclusion of internet communications and computer software programming companies under the Pen Register Act. This overwhelming inclusion allowed for the national security agencies to compel service providers such as Verizon, AT&T, Yahoo, Facebook, and Google to give them any records that they sought for potential terrorist information. The broad inclusion also allowed for the national security agencies to legally conduct internet surveillance of any areas that they deemed to be areas where terrorists could be in the United States. Section 202 helps to counter the broadness and secret nature of the pen register provisions by making the bulk requests by the national security agencies illegal. Section 202 gives more freedom and privacy to national communications corporations and innocent individuals by keeping their information safe from government retrieval. After the implementation of the USA FREEDOM ACT, the only way that national security agencies can demand internet communications from individuals through national communications corporations is if they have legitimate probable cause in seeking potential terrorist threats. The new privacy and protective measures established through Section 202 are in the following excerpt from the section:

> The Attorney General shall ensure that appropriate policies and procedures are in place to safeguard non-publicly available information concerning United States persons that is collected through the use of a pen register or trap and trace device installed under this section. Such policies and procedures shall, to the maximum extent practicable and consistent with the need to protect national security, include privacy protections that apply to the collection, retention, and use of information concerning United States persons. (2) RULE OF CONSTRUCTION. Nothing in this subsection limits the authority of the court established under section 103(a) or of the Attorney General to impose additional privacy or minimization procedures with regard to the installation or use of a pen register or trap and trace device. (b) EMERGENCY AUTHORITY.—Section 403 (50 U.S.C. 1843) is amended by adding at the end the following new subsection: ‘(d)

PRIVACY PROCEDURES.—Information collected through the use of a pen register or trap and trace device installed under this section shall be subject to the policies and procedures required under section 402(h) (USA FREEDOM Act, Pub. L. 114-23, 2015, Sec. 202).

Sec. 301. Limits on use of unlawfully obtained information

Section 301 protects civil liberties of national corporations and individuals to an even greater extent through addressing other problems that were brought about by the USA PATRIOT Act. One of the biggest issues with the USA PATRIOT Act was the secrecy through which it allowed the national security agencies to conduct their operations and the abilities they were granted in demanding cooperation from companies and citizens. The national security agencies were allowed to issue letter gag orders to any companies for information that they were demanding and they didn't allow for companies to challenge the intrusive information-gathering methods. Because of the secrecy requirements, there was no way for an individual or corporation to keep their records away from the government even if those records had absolutely nothing to do with terrorist activities. The intrusive national security measures allowed for the federal government to view private documents that would never have been allowed to be seen before the implementation of the USA PATRIOT Act. Section 301 resolves all of these issues in a very simple manner by allowing national corporations and individuals the right to challenge letter gag orders and information demands from national security agencies in court. The section specifically defines a procedure for the challenge of such orders and requires intermittent reviews of the orders and demands to determine whether or not they are even relevant to any ongoing terrorist investigations. The USA PATRIOT Act conditions were heavily abused and

Section 301 eliminates all of the channels that were used to conduct the civil liberty abuses as can be seen by the following excerpt from the section:

> (i)IN GENERAL.—Except as provided in clause (ii), if the Court orders a correction of a deficiency in a certification or procedures under subparagraph (B), no information obtained or evidence derived pursuant to the part of the certification or procedures that has been identified by the Court as deficient concerning any United States person shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired pursuant to such part of such certification or procedures shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of the United States person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person. (ii) EXCEPTION.—If the Government corrects any deficiency identified by the order of the Court under subparagraph (B), the Court may permit the use or disclosure of information obtained before the date of the correction under such minimization procedures as the Court may approve for purposes of this clause (USA FREEDOM Act, Pub. L. 114-23, 2015, Sec. 301).

Sec. 401 Appointment of Amicus Curiae

Section 401 and all of Title IV of the USA FREEDOM Act were designed to counter the problems of no transparency and no information sharing with the American public. Constituents and the United States Congress were fed up with the secrecy in the national security agencies actions so they specifically provided for mandatory ways of making investigations public. Section 401 makes two drastic changes to the United States Foreign Intelligence Surveillance Court; the court that was created by the Foreign Intelligence Surveillance Act of 1978, primarily to conduct proceedings that fell under the scope of terrorist investigation substantive procedures. The first change that Section 401 makes is that it creates a board of amicus curiae for the United States Foreign Intelligence Surveillance Court to help ensure the protection of private documents

and civil liberties for national companies and individuals that are being demanded to produce information. The amicus curiae, or “friends of the court”, are designated as communications technology experts, constitutional lawyers, and national security lawyers that can best provide advice and suggestions to courts on how they should rule on information gathering methods. Anytime the court faces new information gathering methods they are better equipped to make accurate evaluations and determinations of what the correct interpretations of the methods should be. The second change that Section 401, in attempting to improve transparency within national security investigations, is that it forces all decisions of the United States Foreign Intelligence Surveillance Court to be declassified and public. This declassification forces the courts to make constitutional interpretations and utilizations of the law or else they would be challenged in court by public civil liberties groups and the rulings would never hold up if they were incorrect. These publicizing of the court decisions makes the addition of the amicus curiae even more important because the experts are necessary to make adequate decisions that later are not likely to be successfully challenged in court. The benefits of such a section are clearly seen through the following excerpt from Section 401:

> RECEIPT OF INFORMATION.—Nothing in this subsection shall limit the ability of a court established under subsection (a) or (b) to request or receive information or materials from, or otherwise communicate with, the Government or amicus curiae appointed under paragraph (2) on an ex parte basis, nor limit any special or heightened obligation in any ex parte communication or proceeding.(j) REVIEW OF FISA COURT DECISIONS.—Following issuance of an order under this Act, a court established under subsection (a) shall certify for review to the court established under subsection (b) any question of law that may affect resolution of the matter in controversy that the court determines warrants such review because of a need for uniformity or because consideration by the court established under subsection (b) would serve the interests of justice. Upon certification of a question of law under this subsection, the court established under subsection (b) may give binding instructions or require the entire record to be sent up for decision of the entire matter in controversy (USA FREEDOM Act, Pub. L. 114-23, 2015, Sec. 401).

Sec. 501 Prohibition on bulk collection

Section 501 helps to ensure a national security change that was greatly needed after many national security abuses under the USA PATRIOT Act. The main change that the section helps to bring about is the end of bulk collection of telephone metadata and internet communications from companies on individual citizens. The section forces national security information demands to have probable cause and to be specific in their attempts. For example, national security agencies will no longer be allowed to request information from entire area codes in the hopes of finding only a few people that could potentially be linked to terrorist activities. The redefining of key terms in the information gathering methods to ensure more defined searches can be seen by the following excerpt from Section 501:

> (c) DISCLOSURES TO FBI OF CERTAIN CONSUMER RECORDS FOR COUNTERINTELLIGENCE PURPOSES. Section 626 of the Fair Credit Reporting Act (15 U.S.C.1681u) is amended—(1) in subsection (a), by striking 'that information,' and inserting 'that information that includes a term that specifically identifies a consumer or account to be used as the basis for the production of that information,'; (2) in subsection (b), by striking 'written request,' and inserting 'written request that includes a term that specifically identifies a consumer or account to be used as the basis for the production of that information,'; and (3) in subsection (c), by inserting, 'which shall include a term that specifically identifies a consumer or account to be used as the basis for the production of the information,' after 'issue an order ex parte'. (d) DISCLOSURES TO GOVERNMENTAL AGENCIES FOR COUNTERTERRORISM PURPOSES OF CONSUMER REPORTS.—Section 627(a) of the Fair Credit Reporting Act (15 U.S.C. 1681v (a)) is amended by striking 'analysis 'and inserting 'analysis and that includes a term that specifically identifies a consumer or account to be used as the basis for the production of such information (USA FREEDOM Act, Pub. L. 114-23, 2015, p. Sec. 501).

Section 501 makes adjustments to how national security agencies can meet the requirements of a specific selection criterion by ruling out many of the loopholes that were inherent in the USA PATRIOT Act's rendition of the selection criteria. The loopholes in bulk

collection gathering were in their vagueness, basically allowing for all information to be requested because of no limits on what the term specific selection meant. The provision forces national security agencies to conduct more interrogations with their own equipment and services in order to narrow down their targets before requesting telecommunications and internet communications information from national service providers and corporations.

Sec. 502 Limitations on disclosure of national security measures

Section 502 gives more options to national service providers and telecommunications corporations in dealing with national security demands for information. The authoritarian behavior of national security agencies in controlling national corporations was domineering under the USA PATRIOT Act and thus needed to be addressed by the USA FREEDOM Act. Section 502 does an excellent job in creating barriers between the national security agencies' authority to demand information and the national corporations' abilities to respond or request exclusion from such intrusive methods. Section 502 allows for national telecommunications corporations and national service providers to publically disclose certain information that was requested during investigations if that information should legally be disclosed to clients that are not in any way connected to the terrorist investigations. Section 502 also allows companies to respond in various ways to information demands that are more reasonable to their specific companies. For example national telecommunications companies may now request documents showing a need for specific information from national security agents and may request additional time in gathering information that would have been mandatory by a specific time under the USA PATRIOT Act. The leniency granted to national service providers in dealing with complicated

metadata and telecommunications requests can be seen in the following excerpt from Section 205:

> (A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (c) is provided, no governmental or private entity that receives a request under subsection (a), or officer, employee, or agent thereof, shall disclose to any person that an authorized investigative agency described in subsection (a) has sought or obtained access to information under subsection (a). (B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the head of an authorized investigative agency described in subsection (a), or a designee, certifies that the absence of a prohibition of disclosure under this subsection may result in '(i) a danger to the national security of the United States;'(ii) interference with a criminal, counterterrorism, or counterintelligence investigation; '(iii) interference with diplomatic relations; or '(iv) danger to the life or physical safety of any person'. (2) EXCEPTION. (A) IN GENERAL.—A governmental or private entity that receives a request under subsection (a), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to'(i) those persons to whom disclosure is necessary in order to comply with the request';'(ii) an attorney in order to obtain legal advice or assistance regarding the request'; or '(iii) other persons as permitted by the head of the authorized investigative agency described in subsection (a) or a designee (USA FREEDOM Act, Pub. L. 114-23, 2015, Sec. 502).

Sec. 602 Annual Reports by the Government

Section 602 deals with mandatory federal government reporting of national security investigations and even further limits the definition of specific selection criteria for information gathering requests. The section expands the amount of national security reporting to the public, as well as the in-depth approach to such information to explain how the national security authority is used and is impacting American citizens. Section 602 is primarily focusing on making the federal government more transparent so that individuals feel safer and more comfortable in knowing that they are not being spied on if they are not connected to a terrorist investigation. Additional limits of the specific selection criteria under the section primarily deal with how long the national security agencies are allowed to keep the gathered information, how

many orders may be processed within specific time limits, and the specific details of their terrorist targets being written out in their requests. The specific details of their information gathering requests and the time restrictions on information storing are required by the following excerpt from Section 602:

> MANDATORY REPORTING BY DIRECTOR OF NATIONAL INTELLIGENCE.—Except as provided in subsection (d), the Director of National Intelligence shall annually make publicly available on an Internet Web site a report that identifies, for the preceding 12-month period- (1) the total number of orders issued pursuant to titles I and III and sections 703 and 704 and a good faith estimate of the number of targets of such orders; (2) the total number of orders issued pursuant to section 702 and a good faith estimate of (A) the number of search terms concerning a known United States person used to retrieve the unminimized contents of electronic communications or wire communications obtained through acquisitions authorized under such section, excluding the number of search terms used to prevent the return of information concerning a United States person; and (B) the number of queries concerning unknown United States person of unminimized noncontents information relating to electronic communications or wire communications obtained through acquisitions authorized under such section, excluding the number of queries containing information used to prevent the return of information concerning a United States person; (3) the total number of orders issued pursuant to title IV and a good faith estimate of—(A) the number of targets of such orders; And (B) the number of unique identifiers used to communicate information collected pursuant to such orders; (4) the total number of orders issued pursuant to applications made under section 501(b)(2)(B) and a good faith estimate of—(A) the number of targets of such orders; and (B) the number of unique identifiers used 7 to communicate information collected pursuant to such orders; (5) the total number of orders issued pursuant to applications made under section 501(b)(2)(C) and a good faith estimate of—(A) the number of targets of such orders; (B) the number of unique identifiers used to communicate information collected pursuant to such orders; and (C) the number of search terms that included information concerning a United States person that were used to query any database of call detail records obtained through the use of such orders; and (6) the total number of National Security Letters issued and the number of requests for information contained within such National Security Letters (USA FREEDOM Act, Pub. L. 114-23, 2015, Sec. 602).

Sec. 701 Emergencies involving non-United States persons

A recurring theme of strengthening national security starts with Section 701 and continues through Title VII and Title VIII of the USA FREEDOM Act. Titles VII and VIII are

primarily concerned with making sure the national security agencies still have enough power to be useful in containing new terrorist threats that took a stronghold in 2014 and the beginning of 2015. The emergence of the Islamic State and the lone wolf terrorist attacks on United States entities created a need for certain provisions of the USA PATRIOT Act to be maintained while adding new measures that could facilitate the discovery of terrorist threats and the prevention of future attacks. Title VII explicitly creates a new call detail records program that is more specific to ensure civil liberties without giving up powers necessary in the tracking of terrorist threats. Section 702 specifically closes a loophole in foreign intelligence security law that forced the foreign intelligence gathering agencies to stop tracking known terrorist threats immediately upon their arrival in the United States. Section 702 allows for an added power of tracking suspected foreign terrorist threats for up to 72 hours after their arrival in the United States. This addition will help greatly in narrowing the requests by national security agents to national service providers and national telecommunications corporations because national security agencies will have a much better idea of where the terrorists are located by tracking their movements within the country for 72 hours. The narrowed requests will also allow for less broad requests and less gathering of information from individuals not connected to terrorist threats. The new addition to national security law can be seen from the following excerpt from Section 702:

> (f)(1) Notwithstanding any other provision of this Act, the lawfully authorized targeting of a non-United States person previously believed to be located outside the United States for the acquisition of foreign intelligence in-formation may continue for a period not to exceed 72 hours from the time that the non-United States person is reasonably believed to be located inside the United States and the acquisition is subject to this title or to title III of this Act, provided that the head of an element of the intelligence community—(A) reasonably determines that a lapse in the targeting of such non-United States person poses a threat of death or serious bodily harm to any person; (B) promptly notifies the Attorney General of a determination under subparagraph (A); and(C) requests, as soon as

practicable, the employment of emergency electronic surveillance under subsection (e) or the employment of an emergency physical search pursuant to section 304(e), as warranted (USA FREEDOM Act, 2015, Pub. L. 114-23, Sec. 701).

Sec. 704. Increase in penalties for material support of foreign terrorist organizations.

Section 704 is an attempt by the United States Congress to deter future lone wolf attacks in the United States by imposing harsher penalties on people who consider helping terrorists in their attempts. Section 704 increases the statutory minimum prison sentence to 20 years for providing measurable support or resources to a potential domestic terrorist. Unfortunately, this section is very unlikely to have any substantial effects on reducing lone wolf attacks because it only raises the minimum prison sentence by five years and does nothing to address the specific reasons why people have been known to help domestic terrorists. The slight increase in penalty is in the following excerpt from section 704, "Section 2339B (a)(1) of title 18, United States Code, is amended by striking '15 years' and inserting '20 years'"(USA FREEDOM Act, Pub. L. 114-23, 2015, Sec. 704).

The vast majority of people that have been discovered to have helped domestic terrorists to commit their crimes were in no way in fear of the criminal penalties that could have resulted. They were people who were brainwashed by religious fanaticism to have no fear of death or punishment from United States authorities. The Boston Marathon bombings on April 15, 2013 are a prime example. The culprits, the Tsarnaev brothers, were both Muslim radicals that had written that their purpose for the bombings was to protest the United States' involvement in Middle Eastern affairs. The college friends that helped the Tsarnaev brothers cover up evidence of their involvement in the Boston Marathon bombing had also been brainwashed by Muslim

radical ideologies (*United States v. Dzhokar Tsarnaev*, 13-cr-10200 (2015))[7]. A slight increase in punishment for accessories to domestic terrorists will more than likely have no measurable effect on the mind sets of religiously fanaticized people.

Chapter 4: Constitutional Analysis

[7] This Decision does not yet have a Citation reference. No citing cases found.

In Chapter 2, the USA PATRIOT Act was shown to give too much power to national security agencies to the extent that civil liberties were threatened by powers granting metadata search access that was highly intrusive into the affairs of American corporations and individuals. In Chapter 3, we discussed how the USA FREEDOM Act arguably made life better for American citizens by protecting civil liberties without infringing on necessary national security powers. The USA FREEDOM Act is an improvement compared to the USA PATRIOT Act; however, whether or not these improvements are constitutional remains to be seen. While the USA FREEDOM Act is a step in the right direction for guarding civil liberties and curtailing national security powers, there are many areas in which the USA FREEDOM Act does not go far enough in repealing the substantial surveillance powers granted by the USA PATRIOT Act. In this constitutional analysis, the USA PATRIOT Act and the USA FREEDOM Act sections will be further discussed to show which sections are unconstitutional and allow unconstitutional surveillance activities by being in violation of the First Amendment, Fourth Amendment, Fifth Amendment, and Sixth Amendment.

Amendment I

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances (U.S. Const. Amend. I).

The USA PATRIOT Act's Section 505 was arguably in violation of the First Amendment by the restrictions on free speech created by the implemented powers and the various investigative measures for gathering intelligence information. National Security Letters are one

of the preeminent ways in which national security agencies gathered intelligence information from various corporations and individuals and the reasoning behind why the letters are dangerous and unconstitutional can be understood through the following excerpt:

> The nondisclosure requirements contained within the NSL provisions of the ECPA, RFPA, and FCRA clearly impose restrictions on the free speech of NSL recipients. For example, Section 2709 of the ECPA provides that 'No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.' The RFPA contains a similar provision, whereas the FCRA allows disclosure to 'those officers, employees or agents of a consumer reporting agency necessary to fulfill the requirement to disclose information to the [FBI].' The fact that the NSL statutes restrict speech does not, in and of itself, establish that the nondisclosure provisions violate the First Amendment. In determining whether a particular statutory scheme violates the First Amendment, the reviewing court must first choose the appropriate level of judicial review to be applied. Under the strict scrutiny standard, a speech restriction will be upheld only if 'narrowly tailed to promote a compelling Government interest' and will be deemed invalid if 'less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve.' Critics of Section 505 contend that the appropriate standard of review for the nondisclosure provisions is strict scrutiny. They argue that the provisions fail to pass constitutional muster under this analysis because they 'impose secrecy with respect to every investigation without requiring the FBI to make any particularized showing that such secrecy is necessary.' Furthermore, the nondisclosure provisions do not terminate at any point in time. As a result of this permanent secrecy 'recipients and others affected by the … NSLs are unable to bring abuses … to the attention of Congress or the public.' In other words, the level of secrecy mandated by Section 505 was not the least restrictive option for safeguarding the government's interest in preserving national security. Critics advocated for amendments to the nondisclosure provisions that would provide for case-by-case review of the necessity of nondisclosure, as well as for narrowly tailored orders in those cases where nondisclosure is warranted (Gorham-Oscilowski, 2008, p. 630-631)[8].

While the National Security Letters have been shown to be too restrictive of citizen's civil liberties, there are many more ways in which the USA PATRIOT Act has violated the First

[8] Gorham-Oscilowski, U., & Jaeger, P. T. (2008). National Security Letters, the USA PATRIOT Act, and the Constitution: The tensions between national security and civil rights. *Government Information Quarterly, 25(4),* 625-644.

Amendment. All of the sections of the USA PATRIOT Act that were summarized in Chapter 1 constitute abuses of civil liberties by the powers that they grant to national security agencies. Section 203(b) and (d), 206, 213, and 215 are not in compliance with the First Amendment. Together, these four sections all provided for a system of national security for the federal government that violates civil liberties. The following excerpt explains how the sections were seen to be in violation of the First Amendment in court cases and how the sections were used in discriminatory and unjustifiable ways:

> Governmental surveillance also may infringe upon the First Amendment rights of Americans by chilling free expression, particularly in the context of political protest. The First Amendment provides that "Congress shall make no law.., abridging the freedom of speech. This explicit constitutional protection of expressive activity is upheld with particular vigor when individuals exercise this freedom as a means of political protest. While many forms of expressive activities are protected by the First Amendment, the courts have allowed little or no protection for those who seek to incite violence, or who use violence or otherwise illegal acts as a means of protest. As the Supreme Court declared in *NAACP v. Claiborne Hardware Co.,* 'violence has no sanctuary in the First Amendment, and the use of weapons, gunpowder, and gasoline may not constitutionally masquerade under the guise of advocacy.' Since violent or illegal acts are not protected under the right to free expression, the First Amendment will not act as a barrier against government surveillance of such activities. Yet, where individuals exercise free expression in a manner protected by the First Amendment, government surveillance may not be targeted specifically at such behavior. Interests protected by the First and Fourth Amendments converge in this context, as intrusive surveillance activities discourage the exercise of protected expression. In *United States v. United States District Court,* the Court stated that 'history abundantly documents the tendency of Government-however benevolent and benign its motives-to view with suspicion those who most fervently dispute its policies' (Rackow, 2002, p.1656-1657)[9].

[9] Rackow, S.H. (2002). How the U.S.A. Patriot Act will permit governmental infringement upon the privacy of Americans in the name of "intelligence" investigations. *University of Pennsylvania Law Review*, 150, 1651-1695, p. 1673

The USA FREEDOM Act has a few provisions which may probably conflict with the civil liberties granted by the First Amendment; specifically with regard to the freedom of speech, freedom to peaceably assemble, and the freedom to petition the federal government for a redress of grievances. While no section of the USA FREEDOM Act is directly restricting any of these liberties, some sections are definitely restricting these rights indirectly by putting fear in the minds of American citizens. If American citizens feel that they could have their conversations via telephone and internet recorded by national security agencies, then they will not be able to freely express their thoughts. The USA FREEDOM Act does not adequately restrict national security agencies' abilities to intrude into the lives of innocent Americans. The USA FREEDOM ACT still allows for the operation of the secret National Security Agency programs that are authorized under section 702 of the FISA Amendments Act. The dangerous authority of the agencies was exposed in 2013 by whistleblower Edward Snowden and is described in the following, "The leaked reports, published in May 2013, revealed a number Internet Surveillance programs used by the NSA; these included the Tempora, PRISM, and XKeyscore programs, as well as information involving metadata from telephone Interceptions in the US and Europe" (Verble, 2014, p.5)[10].

The authorized National Security Agency programs such as PRISM and XKeyscore are able to view all public and private information on the internet without citizens ever knowing that they were spied upon. Without addressing the abuses of these national security programs, the First Amendment rights of American citizens will continue to be in jeopardy because of citizens

[10] Verble, J. (2014). The NSA and Edward Snowden. *SIGCAS Comput. Soc. ACM SIGCAS Computers and Society*, 1-20.

having a constant fear of having personal communications in private online forums being used against them by government officials. Sections 101, 103, 301, 501, and 502 of the USA FREEDOM Act limit the authority of the national security agencies to conduct broad surveillance measures; however, the sections do not exclude any possibilities of government overreach in metadata collection of individuals because of the continued secrecy and questionable legality of national security data collection programs. The sections also fail to address the concern of what will happen to all of the information that has already been collected under the USA PATRIOT Act. Since no legislation has been implemented to negotiate the disposal of the unconstitutionally gathered information by the national security agencies, the information will remain legally under the authority of the national security agencies and thus innocent Americans may still live in fear of having personal information stored on the hard drives of national security computer systems.

Amendment IV

> The right of the people to be secure in their persons, houses, papers, and effects,[a] against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized (U.S. Const. Amend. IV).

THE USA PATRIOT Act's entire framework on domestic surveillance and national security fostered one of the most constitutionally egregious eras in American history since the early 1800's when the Alien and Sedition Acts were in full effect. The injustices caused by the USA PATRIOT Act were numerous and eventually Federal Courts were able to put a stop to the

abuses by the Executive Branch. The main controversies created by the USA PATRIOT Act dealt with the acts complete disregard for the Fourth Amendment as can be seen in the following passage:

> The Supreme Court, in *United States v. United States District Court* ('Keith'), has also acknowledged that national security investigations may call for a different level of Fourth Amendment protection. In that case, the Court opined that 'different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of government for intelligence information and the protected rights of our citizens.' A lower level of protection, however, does not change the fact that there must be an opportunity for judicial review. In the context of administrative subpoenas, for example, constitutionality 'is predicated on the availability of a neutral tribunal to determine, after a subpoena is issued, whether the subpoena actually complies with the Fourth Amendment's demand.' After the USA PATRIOT Act was passed, Section 505 came under fire as critics argued that it violated the Fourth Amendment in two ways: 1) it failed to provide an opportunity for meaningful judicial review (either before or after issuance of an NSL); and 2) the showing the government must make in order to obtain an NSL (i.e., certification of relevance to a terrorism investigation) is inadequate. Specifically, with regard to the latter argument, concern has been expressed over the fact that 'no individualized suspicion of the person whose records are being sought is required' and that 'the FBI does not have to show a judge a compelling need for the records'…In Doe v. Ashcroft, an Internet Service Provider (ISP) sued the government after receiving an NSL, asserting that Section 2709 of the ECPA violated its First and Fourth Amendment rights. Specifically, the plaintiff argued that Section 2709 'gives the FBI extraordinary and unchecked power to obtain private information without any form of judicial process' and that the nondisclosure provision 'burdens speech categorically and perpetually, without any case-by-case judicial consideration of whether the speech burden is justified.' The court agreed with the plaintiff that Section 2709 violated the First and Fourth Amendments both facially and as applied to the facts of this case. First and foremost, notwithstanding its characterization of NSLs as a 'unique form of administrative subpoena,' the court found that both amendments were violated by the absence of meaningful judicial review. In doing so, the court rejected the government's contention that judicial review was 'implied' by the law (Gorham-Oscilowski, 2008, 632-634)[11].

[11] Gorham-Oscilowski, U., & Jaeger, P. T. (2008). National Security Letters, the USA PATRIOT Act, and the Constitution: The tensions between national security and civil rights. *Government Information Quarterly, 25(4),* 625-644.

Amendment IV of the United States Constitution was by the far the most infringed upon amendment by the USA PATRIOT Act and is still the most interfered with by the USA FREEDOM Act. The USA FREEDOM Act made great strides in making national security laws much more in line with the intent of the Fourth Amendment by demanding much higher standards for searches of individuals through metadata and telecommunications through sections 101, 103, and 105. Since corporations are also considered as people by the federal government and the United States Supreme Court, the USA FREEDOM Act does an excellent job in fighting for corporations' freedom from unreasonable searches and seizures of information in sections 202, 501, and 502. These sections allow for corporations to be given more options in responding to national security agencies' information demands, allow corporations to have more control over their clients' metadata, and allow for corporations to have immunity from prosecution for providing information on suspected terrorists.

The reasons why the USA FREEDOM Act is still in violation of the Fourth Amendment are few though significant; the sections still allow for unreasonable searches and seizures of individuals on a smaller scale through the granting of warrants with unsubstantiated claims of probable cause by national security officials in very secretive courts. These secretive courts such as the United States Foreign Intelligence Surveillance Court make it almost impossible for people to challenge illegal searches and seizures of their property if those searches and seizures were conducted under the warrants of those courts. There is no system of checks and balances on these terrorist combatting courts so their jurisdiction is unlimited and unresponsive to any challengers in the legal system. The following excerpt discusses the illegal surveillance network

of the National Security Agency and how the surveillance actions are affecting American citizens:

> The result of this global surveillance network is a massive amount of raw intelligence, including virtually every electronic conversation around the world. This information is generally sifted through by data mining techniques that register particular words, phrases, or voices. The NSA collects this information for analysis by tactical and strategic military leaders, policymakers, and other intelligence agencies. For much of its history, the immense capabilities and collection framework of the NSA were limited to targeting foreign powers and organizations. The Bush administration changed that scope by allowing the NSA to conduct warrantless electronic surveillance on persons in the United States. No longer would the NSA restrict its warrantless actions to foreign to foreign terminal communications, but it would now include information originating from or going to a domestic terminal. The NSA eavesdrops on an estimated 500 persons in the United States at any given time (Bloom, 2006, p.153-154)[12].

The cited abuses and unconstitutional powers of the National Security Agency under the President George W. Bush administration are not deterred enough by the USA FREEDOM Act to make a substantial difference in how domestic and foreign surveillance of records will be conducted in the future. The USA FREEDOM Act does make significant changes that will be able to be enforced thanks to transparency sections such as sections 401 and 602; but these are only a small step in the direction towards complete compliance with the Fourth Amendment.

Amendment V

> No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived

[12] Bloom, R. M., & Dunn, W. J. (2006). The Constitutional Infirmity of Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury to the Fourth Amendment. *William & Mary Bill of Rights Journal*, 15, 147-202.

> of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation (U.S. Const. Amend. V).

The USA PATRIOT Act's allowance for secrecy in all national security measures caused many abuses of the Fifth Amendment. The secrecy of the courts involved in the suspected terrorist trials allowed for trials that violated many substantive and procedural rules that are required in criminal cases. Some of the Fifth Amendment issues created by the text of the USA PATRIOT Act are described in the following passage:

> This Note argues that the USA PATRIOT Act's provisions for certification and mandatory detention contravene the Fifth Amendment's guarantee of due process of law. By denying noncitizens the opportunity for meaningful review of the certification decision, and by authorizing the detention of aliens on substantively inadequate grounds, the USA PATRIOT Act raises serious constitutional concerns under both the procedural and substantive prongs of the Due Process Clause…The Due Process Clause provides two independent tests for evaluating whether government action passes constitutional muster: Procedural due process considers whether government action depriving an individual of life, liberty, or property was implemented in a 'fair manner,' while substantive due process prevents government conduct that 'shocks the conscience' or intrudes on rights 'implicit in the concept of ordered liberty.' The certification and mandatory detention of suspected aliens can be challenged on both procedural and substantive due process grounds. The procedural due process claim, considered first in this Note, finds constitutional fault in the absence of fair procedures protecting against wrongful certification. The opportunity for a meaningful hearing is a critical component of procedural due process, yet the USA PATRIOT Act offers an alien no opportunity for a hearing before certification and only tenuous and uncertain opportunities for judicial review after certification. As argued below, whether or not this problem amounts to an actual constitutional violation will depend largely on how courts construe the scope of habeas corpus review of certification. Meanwhile, the substantive due process challenge stems from the excessive scope of the grounds for certification in section 412: The USA PATRIOT Act authorizes the certification of individuals who may neither be dangerous nor present a risk of flight, permitting detention for substantively inadequate grounds (Sinnar, 2003, 1421-1429)[13].

[13] Sinnar, S. (2003). Patriotic or unconstitutional? The mandatory detention of aliens under the USA PATRIOT Act. *Stanford Law Review*, 1419-1456.

The due process clause of the Fifth Amendment has been repeatedly violated throughout the USA PATRIOT Act era and will likely continue to be violated under the USA FREEDOM Act. There have been many secretive court cases over the last decade conducted by the Foreign Intelligence Surveillance Court that were clearly unconstitutional and solely justified in the name of national defense. The court conducted the trials ex parte, with only the judge and government officials present, allowing for some of the most biased and unfair trials in American history. These trials were used to detain alleged terrorists for indefinite amounts of time and with no knowledge of when they would be released. Many of these alleged terrorists were eventually exonerated and compensated for their unjustified time in prison. The following passage explains the risk of having such courts unchecked and authorized to deal with all detained terrorist suspects in an authoritarian way:

> From a constitutional perspective, the certification and mandatory detention of suspected immigrants in the USA PATRIOT Act should give pause. In particular, there is good reason to believe that the provisions do not comport with the procedural due process required by the Fifth Amendment. Without an opportunity to hear the charges against him and to contest them in a true adversarial proceeding, a wholly innocent person may well find himself deprived of liberty on unfounded allegations of terrorism. Accusations of terrorism do not justify procedural injustice. Furthermore, widespread reports of individuals wrongfully detained by the Justice Department since September 11th suggest the frequency of mistaken suspicion and government error in the terrorism probe. Truncated procedures only increase the risk of such deprivations (Sinnar, 2003, p.1455).

Sections 202, 401, and 602 of the USA FREEDOM Act help in addressing the illegal proceedings conducted by the Foreign Intelligence Surveillance Court by increasing transparency in the court decisions on suspect detentions through reporting to the Legislative Branch in annual hearings. Unfortunately, the mandatory reporting requirements are very vague and can easily be ignored by a narrow interpretation. Even if all of the annual reports are conducted as written in

the legislative sections, the fact that they are only annual reports leaves a significant amount of time when abuses can be conducted in secrecy. The mandatory annual reports only require basic details such as the number of court cases and the number of document requiring orders sent to corporations, with nothing stated regarding specific contextual details about the cases and court ordered documents. The USA FREEDOM Act does little to improve due process for American citizens that are detained for alleged terrorist activities.

Amendment VI

> In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defence (U.S. Const. Amend. VI).

The fact that all of the Foreign International Surveillance Court Trials are conducted ex parte, with only the judge and government officials present, makes it clear why the accused terrorist suspects are being denied their Sixth Amendment rights. While it is true that ex parte trials help to advance important actions in trials and thus make the verdicts on the accused much quicker, they also allow for actions to be conducted in privacy and without a public check on fairness and obeying rules. Ex-parte trials are dangerous in any type of criminal case because they keep the defense attorney unaware of important trial procedures that could be important to know when defending clients. In an adversarial system present in the United States trials, it is vital that defense attorneys are made aware of all private interactions between the federal or state prosecutor and the judge to facilitate an equal playing field. The federal prosecutors could

potentially be given an unfair advantage in Foreign International Surveillance Court Trials by being allowed to conduct private actions with the judges, thus developing relationships with the judges and the case material that the defense attorney would be unable to gain or understand.

The Sixth Amendment demands a speedy and public trial for the accused; however, the suspects for these alleged terrorist activities can sit in jails indefinitely for very long periods of time before being given a trial and once they are given trials, the trials are completely private. There are no jury decisions in the Foreign Intelligence Surveillance Court and there are no media personnel or public citizens to judge whether or not the correct substantive and procedural rules are being followed. The proceedings are non-adversarial, the defendants are not given attorneys and the judges make their decisions solely based on the surveillance information provided by national security agencies. It is clear that these trials are not presuming the defendants to be innocent until proven guilty as the courts offer no legitimate way for the defendants to challenge the accusations by the federal government. Sections 401 and 602 of the USA FREEDOM Act help to alleviate the Sixth Amendment issues that were rampant under the USA PATRIOT Act by increasing public awareness of the Foreign Intelligence Surveillance Court decisions. The sections specifically direct the Office of the Director of National Intelligence to declassify FISA Court opinions and to summarize opinions that cannot be released.

The sections also create a panel of special advocates with the purpose of supporting legal interpretations of national security laws and court procedures that advance individual privacy and civil liberties. These special advocates are required to serve defendants whenever an application of a ruling presents a novel or significant interpretation of the law, thus ensuring that the trials of the accused will not be completely unfair and biased against them. The difficulty that the USA

FREEDOM Act failed to address was the lack of oversight over the Foreign Intelligence Surveillance Court trials as can be seen by the following reference:

> In terms of its core function, the FISC is effectively a federal district court. The vast majority of its work involves a single judge's determinations of the legality of government requests to authorize surveillance or compel production. Although it is hard to be certain without more publicly available information, FISC judges likely treat their opinions as non-precedential, as is standard practice for federal district courts. The relatively few public FISC opinions do cite earlier FISC opinions and principles of law, but we have seen no clear evidence to suggest that the judges feel formally bound by those earlier opinions in any manner that would set them apart from other Article III district courts (Boeglin, 2015, p. 2192)[14].

The above excerpt makes it clear that the Foreign Intelligence Surveillance Court operates under an entirely secret set of rules that are completely nonconforming with legal precedent and the United States Constitution. The court must be abolished or severely modified in order to be in compliance with the Sixth Amendment. Innocent Americans accused of being potential terrorist threats can be adjudicated guilty under a system that is secretive and Orwellian until major reforms are made to the national security system.

Chapter 5: Conclusion

[14] Boeglin, J., & Taranto, J. (2015). Stare Decisis and Secret Law: On Precedent and Publication in the Foreign Intelligence Surveillance Court. *Yale Law Journal*, 124(6), 2189-2201.

The balance between privacy and security is still out of sync after the improvements made by the USA FREEDOM Act. The USA FREEDOM Act fails to address many problems that were caused by the USA PATRIOT Act and the FISA Amendments Act of 2008. Many unconstitutional intelligence gathering powers that were granted to the national security agencies by the USA PATRIOT Act and the FISA Amendments Act of 2008 remain in effect today. There must be a substantial decrease in these intelligence gathering powers for citizens to have their civil liberties protected from further obstruction. There are three ways in which the inversely correlated balance between security and privacy can be tipped more towards the protection of federal privacy rights and the decrease of national security powers. The first way is through the Supreme Court making a ruling in a specific case or cases that would deem USA FREEDOM Act provisions unconstitutional and thus require Congress to amend them to be more in favor of protecting civil liberties. The second way would be through the passage of many limited acts in Congress, which would be necessary if the houses of Congress contained majorities of members that were unwilling to make drastic changes to national security laws but would be willing to make minor changes over a long period of time. The third way would be through the initial passage of one all-encompassing act called the State Surveillance Repeal Act, though the proposed enactment would be unlikely due to Congressional differences of opinion on making drastic changes to the national security agenda.

The first way that the powers can be abolished is through a Supreme Court case or cases that would directly rule certain national security powers granted under the USA PATRIOT Act and the USA FREEDOM Act to be unconstitutional; however, that process would be very arduous and would allow national security agencies to continue to violate American citizens'

privacy rights for many years. There would also likely be a need for multiple Supreme Court cases because typical individual cases do not answer questions on the constitutionality of a multitude of complex issues. A great example of a Supreme Court case that directly limited national security powers was *United States v. Jones*, 132 S. Ct. 945, 565 U.S. ___ (2012). In *United States v. Jones*, the Supreme Court held that the installation of a GPS tracking device on defendant Jones' vehicle for twenty eight days, without a warrant, constituted an unlawful search under the Fourth Amendment because it violated his reasonable expectation of privacy. Applying this case to the national security powers allowed under the USA PATRIOT Act could make many of them unconstitutional. For example, the ability of national security agents to collect telephone records in bulk without specifically tailored warrants could be considered as the same type of search only through a different medium according to the concurring opinion of Justice Sotomayor. Justice Sotomayor reasoned that the Fourth Amendment applies to all violations of subjective expectations of privacy even if the violations do not require physical intrusion such as in metadata and telephone surveillance. A great example of this slow process of Supreme Court cases creating law through judgments in cases can be seen in the attempts at increasing sexual reproduction rights for women by ruling on the constitutionality of many state laws on issues such as the allowance of contraceptives for married and unmarried couples (*Griswold v. Connecticut*, 381 U.S. 479 (1965*), Eisenstadt v. Baird,* 405 U.S. 438 (1972), etc.) and abortion rights for women (*Roe v. Wade,* 410 U.S. 113 *(1973)* , *Planned Parenthood of Southeastern Pa. v. Casey,* 505 U.S. 833 *(1992),* etc.).

The second option to tip the balance between privacy and security in favor of increased protection of civil rights and a decrease in national security powers would be for Congress to

pass many more acts like the USA FREEDOM Act that would slowly repeal small parts of the USA PATRIOT Act until the entire act becomes repealed over many years. This process of passing many small acts by Congress would probably be the most effective and likely way to change the law; however, it would also take a very long time and would not bring about the required results in an efficient time frame. Support from legal academics and from the Supreme Court for this gradual process conducted by Congress can be seen by the following, "If technological infringement upon Fourth Amendment privacy is to be limited in any meaningful fashion, in a manner that concurrently protects American citizens without depriving them of their constitutional rights, Congress must hear the cry of the Court and take preemptive action. When it comes to technological innovation, Congress is best suited to balance the needs of national security with the American citizens' privacy rights" (Michaud, 2012, Harvard Law School National Security Journal)[15]. This process has been used by political parties holding the majority in Congress in the past to deal with many controversial issues such as bank and automotive industry bailout bills in order to achieve a desired result without causing too many gridlocks on other issues being debated. For example when House of Representatives Democrats were trying to pass President Obama's economic $819 billion stimulus package in 2009, they were unanimously opposed by House of Representative Republicans but were still able to pass it through the House of Representatives thanks to having a majority of seats. However, the only way to get the bill through the Senate was by getting the favor of three crucial Republican votes and they were able to get these votes from Rep. Susan Collins, Rep. Arlen Specter, and Rep.

[15] Michaud, Kate (2012). *United States v. Jones*: Why the Whole Court is calling for Congressional Action. *Harvard Law National Security Journal*.

Olympia Snowe by decreasing the total amount of money spent on various health and education programs and extending the total amount of money over more years, thus making it as if it would be conducted in many small parts instead of in one big package. Another possible negative consequence of this process would be the possibility of having many bills with hidden contingencies allowing for the continued abuse of civil liberties, similar to how vague language in the USA FREEDOM Act allows certain national security powers from the USA PATRIOT Act to continue. However, these hidden contingencies safeguarding dangerous national security powers would eventually have to be expelled from bills or else there would be little reason to continue passing such bills for practical purposes.

The solution that makes the most viable sense is the last option which requires passing the State Surveillance Repeal Act which completely abolishes the USA PATRIOT Act and FISA Amendments Act of 2008 immediately, thus restoring all civil liberties that were protected prior to 2001. The act would be able to make a significant amount of changes to national security law in a single passage, thus being the quickest way to resolve many civil liberty violation issues in the United States. The State Surveillance Repeal Act was introduced in the House of Representatives on July 24, 2013 by Rep. Rush Holt [D-NJ-12]; however, the act never came to a vote and thus was not implemented. The State Surveillance Repeal Act's passage would tip the balance between privacy and security through very concise and clear terminology designed to be heavily in favor of protecting individual liberties without unduly risking any national security concerns.

State Surveillance Repeal Act

The State Surveillance Repeal Act is the perfect act for restoring the protection of civil liberties to American citizens. The basis of the act is described in sections 2 and 3(a) of the act:

> Section 2 Repeal of USA PATRIOT Act. The USA PATRIOT Act (Public Law 107–56) is repealed, and the provisions of law amended or repealed by such Act are restored or revived as if such Act had not been enacted. Section 3 Repeal of the FISA Amendments Act of 2008 (a) Repeal.—The FISA Amendments Act of 2008 (Public Law 110–261; 122 Stat. 2477) is repealed, and the provisions of law amended or repealed by such Act are restored or revived as if such Act had not been enacted (State Surveillance Repeal Act, 2013, Sections 2 and 3(a))

Sections 2 and 3 use very clear language to ensure that no future court can misinterpret the intention to completely abolish the provisions in the stated acts. The remaining eight sections of the act are used to further ensure the protection of civil liberties and the reduction of national security powers. The State Surveillance Repeal Act's requirements for the reduction of national security powers and the protections of civil liberties force increased transparency in the federal court system and an increase of independent checks on national security agent activities. Some of the included provision requirements are as follows: they extend the maximum term of FISA judges to ten years from seven years, permit FISA courts to appoint amicus curiae to advise on technical issues raised during proceedings, require orders approving certain electronic surveillance to accomplish such surveillance in a manner to protect its secrecy and produce a minimum of interference with the subject being spied on, prohibits information relating to an American citizen from being acquired pursuant to FISA without a valid warrant based on probable cause, bar the federal government from requiring manufacturers of electronic devices and related software to build in mechanisms allowing the federal government to bypass encryption or privacy technology, and direct the Comptroller General to report annually on the

federal government's compliance with FISA. All of these provisions are sufficient for national security powers to be in constitutional harmony with the civil liberties of American citizens and thus the adoption of the State Surveillance Repeal Act into federal law is strongly recommended to strike the proper balance between security and privacy in the United States.

The proper balance between security and privacy has been achieved many times throughout American history in order to cope with different national and international situations. The proper balance constantly changes to deal with threats against domestic safety; in times of war the balance must shift towards national security to ensure the protection of the American citizens and in times of peace the balance must shift towards the protection of privacy rights to ensure the protection of civil rights and domestic tranquility. During extremely dangerous international situations, it may be necessary to suspend certain civil rights for a temporary period of time; however, the period of time must be temporary and the suspension should be no greater than necessary to protect our democracy. A great example of the Federal Government mishandling the balance between privacy and security is when the President George W. Bush Administration created the USA PATRIOT Act in response to the September 11th terrorist attacks. The terrorist attacks established the prerequisite for changing the balance to restore order to domestic affairs; however, the USA PATRIOT Act was not temporary and suspended far too many civil rights to be justified under the United States Constitution. The USA PATRIOT Act lasted over a decade and was an overreaction that allowed for the Federal Government to continue making decisions that jeopardized the democracy as a whole such as the decision to enter into the war in Iraq in 2003. The decision to enter into the war in Iraq was completely

unjustifiable, yet it was undertaken thanks to a very deceptive and guarded administration created by acts such as the USA PATRIOT Act.

The President George W. Bush Administration was not the only administration to have ever created a shift in the balance between privacy and security that was dangerous for maintaining a democracy. There are many examples of United States Presidents completely overreacting to national and international threats by ignoring the United States Constitution. Examples of Presidents shifting the balance too far towards complete authoritarian control and dismissal of necessary civil rights can be seen in President John Adams Administration's passage of the Alien and Sedition Acts in 1798 in response to a possible war with France, President Abraham Lincoln Administration's suspension of habeas corpus in order to quell Southern rebellion during the Civil War, and President Franklin D. Roosevelt Administrations' establishment of Japanese internment camps to prevent potential attacks and spying in World War II. In all of these examples, the Federal Government completely ignored vital constitutional rights in order to deal with very dangerous international and national threats; however, none of the security actions were necessary to defeat their enemies and the actions suspended civil rights to the extent that they could not be justified.

The proper balance between security and privacy is very difficult to maintain because of constant changes in international and national threats against society. The proper balance must constantly change to adapt to changes in the global environment without going towards either extreme. If the balance between privacy and security goes too far towards granting dangerous national security powers then it defeats the entire purpose of living in a democratic and free society. If the balance between privacy and security goes too far towards granting complete civil

rights and eliminating all national security powers then the country will risk the safety of its citizens against unforeseen international and national attacks.

An example of the Federal Government doing an excellent job of altering the balance between security and privacy in response to an international threat can be seen in the way the Reagan Administration dealt with the Cold War against the Soviet Union. The Reagan Administration had the prudent policy of peace through strength. The administration was able to defeat the Soviet Union by increasing national security powers without decreasing civil rights for American citizens, thus perfectly balancing security with privacy in its unique global situation. The Reagan Administration mainly focused on the enemy overseas instead of potential domestic enemies. The Reagan Administration decreased Soviet access to high technology and diminished their resources, increased American defense expenditures to strengthen the U.S. negotiating position; and forced the Soviets to devote more of their economic resources to defense until the Communist government collapsed from within due to economic stagflation (a situation in which the inflation rate is high, the economic growth rate slows, and unemployment remains steadily high). The Reagan Administration never substantially reduced any civil rights for American citizens. In fact, quite the opposite occurred. An example of the increased awareness of the importance of maintaining civil rights protections for all Americans during the Reagan Administration was the passage of the Civil Liberties Act in 1988 which gave a formal apology and paid out $20,000 in compensation to each surviving victim of the Japanese-American World War II internment camps. The Reagan Administration's actions should be followed by future presidential administrations that seek to establish a proper balance between security and privacy for a specific time period.

References

Banks, C. P. & Tauber, S. (2014). U.S. District Court decision-making in USA PATRIOT Act cases after September 11. *Justice System Journal, 35*(2). 139-161.

Barnett, R. (2015).Why the NSA data seizures are unconstitutional. *Harvard Journal of Law and Public Policy, 38***.**

Bergen, P., Sterman, D., Schneider, E., & Cahall, B. (2014). Do NSA's Bulk Surveillance Programs Stop Terrorists? *New American Foundation*, 13.

Bloom, R. M., & Dunn, W. J. (2006). The Constitutional Infirmity of Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury to the Fourth Amendment. *William & Mary Bill of Rights Journal*, 15, 147-202.

Boeglin, J., & Taranto, J. (2015). Stare Decisis and Secret Law: On Precedent and Publication in the Foreign Intelligence Surveillance Court. *Yale Law Journal*, 124(6), 2189-2201.

Doe v. Gonzales, 546 U.S. 1301 (2005).

Eisenstadt v. Baird 405 U.S. 438 (1972).

Drew Fennell, The USA PATRIOT Act: Can We Be Both Safe and Free? 21 Del. Law. 10 (2003). Microforms, via Lexis, WESTLAW.

Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§1801 et seq.) (Oct. 25, 1978).

Goodlatte, B. (2015). USA FREEDOM Act. *United States House of Representatives Judiciary Committee,* Retrieved from http://judiciary.house.gov/index.cfm/usa-freedom-act

Gorham-Oscilowski, U., & Jaeger, P. T. (2008). National Security Letters, the USA

PATRIOT Act, and the Constitution: The tensions between national security and civil rights. *Government Information Quarterly, 25(4),* 625-644.

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

Hardin, D. (2003). Fuss over Two Small Words: The Unconstitutionality of the USA PATRIOT Act Amendments to FISA under the Fourth Amendment, *The. Geo. Wash. L. Rev.*, 71, 291.

Intelligence Reform and Terrorism Prevention Act of 2004 Pub. L. 108-458. 118 Stat. 3638. 17 Dec. 2004. Print.

Klayman v. Obama, 134 S.Ct. 1795 (2014).

Lane, F. S. (2009). *American Privacy: The 400-Year History of Our Most Contested Right.* Boston, MA, USA: Beacon Press.

Lisa Finnegan Abdolian & Harold Takooshian, The USA PATRIOT Act: Civil Liberties, the Media, and Public Opinion, 30 Fordham Urb. L. J. 1429 (2003). Via Lexis, WESTLAW, HeinOnline Law Journal Library.

Lungren, D. E. (2012). Congressional Perspective on the Patriot Act Extenders, *A. Notre Dame JL Ethics & Pub. Pol'y, 26*, 427. Retrieved from http://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1012&context=ndjlepp

Mayfield v. United States, 504 F. Supp. 2d 1023 (2007).

McGowan, C. J. (2013). Relevance of Relevance: Section 215 of the USA PATRIOT Act and the NSA Metadata Collection Program, *The. Fordham L. Rev., 82*, 2399. Retrieved from http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4988&context=flr

Michaud, Kate (2012). *United States v. Jones*: Why the Whole Court is calling for Congressional Action. *Harvard Law National Security Journal*.

National Association for the Advancement of Colored People v. Claiborne Hardware Co., 458 U. S. 886 (1982).

Ombres, D. (2015). NSA Domestic Surveillance from the Patriot Act to the Freedom Act: The Underlying History, Constitutional Basis, and the Efforts at Reform. *Seton Hall Legis. J., 39,* 27. Retrieved from http://scholarship.shu.edu/cgi/viewcontent.cgi?article=1075&context=shlj

Planned Parenthood of Southeastern Pa. v. Casey 505 U.S. 833 (1992).

Rackow, S.H. (2002). How the U.S.A. Patriot Act will permit governmental infringement upon the privacy of Americans in the name of "intelligence" investigations. *University of Pennsylvania Law Review*, 150, 1651-1695, p. 1673

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

Rubel, A. (2007). Privacy and the USA PATRIOT Act: Rights, the value of rights, and autonomy. *Law and Philosophy, 26(2),* 119-159.

Sinnar, S. (2003). Patriotic or unconstitutional? The mandatory detention of aliens under the USA PATRIOT Act. *Stanford Law Review*, 1419-1456.

Thorne, K., & Kouzmin, A. (2010). The USA PATRIOT Acts (et al.): Convergent legislation and oligarchic isomorphism in the "politics of fear" and state crime (s) against democracy (SCADs). *American behavioral scientist, 53(6),* 885-920.

U.S. Congress House of Representatives. (2013-2014). *H.R.2818 - Surveillance State Repeal Act 113th Congress.* Retrieved from https://www.Congress.gov/bill/113th-Congress/house-bill/2818

U.S. Const. Amend. I, IV, V, VI, XIV.

U. S. District Court for the District of Massachusetts. (2015). *United States v. Dzhokar Tsarnaev*, 13-cr-10200 (2015) Retrieved from https://casetext.com/case/united-states-v-tsarnaev-11

United States v. Jones, 132 S. Ct. 945, 565 U.S. ___ (2012).

United States v. U.S. District Court, 407 U.S. 297 (1972).

USA FREEDOM Act of 2015. Pub. L. 114-23. 2 Jun. 2015. Print.

USA PATRIOT Act of 2001. Pub. L. 107-56. 115 Stat. 272. 26 Oct. 2001. Print.

USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, Pub. L. No. 109-178, 120 Stat. 278 (Mar. 9, 2006)

USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (Mar. 9, 2006).

Verble, J. (2014). The NSA and Edward Snowden. *SIGCAS Comput. Soc. ACM SIGCAS Computers and Society*, 1-20.

Whitehead, J. W., & Aden, S. H. (2001). Forfeiting Enduring Freedom for Homeland Security: A Constitutional Analysis of the USA PATRIOT Act and the Justice Department's Anti-Terrorism Initiatives. *Am. UL Rev.*, *51*, 1081.

Xhelili, B., & Crowne, E. (2012). Privacy & Terrorism Review: Where Have We Come in 10 Years. *J. Int'l Com. L. & Tech.*, *7*, 121.

Yoo, John (2014). The Legality of the National Security Agency's Bulk Data Surveillance

Programs, *Berkeley Law School Repository.*

Zieske, W. F. (2004). Demystifying the USA PATRIOT Act. *Illinois Bar Journal*, *92*(2), 82-87.